JULIA ANGWIN

SPOŁECZEŃSTWO NADZOROWANE

W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji

SERIA CYWILZACJA

INNE SERIE:

BIZNES HORYZONTY

NOBEL Z EKONOMII

ZDROWIE

REFLEKSJE

ENERGIA

PRZYWÓDCY

BEZ MAKIJAŻU

SYZYF 2.0

SPOŁECZEŃSTWO NADZOROWANE

W POSZUKIWANIU PRYWATNOŚCI, BEZPIECZEŃSTWA I WOLNOŚCI W ŚWIECIE PERMANENTNEJ INWIGILACJI

JULIA ANGWIN

Przekład Kurhaus Publishing®

WARSZAWA 2017

Tytuł oryginału: *Dragnet nation: a quest for privacy, security and freedom in a world of relentless surveillance*
First published in 2014 by Times Books Henry Holt and Company, LLC

Wydanie polskie:

Przekład: Dominik Jednorowski, Paulina Jagielska
Redakcja i korekta: Kurhaus Publishing
Skład i łamanie: Anna Dąbrowska
Projekt okładki: Bart Biały

Wydanie elektroniczne 2017

ISBN: 978-83-65301-33-8
EAN: 9788365301338

Dostarczamy wiedzę
www.kurhauspublishing.com

Kurhaus Publishing Kurhaus Media sp. z o.o. sp. k.
Dział handlowy:
kontakt@kurhauspublishing.com, tel. +48 601803503
ul. Cynamonowa 3, 02-777 Warszawa

Konwersja publikacji do wersji elektronicznej

Spis treści

Moim dzieciom

PRZEDMOWA DO WYDANIA POLSKIEGO

„W świecie, w którym niemal wszystko jest monitorowane, łatwo jest poczuć się bezradnym, gdy chodzi o prywatność. Kiedy mówię napotkanym osobom, że piszę o prywatności, często ich natychmiastową reakcją jest: «Ja już się poddałem. Prywatność umarła». Czy da się żyć w nowoczesnym świecie i jednocześnie wymknąć się spod nadzoru sieci? Czy w jakimś sensie nie pogodziłam się już z wszechobecną inwigilacją, wymieniając moje dane na darmowe usługi albo większe bezpieczeństwo?". To pytanie, stawiane przez Julię Angwin, autorkę książki *Społeczeństwo nadzorowane* staje się jednym z kluczowych problemów współczesności. Od tego, jak na nie odpowiemy, zależy bowiem sposób naszego funkcjonowania w społeczeństwie epoki internetu, rozwiązań chmurowych, e-zakupów czy sieci społecznościowych. Czy pełne wykorzystanie dostępnych rozwiązań technologicznych, niewątpliwie ułatwiających życie i kontakty międzyludzkie, oznacza jednocześnie rezygnację z prywatności? Gdzie leży granica pomiędzy tym, co możemy ujawniać w sieci, a tym, co jednak należy zachować dla siebie?

Hasło „cyberbezpieczeństwo" jeszcze nie do końca kojarzy się nam z życiem osobistym, choć powinno. Ale też i w komunikowaniu wiedzy o związanych z nim zagrożeniach, większą wagę przywiązuje się do odbiorców biznesowych niż indywidualnych. Tymczasem „sieć", czyli rozliczne bazy danych, gromadzące – za naszą zgodą lub bez niej – informacje o tym, co robimy, czym się interesujemy, dokąd jeździmy, co lubimy najbardziej, wie o nas znacznie więcej, niż przypuszczamy. Prawdopodobnie nawet zna nas lepiej niż my znamy samych siebie, bo człowiek o wielu rzeczach potrafi szybko zapomnieć, gdy tymczasem cyfrowy zapis trwa aż do jego usunięcia, a nawet dłużej. Większości z nas

zresztą specjalnie nie interesuje, co dzieje się z informacjami zbieranymi przez Facebook, Google, Amazon, Twitter, sklepy internetowe, wszelkiego rodzaju systemy rezerwacyjne itd. Nie zdajemy sobie także sprawy, jak dokładne i precyzyjne portrety można na ich podstawie sporządzić i jak wiele o nas mówią.

Tak naprawdę to jednak tylko część problemu. Ta, na którą mamy pewien wpływ, bo zgodnie z europejskim prawem możemy sprawdzać w bazach danych, jakie informacje o nas są przechowywane, weryfikować je, poprawiać lub żądać ich usunięcia. Coraz trudniej je zidentyfikować, bo często bez świadomości tego, co to oznacza, zgadzamy się na udostępnianie tych informacji podmiotom trzecim dla celów marketingowych czy informacyjnych, a handel bazami danych to dziś coraz bardziej intratna dziedzina biznesu. Nie mamy natomiast wpływu na to, w jaki sposób naszą aktywność monitorują władze, a przede wszystkim różne rządowe agencje, które – wykorzystując m.in. rosnące zagrożenie terrorystyczne – w wielu krajach otrzymały prawo do głębokiej inwigilacji obywateli: sprawdzania, o czym piszą w e-mailach, o czym rozmawiają przez telefony komórkowe czy komunikatory i jak się przemieszczają (co łatwo zweryfikować za pomocą danych GPS z komórki czy samochodowej nawigacji).

Skalę usankcjonowanego przez władze USA procederu szpiegowania obywateli pokazał czarno na białym Edward Snowden, były pracownik Centralnej Agencji Wywiadowczej (CIA) i współpracownik Agencji Bezpieczeństwa Krajowego (NSA). 17 czerwca 2013 roku brytyjski dziennik „The Guardian" opublikował przekazane przez niego informacje, z których wynikało, że służby wywiadowcze Stanów Zjednoczonych inwigilowały polityków biorących udział w szczycie G20 w 2009 roku, monitorując ich komputery i telefony. Snowden ujawnił także dokumenty, które potwierdzały, że rząd Stanów Zjednoczonych masowo śledzi swych obywateli m.in. za pomocą programu PRISM, umożliwiającego podsłuchiwanie rozmów Amerykanów i obywateli innych krajów, prowadzonych poprzez telefony VoIP i internet. Według Snowdena PRISM pozwalał NSA nie tylko na przeglądanie poczty elektronicznej, dostęp do czatów i wideoczatów, ale też na czerpanie informacji z serwisów społecznościowych. W program zostały zaangażowane globalne firmy związane z internetem i komunikacją, m.in. Microsoft, Google, Yahoo!, Facebook, YouTube, AOL czy Apple. Podobnym systemem do inwigilacji, o nazwie Tempora, dysponowały – według Snowdena –

służby brytyjskie. Obrońcy rządowego „podglądania" powołują się przede wszystkim na kwestie bezpieczeństwa narodowego, jednak skala operacji, na które pozwalają dzisiejsze technologie, zaskoczyła chyba wielu.

Jeszcze innym, narastającym w bardzo szybkim tempie, problemem jest działalność hakerów i nasilające się ataki – zarówno na komputery prywatne, jak i te należące do korporacji. Według szacunków firm zajmujących się cyberbezpieczeństwem, średnia liczba ataków hakerskich (o różnej skali, służących wszelkim celom), dokonywanych na świecie każdego dnia, wynosi ok. 26 tysięcy. Przewiduje się, że – także w Polsce – będzie wciąż rosła. Sprzyja temu proliferacja narzędzi hakerskich, w tym również tych wykorzystywanych przez służby specjalne – ujawnionych między innymi przez grupę Shadow Brokers. O skali zagrożenia można się było przekonać w czerwcu 2017 roku, kiedy z pomocą złośliwego oprogramowania typu *ransomware* o nazwie WannaCry, Petya (notPetya) zaatakowano m.in. systemy komputerowe na Ukrainie, w Danii, Rosji, Wielkiej Brytanii, Indiach, USA i Holandii. Ukraina była jednym z krajów, które ucierpiały najbardziej – celem były m.in. system bankowy i telekomunikacyjny, rządowe sieci komputerowe, najważniejsze lotniska w kraju, ciepłownie, elektrownie oraz metro w Kijowie i sieci supermarketów. Zagrożenie nie ominęło także Polski. Coraz większym problemem staje się bezpieczeństwo systemów przemysłowych, jeszcze do niedawna odciętych od zewnętrznych wpływów, a obecnie, dzięki rozpowszechniającemu się ich „usieciowieniu", coraz bardziej podatnych na takie ataki. A przecież w perspektywie mamy jeszcze autonomizację transportu, która także będzie oparta na protokołach sieciowych, czy internet rzeczy. Hakerzy jednak nie zagrażają wyłącznie firmom – ich celem stają się także nasze prywatne komputery i smartfony, w których można znaleźć wiele wrażliwych danych (m.in. kody do bankowości internetowej, hasła do portali społecznościowych czy skrzynek mailowych) albo wykorzystać je, jako zasoby do przechowywania danych czy moc obliczeniową do kopania kryptowalut.

Obywatele i przedsiębiorstwa znajdują się dziś nie tylko w centrum zainteresowania tzw. dragnetów państwowych (elektroniczne bazy danych dozoru amerykańskich obywateli, rozwijane w ramach projektu Dragnet, o którym po raz pierwszy poinformowano w 2005 roku, a więcej informacji o nim ujawnił dopiero w 2013 roku Edward Snowden). Wirtualną aktywność wnikliwie śledzą także podmioty komercyjne, organy ścigania i cyberprzestępcy. Kierunki rozwoju gospodarczego

i społecznego wyraźnie wskazują, że usieciowienie będzie postępować. Internet jest siecią globalną, integrującą wiele elementów, wśród których są rozliczne bazy danych. Będzie ich zresztą zespalać coraz więcej. Obserwować będziemy także intensyfikację zjawiska migracji najważniejszych danych i procesów do chmur rozliczeniowych oraz wzrost znaczenia analityki wielkich zbiorów danych (Big Data). Odpowiednie wykorzystanie tych ostatnich pozwala scalać rozproszone zasoby i tworzyć nie tylko innowacyjne strategie biznesowe, oparte na analizie danych, ale też generować niezwykle precyzyjne profile klientów.

Trudno zatem nie zgodzić się z tezą, którą stawia Julia Angwin – w dobie internetu niemożliwe jest zachowanie takiej prywatności, jaką znaliśmy wcześniej. Z tym musimy się pogodzić, chyba że postanowimy całkowicie odciąć się od zdobyczy nowoczesnych technologii. Nie znaczy to, że prowadząc wirtualną aktywność jesteśmy całkowicie bezbronni. W tym kontekście książka *Społeczeństwo nadzorowane* jest dobrym punktem wyjścia do dyskusji i refleksji nad współczesnym modelem prywatności. Pokazuje bowiem, co należy wiedzieć i w jaki sposób myśleć o swoim życiu w sieci, aby uchronić się od groźnych skutków ataków cyfrowych oraz problemów wynikających z braku frasobliwości. Choć od jej światowej premiery minęły trzy lata, a to w rozwijającej się błyskawicznie cyfrowej rzeczywistości czas równy co najmniej dekadzie, to jednak proponowane przez autorkę procedury związane chociażby z przeprowadzaniem własnego, prywatnego „audytu sieciowego bezpieczeństwa" i weryfikacją mocnych i słabych stron naszych wirtualnych tożsamości, są uniwersalne i aktualne.

Podstawą bezpieczeństwa w sieci, a zatem i zachowania choć części prywatności, jest bowiem realna świadomość możliwych zagrożeń. Odnosi się to zarówno do korporacji, jak i osób prywatnych. Tym, co czyni z nas łatwy łup w internecie, jest niefrasobliwość i brak wiedzy. Wciąż bez zastanowienia wchodzimy na zainfekowane strony, podszywające się pod prawdziwe serwisy, nie sprawdzając ich certyfikatów bezpieczeństwa, otwieramy załączniki z maili od nieznanych adresatów, z lenistwa nie instalujemy aktualizacji oprogramowania, nie zmieniamy haseł i nie weryfikujemy ich siły. Słowem, nie zachowujemy elementarnej czujności, przejawiając ufność dzieci – niestety, kiedy ignorujemy zagrożenie albo nie chcemy go dostrzec, ono nie znika. Staje się jeszcze bardziej niebezpieczne.

Niewątpliwie w coraz to nowszych sieciowych rozwiązaniach kusi nas oferowana przez nie wygoda. Technologie, na przykład technologie

na rynku finansowym, umożliwiają nam wygodne płacenie kartą zbliżeniową, zaciąganie przez internet pożyczek w formule *peer-to-peer* (P2P), rezerwowanie aut, zamawianie taksówek itd. Jednak niefrasobliwe wykorzystanie tych rozwiązań naraża nas na utratę istotnych, wrażliwych danych. Ponownie wracamy więc do kwestii świadomości zagrożeń i wdrażania odpowiednich procedur, zarówno w życiu prywatnym, jak i w biznesie.

Zaczynają nas w tym wspomagać także rozwiązania prawne. Europejskie instytucje pracują dziś nad przepisami regulującymi zasady przetwarzania danych osobowych w kontekście nowych technologii – a także nad regulacyjnymi standardami technicznymi (np. projekt RTS czyli standardów silnego uwierzytelniania na potrzeby dyrektywy PSD2 itd.). W maju 2018 roku zacznie obowiązywać RODO, czyli unijne rozporządzenie dotyczące ochrony danych osobowych. Jednym z ważnym elementów, z punktu widzenia osób występujących w bazach danych administrowanych przez podmioty gospodarcze, będzie „prawo do bycia zapomnianym", czyli do usunięcia z tych baz informacji o sobie, np. po zakończeniu korzystania z danej usługi (po rezygnacji z abonamentu u operatora telewizji kablowej czy sieci komórkowej). Firmy będą także zobligowane do każdorazowego zgłaszania naruszeń danych osobowych, np. w wyniku ataku hakerskiego, do Generalnego Inspektora Ochrony Danych Osobowych. Obecnie o wielu takich incydentach nawet nie wiemy. Wdrażana jest także dyrektywa NIS (Network and Information Systems Directive) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Polska zmierza w kierunku budowy jednolitego systemu ochrony cyberprzestrzeni. Ma on być podparty stosowną ustawą a także wykorzystywać dotychczas istniejące cywilne komponenty, takie jak funkcjonujący w ramach NASK zespół Cert Polska, zespół Cert.Gov.pl ABW, sektorowe komórki CERT i Abuse czy komórki cyberbezpieczeństwa sfery wojskowej, jak również integrować nowe elementy systemu, jak np. Narodowe Centrum Cyberbezpieczeństwa lub Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji. Nowe narzędzia, wraz z rosnącą świadomością użytkowników sieci, powinny podnieść bezpieczeństwo naszej wirtualnej egzystencji.

Książka ta jest ważna także dla Deloitte, bowiem wpisuje się doskonale w wartości, które staramy się przekazywać naszym Partnerom i Klientom: bezpieczeństwo, świadomość i czujność wobec zagrożenia, a także

odporność na ataki. Zdajemy sobie sprawę, że konsekwencją zmieniającego się otoczenia biznesowego w skali globalnej jest rosnące zagrożenie cyberatakami. Podobnie jak obywatele korzystający z sieci, także firmy muszą się odpowiednio zabezpieczyć, aby ograniczyć ryzyko i móc w pełni wykorzystywać nowe możliwości.

Zapraszamy do lektury i do refleksji nad bezpieczeństwem cyfrowym. Warto poświęcić tym tematom dłuższą chwilę, bowiem, jak pisze autorka, „właśnie prywatność i bezpieczeństwo często umykają uwadze, gdy żyje się w ciągłym pośpiechu".

Jakub Bojanowski
Partner, Dział Konsultingu,
Deloitte Polska

Marcin Ludwiszewski
Dyrektor, Lider ds. cyberbezpieczeństwa,
Deloitte Polska

1

ZHAKOWANI

A was, kto obserwuje? Dawniej to pytanie zadawali wyłącznie królowie, prezydenci i osoby publiczne, próbując umknąć paparazzim czy unieszkodliwić przestępców, usiłujących obejść prawo. Reszta z nas nie musiała się specjalnie martwić tym, że może zostać objęta obserwacją.

Dziś owo niepokojące pytanie – „kto obserwuje?" – odnosi się do wszystkich i nie musi być wcale związane z czyjąś sławą albo przestępczą działalnością. Każdy z nas może być obserwowany niemal w każdej chwili – czy to przez samochód Google Street View, robiący właśnie zdjęcie naszego domu, czy przez reklamodawcę, który obserwuje nas w trakcie przeglądania stron internetowych, czy też przez amerykańską Agencję Bezpieczeństwa Krajowego (National Security Agency, NSA) rejestrującą nasze połączenia telefoniczne.

Sieci dragnet[*1] zbierające informacje dosłownie o wszystkich, którzy znajdą się w ich zasięgu, kiedyś były rzadkością; policja musiała organizować blokady dróg, a sieci handlowe instalować kamery i obserwować obraz. Jednak rozwój technologii dał początek nowej erze superpotężnych programów nadzoru, które potrafią gromadzić olbrzymie ilości danych osobowych bez udziału człowieka. Owe dragnety rozszerzają swój zasięg na coraz bardziej prywatne obszary naszego życia.

Przyjrzyjmy się relacji Sharon Gill i Bilala Ahmeda, bliskich przyjaciół, którzy poznali się w prywatnej sieci społecznościowej PatientLikeMe.com.

Trudno o dwie bardziej różniące się od siebie osoby. Sharon to czterdziestodwuletnia samotna matka mieszkająca w małym miasteczku na południu stanu Arkansas[1]. Próbuje wiązać koniec z końcem, wyszukując okazje na wyprzedażach garażowych i odsprzedając zakupione

towary na pchlim targu. Bilal Ahmed, samotny trzydziestosześciolatek, absolwent Uniwersytetu Rutgersa, mieszka w penthousie w australijskim Sydney[2]. Prowadzi sieć sklepów z produktami pierwszej potrzeby.

Choć nie mieli szansy poznać się osobiście, zaprzyjaźnili się na forum internetowym pacjentów zmagających się z problemami psychicznymi, wymagającym logowania przy użyciu hasła. Sharon próbowała właśnie odstawić leki antydepresyjne. Bilal natomiast stracił matkę – cierpiał na zaburzenie lękowe i depresję.

Łącząc się z dwóch krańców świata, wspierali się nawzajem w trudnych chwilach. Sharon postanowiła otworzyć się przed Bilalem, bo czuła, że nie jest w stanie zaufać bliskim krewnym czy sąsiadom. „Mieszkam w małym mieście. Nie chciałam, by myślano o mnie przez pryzmat choroby psychicznej", wyznała mi[3].

Jednakże w 2010 roku Sharon i Bilal odkryli z przerażeniem, że w tej właśnie prywatnej sieci społecznościowej ktoś ich śledził.

Wszystko zaczęło się od włamania. 7 maja 2010 roku portal PatientsLikeMe odnotował nietypową aktywność na forum o nastrojach, na którym spotykali się zwykle Sharon i Bilal[4]. Nowy członek portalu, wykorzystując do tego zaawansowane oprogramowanie, próbował ściągać [ang. *scrape*] lub skopiować dosłownie każdą wiadomość umieszczoną na prywatnych forach „Nastrój" oraz „Stwardnienie rozsiane", należących do PatientsLikeMe.

Portalowi udało się zablokować i zidentyfikować włamywacza: była to spółka Nielsen Company, zajmująca się badaniem mediów. Dla swych klientów, a są wśród nich wielcy producenci leków, Nielsen zajmuje się monitorowaniem tego, co „grzeje" w internetowej sieci. 18 maja administratorzy PatientsLikeMe przesłali do Nielsena list z żądaniem zaprzestania naruszania praw użytkowników, a samych użytkowników poinformowali o fakcie włamania. (Nielsen później wyjaśniał, że więcej już nie włamywał się na prywatne fora. „Uznaliśmy, że praktyki te są dla nas nieakceptowalne", miał powiedzieć Dave Hudson, szef zaangażowanej w sprawę jednostki Nielsena).

Nastąpił jednak zwrot akcji. PatientsLikeMe wykorzystał tę okazję, by poinformować swych członków, że mogli nie zauważyć, iż wcześniej zaakceptowali zasady korzystania z portalu, przedstawione im drobnym drukiem. Okazało się, że serwis sprzedawał dane o członkach społeczności firmom farmaceutycznym i innym podmiotom[5].

Wiadomość okazała się podwójnym ciosem dla Sharon i Bilala. Podglądał ich nie tylko włamywacz. Robili to także administratorzy platformy, którą każde z nich uważało za bezpieczną. To tak jakby ktoś sfilmował spotkanie anonimowych alkoholików, a organizacja AA przestraszyła się, że to nagranie zagrozi ich biznesowi polegającemu na nagrywaniu spotkań i sprzedawaniu taśm. „Poczułem, że naruszono wszystkie moje prawa", tłumaczył Bilal[6].

Co gorsza, właściwie żadne z tych działań nie było nielegalne. Nielsen poruszał się w prawnej szarej strefie i nawet jeśli naruszał swymi działaniami warunki korzystania z serwisu PatientsLikeMe, to niekoniecznie można było wyegzekwować ich przestrzeganie na drodze prawej[7]. A już całkowicie legalne było poinformowanie użytkowników PatientsLikeMe drobnym drukiem, że portal zamierza zgarnąć wszystkie dane o członkach serwisu i sprzedać je na rynku.

To właśnie tragiczny rys na „prywatności" w erze cyfrowej. Prywatność często jest definiowana jako wolność od podejmowanych przeciwko nam prób nieautoryzowanego dostępu[8]. Jednak wiele incydentów, które zdają się być naruszeniami prywatności, zostaje „autoryzowanych" w wyniku akceptacji formułek napisanych drobnym drukiem.

Zarazem na wiele sposobów sprzeciwiamy się tym autoryzowanym naruszeniom. Nawet jeśli bowiem firmy mają prawo zbierać dane o zdrowiu psychicznym ludzi, to czy jest to społecznie akceptowalne[9]?

Podglądanie rozmów Sharon i Bilala znalazłoby społeczną akceptację, gdyby byli oni dealerami narkotyków, a objęcie ich nadzorem miało podstawę w decyzji sądu. Ale czy zasysanie ich konwersacji do wielkiego dragnetu, który monitoruje poziom „grzania" [ang. *buzz*] w internecie, można uznać za społecznie akceptowalne?

Sieci, które masowo zbierają dane osobowe tego rodzaju plasują się dokładnie w szarej strefie – pomiędzy tym, co legalne, a tym, co społecznie akceptowalne.

* * *

Żyjemy w społeczeństwie nadzorowanym [ang. *dragnet nation*] – w świecie masowego śledzenia, w którym instytucje gromadzą dane o jednostkach w niespotykanym dotąd tempie[10]. Za nasilanie się tego zjawiska odpowiadają te same siły, które dały nam naszą ukochaną

technologię – potężne moce obliczeniowe komputerów osobistych, laptopów, tabletów i smartfonów.

Dopóki komputery nie były dobrym powszechnym, śledzenie jednostek było drogie i skomplikowane. Rządy zbierały dane wyłącznie przy takich okazjach jak narodziny, zawarcie związku małżeńskiego, nabycie własności nieruchomości czy śmierć. Firmy pozyskiwały dane tylko wtedy, gdy klient, zakupiwszy ich produkt, wypełnił kartę gwarancyjną lub przyłączył się do programu lojalnościowego. Tymczasem technologia sprawiła, że generowanie wszelkiego rodzaju informacji o nas, na każdym etapie naszego życia, stało się dla instytucji tanie i łatwe.

Zastanówmy się nad kilkoma faktami, które to umożliwiły. Począwszy od lat 70. moc obliczeniowa komputerów ulegała podwojeniu co około dwa lata, a urządzenia, które początkowo obejmowały swą wielkością obszar pokoju, zaczęły mieścić się w naszych kieszeniach[11]. Koszt magazynowania danych spadł z 18,95 dol. za 1 gigabajt w 2005 roku do 1,68 dol. w 2012 roku. W nadchodzących latach przewiduje się dalszy spadek, do wartości poniżej 1 dolara[12].

To właśnie połączenie potężnej mocy obliczeniowej oraz rozwoju technologii umożliwiających miniaturyzację urządzeń i tanie przechowywanie danych, pozwoliło śledzić nasze dane. Nie wszyscy, którzy nas obserwują, są włamywaczami, takimi jak Nielsen. Do śledzących można też zaliczyć instytucje, które uważamy za sprzymierzeńców, takie jak rząd czy firmy, z którymi robimy interesy.

Oczywiście, największe dragnety to te zarządzane przez rząd USA. Jak wynika z dokumentów ujawnionych w 2013 roku przez Edwarda Snowdena[*2], byłego współpracownika amerykańskiej NSA, agencja zbiera nie tylko olbrzymie ilości danych o komunikacji międzynarodowej[13], ale również te o połączeniach telefonicznych Amerykanów i ich ruchu w internecie.

NSA nie jest bynajmniej jedyną (choć być może jest najbardziej wydajna) instytucją zarządzającą[14] dragnetami. Rządy krajów na całym świecie – od Afganistanu po Zimbabwe – skwapliwie korzystają z technologii nadzoru[15], począwszy od sprzętu do masowego przechwytywania danych[16] [ang. *massive intercept*] po narzędzia, które pozwalają im zdalnie przejmować telefony i komputery ludzi. W Stanach Zjednoczonych technologie nadzoru – od dronów po automatyczne czytniki tablic rejestracyjnych[17] – wykorzystują nawet lokalne i stanowe

władze[18]. Dzięki nim wiedzą o przemieszczaniu się ich mieszkańców więcej niż kiedykolwiek w historii. Także lokalna policja coraz częściej śledzi ludzi z wykorzystaniem sygnałów nadawanych przez ich telefony komórkowe.

W międzyczasie dosłownie kwitną dragnety wykorzystywane dla celów komercyjnych. Sieci AT&T oraz Verizon sprzedają informacje o lokalizacji abonentów[19], choć nie wskazują przy tym ich imion i nazwisk. Właściciele centrów handlowych zaczęli wykorzystywać technologię do śledzenia klientów[20] w trakcie zakupów – w oparciu o sygnały nadawane przez znajdujące się w ich kieszeniach telefony. Markety spożywcze, takie jak Whole Foods, zaczęły wykorzystywać znaki cyfrowe[21] będące w istocie skanerami twarzy. Niektórzy sprzedawcy samochodów korzystają z usług[22], które świadczy m.in. Dataium – jeśli dysponują adresem e-mail swojego klienta, mogą dowiedzieć się, jakie modele aut wyszukiwał w internecie, zanim pojawił się w ich salonie.

Dosłownie setki reklamodawców i brokerów danych obserwuje was, gdy poruszacie się w sieci. Kiedy wyszukujecie hasło: „cukier we krwi", firmy które tworzą profile klienta na podstawie informacji związanych ze stanem zdrowia, mogą przypisać was do kategorii: „cukrzyk", a następnie umożliwić dostęp do tej informacji producentom leków oraz ubezpieczycielom. Poszukiwanie biustonosza może wyzwolić niekończącą się wojnę ofert[23] pomiędzy firmami bieliźniarskimi na jednym z wielu portali aukcyjnych.

Tymczasem jeszcze nowsze technologie śledzenia czają się tuż za rogiem: firmy implementują funkcje rozpoznawania twarzy[24] do telefonów i aparatów fotograficznych, w pojazdach zagnieżdża się lokalizatory[25], a w mieszkania wbudowuje bezprzewodowe „inteligentne" liczniki zużycia[26] energii. Do tego jeszcze firma Google rozwinęła technologię Google Glass[27] – na którą składają się maleńkie aparaty wmontowane w okulary, umożliwiające robienie zdjęć i kręcenie filmików bez konieczności ruszenia palcem.

* * *

Ludzie niefrasobliwi mówią: „Co właściwie jest takiego złego w tym całym zbieraniu danych przez niewidocznych obserwatorów? Czy komuś

dzieje się coś złego?".

Trzeba przyznać, że zobrazowanie osobistej krzywdy będącej wynikiem naruszenia ochrony danych może nastręczać problemów. Jeśli Sharon lub Bilal nie dostaną oferty pracy albo ubezpieczenia, mogą nigdy nie dowiedzieć się, która część tych danych za to odpowiada. Ludzie znajdujący się na liście „zakazu latania" [ang. *no-fly list*][*3] nie są informowani, na jakiej podstawie podjęto decyzję, by ich tam umieścić.

Ogólna odpowiedź na pytania niedowiarków jest prosta: tych cennych zasobów, jakimi są dane osobowe, można nadużywać. I będzie się ich nadużywać.

Przyjrzyjmy się jednemu z najstarszych i, jak by się wydawało, najmniej szkodliwych dragnetów: chodzi o biuro statystyczne USA (U.S. Census). Poufność danych osobowych[28] gromadzonych przez urząd jest gwarantowana prawem, a mimo tego raz za razem dochodzi do naruszeń. Podczas I wojny światowej[29] dane te wykorzystywano do lokalizowania sprawców naruszeń przepisów[30]. W trakcie II wojny światowej[31] urząd statystyczny dostarczał Tajnej Służbie Stanów Zjednoczonych (Secret Service) nazwiska i adresy japońsko-amerykańskich rezydentów. Informacje były wykorzystywane do zatrzymywania rezydentów japońskich i umieszczania ich w obozach odosobnienia. Urząd statystyczny USA oficjalnie przeprosił za to dopiero w 2000 roku. Natomiast w latach 2002–2003 biuro dostarczało[32] Departamentowi Bezpieczeństwa Krajowego informacji statystycznych o Amerykanach arabskiego pochodzenia. Dopiero po serii negatywnych artykułów prasowych[33] Census zrewidował swoją politykę i od urzędów chcących pozyskać informacje wrażliwe, takie jak rasa, pochodzenie etniczne, religia, przekonania polityczne czy orientacja seksualna obywateli, zaczął wymagać zgody najwyższych organów państwowych.

Oczywiście nie tylko Stany Zjednoczone[34] dokonują gwałtu na danych dotyczących ludności. Australia wykorzystywała spisy ludności, by wymusić migrację mieszkańców aborygeńskiego pochodzenia[35] na przełomie XIX i XX wieku. W Południowej Afryce spis powszechny był kluczowym instrumentem w opartym na apartheidzie systemie segregacji rasowej[36]. Podczas ludobójstwa w Rwandzie w 1994 roku[37], ofiary Tutsi były namierzane dzięki dowodom tożsamości, które wskazywały ich pochodzenie etniczne. W czasach Holokaustu[38] – we Francji, Polsce,

Holandii, Norwegii i w Niemczech – naziści wykorzystywali takie dane do lokalizowania Żydów przeznaczonych do eksterminacji.

Dane osobowe narusza się często z powodów politycznych. Jednym z niesławnych przypadków[39] był program Federalnego Biura Śledczego (Federal Bureau of Investigation, FBI) z późnych lat 60., zwany COINTELPRO[*4]. Ówczesny dyrektor FBI, J. Edgar Hoover, zapoczątkował program, by szpiegować „wywrotowców", a pozyskane informacje wykorzystywać do dyskredytowania ich i zniechęcania do działania. FBI posunęła się nawet do przesłania Martinowi Lutherowi Kingowi Jr. nagrań z obserwacji pokoi hotelowych, w których się zatrzymywał, chcąc doprowadzić do jego rozstania z żoną. Były one opatrzone notatką, którą King odczytał jako próbę nakłonienia go do popełnienia samobójstwa[*5].

Także cyberprzestępcy wpadli na to, że wykorzystywanie danych osobowych jest najlepszą metodą łamania zabezpieczeń różnych instytucji. Przypomnijcie sobie, jak chińscy hakerzy przeniknęli do sieci pioniera zaawansowanych zabezpieczeń[40], amerykańskiej spółki RSA. Hakerzy strollowali najpierw sieci społecznościowe, by pozyskać informacje na temat poszczególnych pracowników firmy. Następnie wysłali kilkorgu z nich maile zatytułowane: „Plan rekrutacyjny na 2011 rok". Mail był tak dobrze podrobiony, że jeden z pracowników przywrócił go z folderu ze spamem i otworzył. Plik, który się wówczas załadował, przeprowadził na jego komputerze instalację złośliwego oprogramowania. Stąd już łatwo było atakującym przejąć zdalnie kontrolę nad wieloma urządzeniami tej organizacji.

Krótko mówiąc: hakowano ludzi, nie instytucje.

Hakowaniem ludzi trudnią się nie tylko cyberprzestępcy. Handlowcy śledzą nas, gdy surfujemy w sieci, w nadziei na uzyskanie informacji, które pozwolą im „zhakować" nas do zakupu ich produktu. NSA zbiera dane dotyczące naszych połączeń telefonicznych, by opracować wzorce, które – jak wierzą jej szefowie – pozwolą władzom „zhakować" numery należące do terrorystów.

Oto jak możecie zostać „zhakowani":

- Możecie być w każdej chwili namierzeni.
- Możecie być podglądani we własnym domu – nawet w łazience.

- Możecie być niezdolni do utrzymania czegokolwiek w tajemnicy.
- Ktoś może się pod was podszyć.
- Możecie wpaść w pułapkę „korytarza luster”.
- Możecie zostać wykorzystani finansowo.
- Możecie być poddani okazaniu policyjnemu.

To nie jest wyczerpująca lista, raczej mała próbka tego, co dziś dzieje się w otaczającej nas rzeczywistości. Gdy spojrzymy na nią za jakiś czas, prawdopodobnie będziemy się śmiać – myśląc o wszystkich tych rzeczach, których na niej nie uwzględniłam.

naglowek_podrozdzial_jasny

MOŻECIE BYĆ W KAŻDEJ CHWILI NAMIERZENI

Wasze nazwiska, adresy i informacje o was – także lokalizacja waszych telefonów komórkowych w danym czasie – są gromadzone w różnych bazach danych, do których nie macie wglądu i nad którymi nie macie kontroli. Oczywiście waszym prześladowcom i konkurentom regularnie udaje się włamywać do tych baz.

W 1999 roku obłąkaniec nazwiskiem Liam Youens[41] wykupił u brokera danych o nazwie Docusearch możliwość wyszukania numeru ubezpieczenia, informacji o zatrudnieniu i adresu domowego kobiety, na punkcie której miał obsesję – Amy Boyer. Kilka dni później Youens pojechał do niej do pracy i zastrzelił ją, gdy wychodziła do domu. Następnie zastrzelił samego siebie.

Rodzina Boyer pozwała brokera danych, jednak Sąd Najwyższy stanu New Hampshire podtrzymał stanowisko sądu niższej instancji, że choć na brokerze danych spoczywał obowiązek „wykazywania uzasadnionej troski o bezpieczeństwo danych”, to jednak informacje takie jak adres miejsca wykonywania pracy nie mogą być uznane za prywatne, ponieważ „dają się bez problemu zaobserwować członkom społeczeństwa”.

Rodzice Boyer dostali niewiele: w 2004 roku, po wielu latach batalii prawnych[42] toczonych przeciwko Docusearch, zawarli w końcu ugodę opiewającą na 85 tys. dolarów. Firma Docusearch wciąż jest obecna na rynku[43] i na swej stronie internetowej reklamuje usługi „odwrotnego wyszukiwania numerów telefonów”, „wyszukiwania po tablicach

rejestracyjnych" czy „wyszukiwania numeru ubezpieczenia społecznego po nazwisku" oraz „wyszukiwania ukrytych rachunków bankowych".

Od tego czasu cena po której w sieci można kupić czyjś adres[44] spadła z ok. 200 dolarów, które zapłacił Youens, do zaledwie 95 centów. Dziś za tę kwotę można uzyskać pełen raport dotyczący danej osoby[45]. Cyberprześladowania upowszechniły się tak bardzo, że rzadko urastają dziś do rangi newsów.

Zastanówmy się nad pewnym przykładem. W 2010 roku[46] w wiceszeryf hrabstwa Sacramento, Chu Vue, został uznany winnym morderstwa po tym jak jego bracia zastrzelili Steve'a Lo – mężczyznę, który miał romans z żoną Vue. W trakcie procesu wyszło na jaw, że Vue wyszukiwał nazwiska Lo w bazach policyjnych[47], pytał kolegów o numery tablic jego auta[48] i szukał adresu Lo za pomocą internetowej książki telefonicznej[49]. Vue został skazany na karę dożywotniego więzienia, bez możliwości zwolnienia warunkowego[50].

Nawet z najbardziej niewinnych danych – takich jak informacje o podróży lotniczej – można zrobić użytek. W 2007 roku pracownik amerykańskiego Departamentu Handlu, Benjamin Robinson, został oskarżony o 163 naruszenia[51] rządowej bazy danych o rezerwacjach lotów międzynarodowych. Po rozstaniu z partnerką[52] dostał się do pliku zawierającego informacje o niej, jej mężu oraz synku. Na poczcie głosowej kobiety nagrał wiadomość, w której zapowiedział, że ma zamiar przejrzeć te pliki, by „sprawdzić, czy czegoś przed nim nie ukrywała". Zasugerował, że może sprawić, by została deportowana. W 2009 roku przyznał się do pozyskiwania informacji z zabezpieczonego komputera. Skazano go na trzy lata nadzoru sądowego.

Jesteśmy coraz bliżej czasów, w których śledzenie w czasie rzeczywistym będzie czymś zwyczajnym. Stany Zjednoczone już dziś wbudowują do paszportów technologię RFID[53] [ang. *radio-frequency identification*], która wykorzystuje fale radiowe do wysyłania danych na nieduże odległości[54]. Szkoły i pracodawcy wtapiają te czipy do identyfikatorów. W 2013 roku sąd federalny w Teksasie[55] nie uznał sprzeciwu uczennicy technikum wobec narzuconego przez szkołę obowiązku noszenia legitymacji z czipami RFID. Niektórzy pracodawcy zaczęli eksperymentować z pomysłami implantowania takich mikroprocesorów pod skórę pracowników – co zmusiło stan Kalifornia do wprowadzenia

zakazu takich praktyk[56].

Namierzanie telefonów komórkowych jest dziś codziennością[57] w pracy policji. W 2011 roku wraz z moim kolegą z „Wall Street Journal" Scottem Thurmem wysłaliśmy do dwudziestu największych stanowych i lokalnych wydziałów policji zapytanie w tej sprawie, w trybie dostępu do informacji publicznej. Osiem urzędów przekazało nam co najmniej streszczenia danych statystycznych[58], z których wynikało, że każdego roku stanowe i lokalne agencje namierzają w czasie rzeczywistym tysiące telefonów komórkowych. Gregg Rossman, prokurator w hrabstwie Broward na Florydzie mówi, że to dziś coś tak oczywistego[59], jak „szukanie odcisków palców lub pobieranie próbek DNA".

W sposób nieunikniony, telekomy zaczęły sprzedawać dane o lokalizacji telefonów komórkowych znacznie szerszemu gronu odbiorców niż organy ścigania. W 2013 roku spółka Verizon poinformowała o swoim nowym produkcie[60], nazwanym Precision Market Insight, który pozwala właścicielom firm namierzać telefony komórkowe ich klientów w określonych lokalizacjach.

Jako jedna z pierwszych z usługi Verizonu skorzystała drużyna koszykarska Phoenix Suns, która chciała dowiedzieć się, gdzie żyją jej fani. Wiceprzewodniczący klubu Scott Horowitz wyjaśniał: „To są te informacje, które każdy zawsze chciał posiadać, a których pozyskanie jeszcze do niedawna było niemożliwe".

MOŻECIE BYĆ PODGLĄDANI WE WŁASNYM DOMU – NAWET W ŁAZIENCE

W 2009 roku piętnastoletni uczeń szkoły średniej, Blake Robbins[61], został oskarżony przez wicedyrektor placówki o „nieprawidłowe zachowanie w domu". Kobieta twierdziła, że ma na to dowody. Okazało się, że Harriton Hight School – szkoła, do której uczęszczał chłopak, zlokalizowana w dzielnicy pełnej placówek oświatowych na zamożnych przedmieściach Filadelfii – zainstalowała szpiegowskie oprogramowanie w komputerach Apple MacBook, które rozdała dwóm tysiącom trzystu swych uczniów. Na wybranych laptopach szkolni informatycy zainstalowali oprogramowanie, które mogło robić zdjęcia za pomocą

kamerki wbudowanej w sprzęt, a także kopiować widok ekranu komputera.

Kamera w komputerze Blake'a uchwyciła go, trzymającego coś przypominającego kształtem tabletkę. Blake i jego rodzina twierdzili, że to cukierki marki Mike and Ike[62]. Wicedyrektorka uważała, że to narkotyki.

Rodzina Blake'a pozwała dzielnicę za naruszenie prywatności ich syna. Szkoła poinformowała, że oprogramowanie zostało zainstalowane na komputerach po to, by w przypadku kradzieży informatycy mogli namierzyć sprzęt. Instytucja nie powiadomiła[63] jednak uczniów o istnieniu tego oprogramowania, a także nie stworzyła wytycznych dla informatyków, określających sposób wykorzystywania kamer.

W toku prowadzonego postępowania wyjaśniającego[64] okazało się, że kamery zostały uruchomione na ponad czterdziestu laptopach i przechwyciły ponad sześćdziesiąt pięć tysięcy zdjęć. Niektórzy uczniowie zostali sfotografowani tysiące razy[65], także w sytuacjach, gdy byli częściowo rozebrani lub podczas snu. Były uczeń, Joshua Levin[66], powiedział, że doznał „szoku, upokorzenia oraz silnego urazu emocjonalnego", gdy zobaczył przeszło osiem tysięcy zdjęć i zrzutów z ekranu, wykonanych na jego laptopie. Levin, Robbins i jeszcze jeden uczeń pozwali szkołę[67] i zawarli z nią sądową ugodę, uzyskując finansowe zadośćuczynienie. Rada szkoły zakazała dalszego wykorzystywania kamer do nadzoru uczniów[68].

Przyzwyczailiśmy się do tego, że kamery monitoringu są wszędzie. Szacuje się, że na samym tylko Dolnym Manhattanie[69] działa przeszło cztery tysiące takich jednostek. Londyn słynie z przeszło pięciuset tysięcy kamer monitoringu[70].

Ale gdy kamery stają się coraz mniejsze i zaczynają wędrować do naszych domów i najbardziej nawet intymnych przestrzeni, zmieniają nasze rozumienie tego, co publiczne, a co prywatne. Ceny wyposażonych w kamerki dronów spadły tak bardzo, że obiekty te stały się naszym utrapieniem. Pewna kobieta mieszkająca w Seattle, już w maju 2013 roku skarżyła się na to na lokalnym blogu[71]. Jakiś nieznajomy „skierował drona wprost nad mój ogródek, a następnie obleciał nim cały dom. Dzień był bardzo ciepły i początkowo myślałam, że głośny dźwięk, który ten sprzęt wydawał, pochodził z jakiejś kosiarki do trawy". Mąż kobiety zwrócił uwagę człowiekowi sterującemu dronem, a ten oświadczył, że ma

prawo korzystać z urządzenia, które, co więcej, wyposażone jest w kamery. „Jesteśmy bardzo zaniepokojeni tym faktem. Przecież mógł to być przestępca, który planuje włamanie do naszego domu albo podglądacz".

Te fantastyczne technologie źli ludzie wykorzystują oczywiście do konfigurowania swoich własnych dragnetów. W 2013 roku dziennikarz Nate Anderson opisywał pewną społeczność hakerów, która sprzedaje porady i techniki instalowania oprogramowania szpiegującego w kamerkach internetowych komputerów należących do kobiet[72]. „Działają w sieci w sposób zupełnie otwarty, dzieląc się wiedzą o najskuteczniejszych metodach podglądania", pisał. „W większości przypadków nazywanie tych gości hakerami jest krzywdzące dla hakerów. Do tego, co jest istotą ich działalności, wystarczą minimalne umiejętności techniczne".

W 2011 roku Luis Mijangos z Santa Ana został skazany[73] za hakowanie oraz nielegalne przejęcie kontroli nad kamerkami internetowymi w ponad setce komputerów, którym zainstalował złośliwe oprogramowanie. Między innymi przechwycił obrazy z kamery nastolatki, przedstawiające ją nago. Mężczyzna wykorzystywał takie zdjęcia do wyłudzania kolejnych rozbieranych zdjęć swych ofiar. W trakcie odczytywania wyroku, sędzia stwierdził, że „praktycznie nie różniło się to od regularnych działań polegających na zastraszaniu ofiar". Mijangos został skazany na sześć lat więzienia.

Kamery dragnetów o olbrzymim zasięgu czają się tuż za rogiem. Pojawianie się wyposażonych w kamery urządzeń ubieralnych, takich jak Google Glass, oznacza, że filmować będzie można dosłownie wszystko. Nick Bilton, publicysta dziennika „The New York Times", był zaskoczony, gdy podczas konferencji Google'a zauważył, że uczestnicy mają na sobie kamerki Google Glass nawet w toalecie[74].

Entuzjaści Google Glass twierdzą, że aparaty na ich głowach dosłownie zmieniają ich życie. Po dwóch tygodniach korzystania z nich, bloger Rober Scoble pisał: „Od dziś nie wyobrażam sobie już ani dnia tez tego sprzętu (albo podobnego produktu, pochodzącego od konkurencji)[75]". „Niektórych strasznie to wkurza", przyznał. Dodał jednak: „To dlatego, że są zupełnie nowe. Gdy wejdą na rynek, głosy sprzeciwu znikną".

MOŻECIE BYĆ NIEZDOLNI DO UTRZYMANIA

CZEGOKOLWIEK W TAJEMNICY

Bobbi Duncan, dwudziestodwuletnia lesbijka studiująca na Uniwersytecie Teksasu w Austin, chciała utrzymać swoją orientację seksualną w tajemnicy przed rodziną[76]. Jednak nieumyślnie ujawnił ją Facebook, gdy przewodniczący działającego w kampusie studenckim Chóru Queer dodał Bobbi do grupy dyskusyjnej członków chóru. Bobbi nie wiedziała, że przyjaciel może dodać ją do jakiejś grupy, nie zapytawszy jej wcześniej o zgodę, oraz że gdy już zostanie dodana do jakiejś grupy, Facebook poinformuje o tym wszystkich jej znajomych, włączając w to ojca.

Dwa dni po otrzymaniu powiadomienia, że Bobbi dołączyła do Chóru Queer, jej ojciec napisał na wallu organizacji: „Piszę do was wszystkich, cioty. Wracajcie do waszych nor i czekajcie na Boga. Czeka was piekło, zboczeńcy. Bawcie się dobrze, śpiewając tam".

Rzecznik prasowy Facebooka, Andrew Noyes, poinformowany o sprawie, stwierdził, iż to „nieszczęśliwe doświadczenie uświadamia nam, że musimy kontynuować prace nad wzmacnianiem i edukowaniem użytkowników z zakresu solidnej kontroli prywatności". Swoją postawą dał do zrozumienia, że wina leży po stronie ofiary, która w nieprawidłowy sposób skonfigurowała na swym Facebooku powiadomienia i zabezpieczenia. Nie było jednak ani powiadomienia, ani zabezpieczenia, które zapobiegłoby umieszczeniu Bobbi w danej grupie bez jej zgody.

„Uważam, że wina leży po stronie Facebooka", mówi Bobbi. „Nie powinno być tak, że ktoś za mnie decyduje o tym, co ludzie będą o mnie wiedzieć".

Gdy przemiatanych [ang. *sweep*] jest coraz więcej danych osobowych znajdujących się w różnych bazach, coraz trudniej jest utrzymać jakąkolwiek tajemnicę – nawet specjalistom. Doskonałym przykładem jest historia Davida Petraeusa[77], dyrektora Centralnej Agencji Wywiadowczej (Central Intelligence Agency, CIA), który zrezygnował z funkcji po tym jak w ramach dochodzenia prowadzonego w pewnej niezwiązanej z nim sprawie, odkryto e-maile, wskazujące, że miał romans. W 2012 roku były analityk CIA John Kiriakou został zidentyfikowany[78] jako przekazujący informacje niejawne, częściowo w oparciu o dowody w postaci e-maili. Przyznał się do winy[79] i został skazany na trzydzieści miesięcy pozbawienia wolności.

Dziś trudno jest utrzymać nawet drobne sekrety. Ludzie, którzy

pobierają z sieci filmy pornograficzne stali się celem tzw. *copyright* trolli[80]. Podmioty te masowo pozywają użytkowników portali umożliwiających wymienianie się plikami, którzy ściągnęli takie filmy na swe komputery, sugerując, że chcą chronić właścicieli praw autorskich do tych utworów. W ten sposób pozyskują informacje o tożsamości użytkowników, a następnie wysyłają im wezwania do polubownego załatwienia sprawy poprzez uiszczenie danej kwoty, licząc na to, że zawstydzona ofiara przyjmie ofertę.

W lipcu 2012 roku Sąd Apelacyjny USA dla Piątego Okręgu wymierzył karę[81] jednemu z takich powodów, adwokatowi reprezentującemu producenta filmów dla dorosłych, który pozwał na podstawie adresów IP sześciuset siedemdziesięciu użytkowników portali oferujących taką rozrywkę i próbował pozyskać ich tożsamości bez zgody sądu. Sąd opisał naruszenie, którego dokonał ów adwokat jako „uprawianie procederu pozywania anonimowych użytkowników internetu za rzekome nielegalne pobieranie pornografii, przy wielokrotnie podejmowanych próbach wykorzystania instytucji sądu do ustalania ich tożsamości, a następnie zawstydzenia ich i zastraszania, celem wymuszenia ugód wartości dziesiątków tysięcy dolarów”[82].

W maju 2013 roku sędzia z Kalifornii poszedł jeszcze dalej[83], ogłaszając, że trolle copyrightu wykorzystywali „serię nieaktualnych przepisów dotyczących praw autorskich, zjawisko społecznej stygmatyzacji i strach przed niebotycznymi kosztami obrony sądowej” do „łupienia obywateli”.

KTOŚ MOŻE SIĘ POD WAS PODSZYĆ

Jaleesa Suell została odebrana matce[84] i umieszczona w rodzinie zastępczej, gdy miała osiem lat. W sumie, do opuszczenia systemu pieczy zastępczej, przebywała w siedmiu takich rodzinach. Gdy ukończyła dwadzieścia jeden lat i zrobiła dyplom na Uniwersytecie Jerzego Waszyngtona, złożyła wniosek o wydanie karty kredytowej. Dowiedziała się wówczas, że członek rodziny skradł jej tożsamość, założył na jej nazwisko kartę, zaciągnął dług i nie spłacił go.

Bez możliwości pozyskania kredytu, Jaleesa nie mogła kupić auta i bała się, że nie będzie jej stać po ukończeniu studiów na mieszkanie. Tak mówiła o tym uczestnikom szkoleń poświęconych kradzieży tożsamości

w 2011 roku: „Często ogarniał mnie strach, że następnego dnia nie będę miała gdzie mieszkać albo co jeść. Odkąd się usamodzielniłam, starałam się pracować ciężko na to, by coś takiego nigdy nie powtórzyło się w moim życiu. Tymczasem znalazłam się we właśnie takiej sytuacji – z tego prostego powodu, że nie mam dostępu do linii kredytowej".

Niestety, to dzieci z rodzin zastępczych, takie jak Jaleesa, najczęściej stają się ofiarami przestępstwa kradzieży tożsamości. Osobiście wolę nazywać to „podszywaniem się"[85] [ang. *impersonation*], bo przecież tak naprawdę nikt nie może ukraść wam tożsamości. Jaleesa jest wciąż sobą. Ktoś po prostu podszył się pod nią, by uzyskać finansową korzyść.

W odpowiedzi na problem narastający wśród wychowanków rodzin zastępczych[86], prezydent Barack Obama podpisał w 2011 roku ustawę, na mocy której firmy dostarczające informacje o historii kredytowej obywateli, zobowiązuje się do przesyłania takim dzieciom, po ukończeniu przez nie 16. roku życia, bezpłatnych raportów z ich danymi finansowymi. Firmy te muszą to robić raz do roku – do opuszczenia przez wychowanków systemu pieczy zastępczej.

Jednak problem leżący u podstaw tego zjawiska wciąż narasta. W 2012 roku liczba zgłoszeń kradzieży tożsamości[87] była większa niemal o jedną trzecią w stosunku do roku 2011 – wynosiła 369 milionów wobec 279 milionów rok wcześniej. Według danych zgromadzonych przez Federalną Komisję Handlu (Federal Trade Commission, FTC) przez pięć wcześniejszych lat utrzymywała się na stałym poziomie.

Według Steve'a Toporoffa, prawnika z FTC, który kieruje programem ochrony tożsamości prowadzonym przez agencję, dawniej najczęstszą przyczyną zgłoszeń była kradzież karty kredytowej[88]. Dziś najwięcej dotyczy nadużyć podatkowych. „Obserwujemy także nowe formy nadużyć, na przykład medyczne, polegające na posługiwaniu się danymi dotyczącymi tożsamości innej osoby celem wyłudzenia świadczeń", mówi Toporoff. Stosunkowo trudno jest wykryć nadużycia medyczne czy podatkowe, skoro ludzie mają utrudniony dostęp swych danych. Nie da się ich weryfikować z taką łatwością jak historii kredytowej.

W 2013 roku dwie kobiety pochodzące z Florydy zostały skazane w związku z procederem mającym na celu wyłudzenie 11 mln dolarów[89] od amerykańskiego urzędu podatkowego (Internal Revenue Service, IRS). Miały one przesłać do urzędu prawie dwa tysiące sfałszowanych deklaracji podatkowych. Departament Skarbu wypłacił im niemal 3,5 mln

dolarów zwrotu. Jedna z kobiet, Alci Bonannee, wypełniła wiele fałszywych deklaracji z wykorzystaniem danych osobowych, które kupiła od pielęgniarki pracującej w jednym ze szpitali. Szpital Baptist Health Sougt Florida poinformował[90], że skradziono dane 834 pacjentów. Pracownik urzędu, Tony Gonzalez, powiedział w rozmowie z lokalną telewizją, że „źli ludzie, którzy potrafią pozyskać numery ubezpieczeń chorych, kupują je od pracowników szpitali i centrów medycznych; są sprzedawane po 150 dol. za numer".

Dane identyfikacyjne są nie tylko kradzione. Stale też dochodzi do ich wycieków. Z różnych powodów: począwszy od niedbalstwa po hakerstwo. Oficjalne raporty dotyczące przypadków naruszenia danych wskazują na stałe nasilanie się tego zjawiska – począwszy od 2009 roku[91]. Jak wyczytać można na stronie internetowej Open Security Foundation's DataLossDB, w 2012 roku liczba naruszeń wzrosła drastycznie, bo aż o 43 procent.

Firmy są rzadko karane za to, że nie dopilnowały danych klientów. Swego rodzaju testem może być sprawa, która odbywa się w związku z nawracającymi atakami hakerów na sieć hoteli Wyndham. W 2008 roku hakerzy włamali się do sieci komputerowej hotelu w Phoenix. Poprzez sieć hakerzy uzyskali dostęp do rachunków kart kredytowych[92] przeszło pięciuset tysięcy klientów wszystkich czterdziestu jeden obiektów działających pod marką Wyndham. Informacje te przesłali do Rosji. Obciążając karty tytułem opłat za nieistniejące towary lub usługi[93], mieli uzbierać ponad 10,6 mln dolarów.

Jednak już po włamaniu Wyndham nie potrafił zabezpieczyć swej sieci komputerowej. Następnego roku dwa razy padł ofiarą hakerów, utraciwszy informacje o kolejnych 50 tys., a potem 69 tys. kart kredytowych klientów. W roku 2012 FTC pozwała sieć Wyndham, zarzucając jej, że owo niepowodzenie w zabezpieczeniu sieci, było podstępne i nieuczciwe wobec klientów.

Wyndham się odwołał. Twierdził, że FTC niesprawiedliwie karze firmę, która jest ofiarą a nie sprawcą przestępstwa[94]. Nazwał działanie FTC „odpowiednikiem karania lokalnego sklepu z wyposażeniem wnętrz za to, że został okradziony, a dokumenty znajdujące się w sklepie zostały przejęte przez sprawców włamania". FTC odpowiedziała we wniosku o ukaranie, że „już lepsze byłoby porównanie do sklepu z wyposażeniem wnętrz, który pozostawił skopiowane informacje o kartach kredytowych

i debetowych swych klientów na ladzie, nie zamknął drzwi na noc, a następnego dnia był zaskoczony tym, że ktoś wziął sobie te dane".

MOŻECIE WPAŚĆ W PUŁAPKĘ „KORYTARZA LUSTER"

Firmy, które monitorują zachowanie ludzi surfujących w sieci internetowej, twierdzą, że ich działania są nieszkodliwe: chcą one tylko wyświetlać reklamy butów ludziom, którzy ostatnio poszukiwali tego towaru albo też informacje polityczne tym, którzy preferują rozrywkę tego typu. To masowe zjawisko dopasowywania się do potrzeb klienta nazywam „korytarzem luster"[95].

Czasem „korytarz luster" bywa użyteczny. Nie sprzeciwiam się specjalnie oglądaniu reklamy, przypominającej mi o tym, abym kupiła produkt, którego ostatnio poszukiwałam. Jednak w innej przestrzeni zjawisko „korytarza luster" może być bardzo niepokojące.

Zastanówcie się nad takim przypadkiem: jak wynika z badań przeprowadzonych w styczniu 2013 roku przez wykładowczynię Uniwersytetu Harvarda, Latanyię Sweeney[96], gdy wyszukujemy w sieci nazwisko wskazujące na osobę ciemnoskórą (np. „Trevon Jones"), prawdopodobieństwo, że wyszukiwarka zasugeruje przy nim informację dotyczącą jej aresztowania (np. „Trevon Jones aresztowany?"), jest o 25 proc. większe, niż gdy wyszukujemy nazwisko wskazujące na osobę białą (np. „Kristen Sparrow"). Sweeney zaobserwowała, że owa nierównowaga zachodzi także wtedy, gdy osoba o „białym" nazwisku rzeczywiście ma za sobą kryminalną przeszłość, a nazwisko wskazujące osobę ciemnoskórą nie jest związane z jakimkolwiek przestępstwem.

Dane dotyczące sposobu korzystania przez ludzi z sieci internetowej coraz częściej wykorzystywane są do dostarczania klientom treści dopasowywanych do ich potrzeb. Na przykład, Google wykorzystuje informacje o zwyczajach związanych z wyszukiwaniem i pobieraniem plików, by oferować ludziom różne rezultaty wyszukiwania – nawet, gdy wprowadzają do wyszukiwarki te same zapytania. Czasem takie przewidywania mogą okazać się przydatne, na przykład gdy Google sugeruje wam restaurację niedaleko waszego miejsca zamieszkania, zamiast takiej, która znajduje się na drugim krańcu kraju. Innym razem nie jest to

pożądane.

W miesiącach poprzedzających wybory prezydenckie 2012 roku, które odbyły się w listopadzie, Google typował polityczne sympatie w dość kontrowersyjny sposób[97]. Użytkownicy, którzy wyszukiwali Baracka Obamę, mogli ujrzeć newsy o prezydencie w trakcie kolejnych, niezwiązanych z wyborami, wyszukiwań. Tym, którzy chcieli dowiedzieć się czegoś na temat Mitta Romneya, informacje o kandydacie Republikanów nie były jednak wyświetlane na dalszym etapie surfowania.

Przedstawiciele Google'a twierdzili, że ta nierównowaga była efektem działania matematycznej formuły, którą wykorzystywano do przewidywania zapytań. Specjaliści ds. technologii z tej firmy uważali, że ich wysiłki mają nam pomóc zaspokoić nasze potrzeby – nawet jeśli nie wiemy jeszcze, jakie one są. Warto jednak zauważyć, że gdyby w ten sam sposób zachowała się gazeta – na przykład, gdyby informacje o Obamie umieszczone zostały w przeznaczonych dla pewnego rodzaju czytelników artykułach o paście do zębów – bez ogródek nazwano by ją stronniczą i nachalną. Tak samo nazwano by gazetę publikującą wyłącznie reklamy przeznaczone dla homoseksualistów, w wydaniach kierowanych do prenumeratorów, których uznawałaby za gejów, albo też reklamy leków na cukrzycę w wydaniach kierowanych do prenumeratorów, których uznawałaby za cukrzyków.

Czy technologia czyni Google'a odpornym na skutki działań, które nie znalazłyby społecznej akceptacji? Czy też rację ma Martin Abrams, czołowy ekspert ds. prywatności[98], który określa tego typu zachowanie jako ograniczające swobodę „szufladkowanie", w którym „moja wizja tego, co jest możliwe jest ograniczona rozmiarem szufladki", do której jestem przypisany?

MOŻECIE ZOSTAĆ WYKORZYSTANI FINANSOWO

Gdy firmy gromadzą coraz więcej cyfrowych danych o ich potencjalnych klientach, zyskują możliwość wykorzystywania tych informacji do ustalania różnych cen dla różnych użytkowników lub kierowania różnych użytkowników ku różnym ofertom.

Ryan Calo, profesor prawa na Uniwersytecie Waszyngtonu[99], nazywa

to „masową produkcją błędu”, w której firmy wykorzystują dane osobowe, by żerować na ludziach. Firmy na przykład mogą nadwyrężać silną wolę konsumentów, aż ci ostatecznie dadzą się złamać i zdecydują na zakup. Albo też mogą wykorzystywać algorytm, który ustali dla każdej jednostki ceny usług czy produktów w oparciu o wiedzę o tym, co jest dla niej akceptowalne.

Wystawcy kart kredytowych już zaczęli wykorzystywać niektóre z tych metod. W 2010 roku wraz z kolegami z „The Wall Street Journal” odkryłam[100], że firma Capital One oferowała różne karty kredytowe (z różnym oprocentowaniem) różnym odwiedzającym ich stronę internetową. To, jaka karta była prezentowana danej osobie, zależało od jej prawdopodobnych dochodów i lokalizacji. W efekcie, gdy stronę Capital One odwiedzał Thomas Burney, deweloper budowlany z Kolorado, witała go oferta dla ludzi o doskonałej historii kredytowej – karta Capital One Platinum Prestige. Dla odmiany, gdy tę samą stroną odwiedzała Carie Isaac, młoda matka z Colorado Springs, pokazywano jej kartę określaną jako przeznaczoną ludzi z „przeciętną” zdolnością kredytową.

Odpowiadało za to zastosowane oprogramowanie. W 3,748 wierszach kodu programistycznego, który działał na linii komputer Thomasa – strona internetowa Capital One, zawarto przewidywania wystawcy kart kredytowych odnoszące się do jego poziomu dochodów („ponadprzeciętne”), wykształcenia („dyplom ukończenia college’u”) oraz miejsca zamieszkania („Avon”). Capital One ocenił, że poziom dochodów Carrie jest zaledwie „umiarkowany” i że „uczyła się w college’u”. Rzecznik prasowy Capital One powiedział nam, że „jak każdy sprzedawca, zarówno internetowy, jak i działający poza siecią, na podstawie zgromadzonej wiedzy typujemy, czego według nas chcą konsumenci, a oni mogą swobodnie wybierać produkty, którymi są zainteresowani”.

W 2012 roku, gdy ponownie przyglądaliśmy się[101] manipulowaniu danymi, metody te były jeszcze bardziej wyrafinowane i dość rozpowszechnione. Dowiedzieliśmy się, że wystawcy kart kredytowych wciąż oferowali inne karty różnym użytkownikom. Odkryciem było prezentowanie najlepszych ofert na „właśnie tę” kartę klientom, których komputery łączyły się z takich miast jak: Denver, Kansas City czy Dallas, ale już nie ludziom nadającym ze Scranton w stanie Pensylwania, Kingsport w stanie Tennessee czy Los Angeles.

Ustaliliśmy także, że strony internetowe oferowały zróżnicowane ceny,

w zależności od typowanej lokalizacji użytkowników. W testach wyszło nam, że sieć hipermarketów Lowe's[*6] reklamowała lodówkę za 449 dol. użytkownikom z Chicago, Los Angeles i Ashburn w stanie Wirginia. Użytkownikom z siedmiu innych miast tę samą lodówkę oferowała jednak za 499 dolarów. Na tej samej zasadzie, na stronie internetowej Home Depot, szpulę z siedemdziesięcioześciometrowym kablem elektrycznym wyświetlano w sześciu różnych cenach, w zależności od tego, z jakiego miejsca łączył się ze stroną komputer klienta – i tak, kosztowała ona 70,80 dol. w Ashtabula w stanie Ohio, 72,45 dol. w Erie w stanie Pensylwania, 75,98 dol. w Oleanie w stanie Nowy Jork oraz 77,87 dol. w Monticello w stanie Nowy Jork. Obie sieci, Lowe's oraz Home Depot, utrzymywały, że różnice w cenach wynikały z chęci dopasowania oferty internetowej do oferty najbliższego sklepu w ich okolicy.

Ustaliliśmy, że najbardziej kompleksowo dywersyfikuje ceny sklep internetowy Staples, giganta wśród sieci sklepów z materiałami biurowymi. Zdawało się, że wykorzystuje on dane o klientach do typowania ich miejsca zamieszkania, a następnie wyświetla różne ceny dla różnych użytkowników, w oparciu o oszacowanie ich lokalizacji. Efekt końcowy: gdy Trude Frizzell logowała się na Staples.com z jej komputera w pracy w miejscowości Bergheim w Teksasie, mogła zobaczyć zszywacz biurowy za 14,29 dolarów. Zaledwie kilka kilometrów dalej, w miejscowości Bourne, ten sam zszywacz był oferowany Kim Wamble za 15,79 dolarów. Różnica nie wynikała ze zróżnicowanych kosztów dostawy, które są przecież naliczane już po dokonaniu zakupu. Wyglądało to raczej, jakby ceny odzwierciedlały odległość, jaka – w przekonaniu Staples – dzieliła klienta od najbliższego sklepu konkurencji. Sieć potwierdziła, że różnicuje ceny uwzględniając przy tym kilka czynników, nie chciała jednak ujawnić szczegółów.

Prawo nie zabrania oferowania innych cen różnym grupom klientów, pod warunkiem, że nie ma to związku z ich rasą czy innymi cechami, które mogą stać się podstawą stygmatyzacji klienta. Zróżnicowana oferta cenowa skierowana do grup użytkowników może jednak skutkować niezamierzoną niesprawiedliwością. Nasze doświadczenia przeprowadzone na stronie internetowej Staples wykazały, że do mieszkańców obszarów, w których odnotowywano większy przeciętny poziom dochodu, oferty z promocyjnymi cenami kierowane były z większym prawdopodobieństwem, niż do mieszkańców obszarów, na których

notowano niższe przeciętne dochody. „Myślę, że to właśnie jest dyskryminacja”, uznała Kim.

W najgorszy sposób wykorzystuje się finansowo ludzi biednych, starszych oraz niewykształconych. Pomyślcie o tzw. listach frajerów[102] [ang. *sucker lists*], które handlujący bazami budują z uwzględnieniem ludzi starych, borykających się z problemami finansowymi lub podatnych na pewnego rodzaju oferty sprzedażowe. Listy frajerów często sprzedawane są pozbawionym skrupułów handlowcom, którzy wciskają im podejrzane produkty.

W październiku 2012 roku FTC ukarała[103] jednego z największych brokerów danych, firmę Equifax oraz jej klientów, każąc jej zapłacić 1,6 mln dolarów za naruszenie przepisów o ochronie danych osobowych poprzez sprzedaż nieuczciwym handlowcom list zawierających dane ludzi, którzy opóźniali się z zapłatą rat kredytów hipotecznych. Listy były reklamowane hasłami[104] takimi jak: „Uratuj mnie przed zajęciem obciążonej nieruchomości” oraz „Ubolewający z powodu długu”. Jednym z nabywców była szczególnie podejrzana firma Southern California, stosująca wyrafinowane, nachalne praktyki sprzedażowe[105], która od 1,5 tys. właścicieli domów wyciągnęła ok. 2,3 mln dolarów. Jak się okazało, za rzekome zmiany w zapisach umów kredytowych, do których nigdy nie doszło, płacili oni prowizje w wysokości od 1 tys. do 5 tys. dolarów. Wielu z tych ludzi ostatecznie zresztą straciło swe domy.

Gdy pytam przedstawicielkę władz Stowarzyszenia Marketingu Bezpośredniego (Direct Marketing Association)[106], czy istnieją jakieś listy potencjalnych klientów, z których jego członkowie nie chcieliby zrobić użytku, takie jak „seniorzy z chorobą Alzheimera lubiący zakłady pieniężne”, odsyła mnie ona do katalogu zasad etycznych, które zabraniają sprzedaży na podstawie list, do których przynależność mogłaby dyskredytować klienta. Wszystko inne zdaje się być uczciwe.

MOŻECIE BYĆ PODDANI OKAZANIU POLICYJNEMU

5 kwietnia 2011 roku John Gass z Needham, w stanie Massachusetts, odebrał list i ku swemu zaskoczeniu ustalił, że rozpoczyna się on

od informacji, że właśnie zabrano mu prawo jazdy[107]. „Byłem niemile zaskoczony", mówił John.

John jest pracownikiem miejskim – naprawia kotły grzewczy w Needham. Bez prawa jazdy nie mógłby wykonywać swojej pracy. Zadzwonił więc do urzędu – Massachusetts Registry of Motor Vehicles (RMV) – i usłyszał, że ma się stawić na przesłuchaniu wraz z dowodem tożsamości. Nie chciano mu powiedzieć, na jakiej podstawie zabrano mu prawo jazdy.

Gdy John stawił się na przesłuchaniu, dowiedział się, że urząd zaczął stosować oprogramowanie do rozpoznawania twarzy, by lepiej wykrywać przypadki kradzieży tożsamości. Wykorzystując zdjęcie z dokumentu, oprogramowanie identyfikowało zgłoszenia ludzi, którzy ubiegali się o wiele praw jazdy jednocześnie, pod różnymi nazwiskami. System oznaczył prawa jazdy Johna i jeszcze jednego mężczyzny, Edwarda Perry'ego z miejscowości Rehoboth w tym samym stanie, jako posiadające podobne zdjęcia. Zażądano więc, by potwierdzili swoje tożsamości.

Proceder, którego ofiarą stał się John, nazywam „policyjnym okazaniem". Umożliwiają go wielkie policyjne dragnety, które pozwalają funkcjonariuszom traktować każdego jak podejrzanego. Wywraca on do góry nogami obowiązującą w naszym systemie prawnym zasadę, że człowiek jest „niewinny, dopóki nie udowodni mu się winy".

Najbardziej widocznym tego przykładem są skanery na lotniskach. Za ich pomocą prowadzi się wyjątkowo inwazyjne przeszukania – pozwalają one bowiem nawet przyjrzeć się temu, co znajduje się pod ubraniem danej osoby. I to w sytuacji, gdy nie pojawia się cień podejrzenia, że prześwietlana osoba jest przestępcą. W istocie, ciężar spoczywa w tym przypadku na jednostce, która podlega procedurze prześwietlenia. To ona ma „udowodnić" swoją niewinność, przechodząc przez skaner, uniknąwszy wyświetlenia przez urządzenie jakichkolwiek podejrzanych przedmiotów. Te dragnety są jak z Kafki. Pomyślcie bowiem o liście osób posiadających zakaz latania. Ci, którzy na nią trafiają, nie są informowani o tym, dlaczego tak się stało. Nie mogą też zaskarżyć decyzji o umieszczeniu ich na niej.

John Gass na szczęście miał szansę się bronić[108]. Była to jednak zupełnie absurdalna sprawa. Przedstawiono mu zdjęcie jego samego sprzed trzynastu lat.

– Człowiek na zdjęciu wcale pana nie przypomina – powiedział oficer.

– Oczywiście, że nie. Minęło trzynaście lat odkąd zostało wykonane. Byłem o 45 kg lżejszy – odparł John.

John przedstawił swój paszport oraz akt urodzenia, i na tej podstawie przywrócono mu prawo jazdy. Funkcjonariusz nie dał mu jednak żadnego pisemnego potwierdzenia na to, że ważność prawa jazdy została przywrócona. John domagał się tego, bo chciał okazać takie pismo szefowi, pragnąć udowodnić mu, że może prowadzić auto. „To było jak zły sen", wspominał John.

Wściekły, że tak go potraktowano oraz że tego dnia pozbawiono go zarobku, John zdecydował się pozwać urząd. Argumentował, że pozbawiono go konstytucyjnego prawa do rzetelnego procesu. Urząd twierdził natomiast, że dano mu możliwość zaskarżenia decyzji o cofnięciu prawa jazdy, ponieważ 24 marca wysłano do niego list w tej sprawie, a do 1 kwietnia prawo jazdy wciąż zachowywało ważność. John odebrał list dopiero 5 kwietnia.

Sąd okręgowy hrabstwa Suffolk uznał wniosek urzędu o oddalenie powództwa. Gass się odwołał, ale sąd apelacyjny także orzekł wbrew jego woli. „Choć wzburzenie Gassa związane z tym, że musiał bronić swej tożsamości jest zrozumiałe, nie oznacza to, że jego sprawa rodzi szersze prawne wątpliwości, które musiałyby zostać rozstrzygnięte przez apelację", stwierdził sąd[109].

John poczuł się zdradzony. Stara się omijać łukiem policję stanową, w obawie, że nie będzie traktowany sprawiedliwie. „Nie ma mechanizmów kontroli i równowagi[110]", mówił. „To jasne, że ludzie będą popełniać błędy. Ale w tym przypadku nie istnieje żaden nadzór".

„Naprawdę wydaje mi się, że sprzedajemy naszą wolność w zamian za bezpieczeństwo", powiedział John.

* * *

Te historie odzwierciedlają prostą prawdę: informacja to władza. Każdy kto dysponuje wielkimi ilościami danych o nas, ma nad nami przewagę.

Z początku, era informacyjna miała wzmocnić jednostki, dając im dostęp do informacji wcześniej niedostępnych. Mogliśmy na całym świecie porównywać ceny, poszukiwać najlepszego fragmentu wiedzy, czy ludzi, którzy podzielali nasze poglądy.

Obecnie dochodzi do zmiany układu sił i szala przechyla się ku wielkim

instytucjom: zarówno rządom jak i korporacjom. To one zyskują przewagę w wojnach informacyjnych, dzięki zdolności do śledzenia potężnej ilości danych związanych z najbardziej przyziemnymi aspektami naszego życia.

Dowiadujemy się, że ludzie, którzy dysponują informacjami o nas, mogą nas zawstydzić, wyczyścić nasze portfele lub oskarżyć o przestępcze zachowanie. Ta wiedza może wykreować kulturę strachu.

Pomyślcie o Sharon i Bilalu. Gdy dowiedzieli się, że byli obserwowani na portalu PatientsLikeMe, wycofali się z internetu.

Bilal usunął swoje posty z forum. Ściągnął ze strony swoją kartę dawkowania leków i teraz przechowuje ją w pliku excela na swoim komputerze. Także Sharon przestała korzystać z internetu. Nie pozwala bawić się na nim swemu synowi, gdy nie jest pod nadzorem.

Zaczęli rozmawiać ze sobą przez telefon, jednak stracili kontakt internetowy, który udało im się rozwinąć, gdy byli członkami PatientsLikeMe. „Nie znalazłam dotąd zastępstwa", mówi Sharon. Bilal dodaje: „Tylko ludzie z PLM wiedzą, jak to jest".

Żadne z nich nie jest jednak w stanie zaryzykować bycia nadzorowanym. Sharon twierdzi, że nie mogłaby żyć ze świadomością, iż „każde naciśnięcie klawisza może być zaraportowane do jakiejś innej firmy". Bilal dodaje: „Czuję po prostu, że nadużyto naszego zaufania".

Doświadczenia Sharon i Bilala uświadamiają nam, że z całą swoją technologiczną pirotechniką, era cyfrowa dotyczy jednak człowieka. Technologia pozwala nam znajdować ludzi, którzy podzielają nasze poglądy i zyskać świadomość, że nie jesteśmy osamotnieni. Zarazem jednak technologia umożliwia innym śledzenie nas, i sprawia, że wycofujemy się z cyfrowej intymności.

Gdy ludzie pytają mnie, dlaczego tak bardzo interesuję się kwestią prywatności, zawsze odwołuję się do prostego pragnienia, by na świecie istniały bezpieczne przestrzenie dla Sharon i Bilala, dla mnie, dla moich dzieci, dla wszystkich. Chciałabym, aby w cyfrowym świecie istniała przestrzeń na listy z pieczęcią lakową. Czy naprawdę musimy być skazani na pisanie pocztówek – ze świadomością, że mogą one, i będą, czytane po drodze przez przypadkowe osoby?

Czy chcemy żyć w świecie, w którym zawsze narażeni będziemy na ryzyko bycia zhakowanymi? W świecie, w którym będzie można nas zlokalizować? W którym nie będziemy mogli mieć swoich tajemnic? W którym będziemy podglądani nawet w naszych domach, w którym będzie można się pod nas podszyć, i w którym będziemy żyć w pułapce

„korytarza luster”? W którym będziemy wykorzystywani finansowo i bez powodu będziemy trafiać przed oblicze funkcjonariuszy policji? Moja książka to próba odpowiedzi na te pytania. Robię to w dwóch częściach.

W pierwszych rozdziałach odkrywam, dlaczego masowy nadzór ma tak wielkie znaczenie. W tym celu badam prawne i technologiczne korzenie naszego społeczeństwa nadzorowanego, a także nadużycia związane z nadzorem i wpływ tego zjawiska na życie jednostki i społeczeństwa.

W kolejnych rozdziałach sprawdzam, czy istnieje jeszcze nadzieja na zbudowanie alternatywnego świata, w którym moglibyśmy czerpać z owoców rozwoju technologii, bez obaw o ryzyko bycia obiektem cyfrowego ataku. Testuję różne strategie omijania dragnetów, od częstego zmieniania telefonów na kartę po ustanawianie fałszywych tożsamości.

Mam nadzieję, że moje odkrycia pomogą rozwijać się debacie o prywatności – wyjść poza kwestie związane z prostą obawą o to „kto mnie obserwuje”, ku bardziej szczegółowym rozważaniom nad tym „dlaczego ma to tak duże znaczenie” oraz, ostatecznie, ku produktywnej dyskusji o tym, co możemy zrobić.

2

KRÓTKA HISTORIA ŚLEDZENIA

Siedem tygodni po atakach terrorystycznych[1], w których zabito tysiące ludzi i zniszczono World Trade Center, jeden z najlepszych w naszym kraju łamaczy kodów po raz ostatni opuścił biuro największej amerykańskiej agencji wywiadowczej.

Był 31 października 2001 roku. Ogień wciąż tlił się na Dolnym Manhattanie[2]. Do członków Kongresu i redakcji w całym kraju trafiały listy z wąglikiem[3]. Codziennie donoszono o nowych pogróżkach. Straszono zamachami bombowymi. Roztrzęsione społeczeństwo było w stanie wojny z niewidzialnym wrogiem.

Jednak Bill Binney[4], łamacz kodów z Agencji Bezpieczeństwa Krajowego (National Security Agency, NSA), odpowiadający rangą generałowi wojska, nie przyłączył się do walki. Po ponad trzydziestu latach pracy w agencji, przeszedł na emeryturę. Gdy opuścił schody prowadzące do kwatery głównej agencji w Fort Meade w stanie Maryland, powiedział: „Jestem wreszcie wolny. Wreszcie wolny”[5].

Binney całe lata poświęcił na próby zmodernizowania technik nadzoru stosowanych przez agencję wywiadowczą. Chciał, by pozwalały one obserwować komunikację prowadzoną w internecie z nadawcami z całego świata, a zarazem respektowały prawo obywateli USA do prywatności korespondencji. Jego wysiłki za każdym razem były jednak udaremniane.

Koledzy mówili mu, że obecnie agencja gromadzi informacje z korespondencji internetowej Amerykanów, praktycznie ich nie filtrując. Nie chciał uczestniczyć w tym procederze.

Opuszczając grodzony teren Fort Meade, Binney uciekał z miejsca, które postrzegał jako miejsce zbrodni. „Nie mogłem zostać tam dłużej, odkąd

NSA w sposób zamierzony zaczęło naruszać Konstytucję”[6], powiedział później, zeznając przed sądem przeciwko byłemu pracodawcy.

W międzyczasie oczywiście dowiedzieliśmy się, że Binney miał rację. Po atakach terrorystycznych 11 września 2001 roku, amerykański rząd zapoczątkował procedurę tzw. przemiatania [ang. *sweeping*], ustanawiając prawdopodobnie nielegalne dragnety, które przejmowały treść połączeń telefonicznych i korespondencji e-mail praktycznie wszystkich Amerykanów.

* * *

W podejmowanych przeze mnie próbach zrozumienia historii i korzeni masowego nadzoru, wciąż wracam do roku 2001 roku. Był to nie tylko rok niszczącego ataku terrorystycznego na USA, lecz również czas, w którym branżą technologiczną wstrząsnęło pęknięcie bańki spekulacyjnej[7] – tzw. bańki dot.comów. Te dwa, z pozoru niewiążące się ze sobą, wydarzenia zapoczątkowały cały łańcuch zjawisk, które położyły podwaliny pod współczesne dragnety. Ataki terrorystyczne dały do zrozumienia amerykańskiemu rządowi, że tradycyjne techniki pozyskiwania informacji wywiadowczych już nie działają. Z kolei ludziom z Doliny Krzemowej krach giełdowy uświadomił, że muszą poszukiwać nowych sposobów na zarabianie pieniędzy.

Jedni i drudzy znaleźli tę samą odpowiedź na trapiące ich, tak przecież różne, problemy. Było nią gromadzenie i analizowanie potężnych ilości danych osobowych. Oczywiście, robili to dla zupełnie innych celów. Rządowi chodziło o poszukiwanie i typowanie terrorystów, którzy mogą ukrywać się wśród zwykłych obywateli. Branży nowych technologii chodziło o to, by zwabić reklamodawców na solidnie opracowane akta osobowe. W sposób nieunikniony cele te zaczęły być zbieżne, gdy rząd Stanów Zjednoczonych postanowił wykorzystać swą władzę do tego, by zanurzyć się w profile, którymi dysponowała branża technologiczna.

To rząd i branża technologiczna, wspólnie, zgotowały nam społeczeństwo nadzorowane. Niniejsza historia opowiada o tym, jak to się wszystko zaczęło.

* * *

W XVIII wieku Brytyjczycy zmagali się z problemami z kontrolą nad swymi amerykańskimi koloniami. Amerykanie buntowali się przeciwko brytyjskim próbom blokowania handlu między koloniami i innymi krajami Europy, a także przeciwko opodatkowaniu na rzecz Brytyjczyków, które nie dawało prawa do posiadania reprezentantów w parlamencie.

By walczyć z plagą przemytu[8], Brytyjczycy wdrożyli nowy typ nadzoru: generalny nakaz rewizji, zwany jako ryt *assistance* [ang. *writ of assistance*], który pozwalał brytyjskim oficerom prowadzić przeszukania domów oraz dokonywać konfiskat praktycznie bez nadzoru sądowego. Amerykanie byli źli, że Brytyjczycy mogą wpaść do każdego domu o dowolnej godzinie, nawet podczas wesela czy pogrzebu. „Mam wrażenie, że to najgorsze z narzędzi arbitralnej władzy", przekonywał prawnik James Otis Jr. w swej słynnej mowie przed sądem w Bostonie w 1761 roku[9].

Wściekłość wobec generalnych nakazów rewizji[10] przyspieszyła rewolucję amerykańską. Doprowadziła do ustanowienia Czwartej Poprawki do Konstytucji Stanów Zjednoczonych, która brzmi: „Prawa ludu do nietykalności osobistej, mieszkania, dokumentów i mienia nie wolno naruszać poprzez nieuzasadnione rewizje i zatrzymanie; nakaz w tym przedmiocie można wystawić tylko wówczas, gdy zachodzi wiarygodna przyczyna potwierdzona przysięgą lub zastępującym ją oświadczeniem. Miejsce podlegające rewizji oraz osoby i rzeczy podlegające zatrzymaniu powinny być w nakazie szczegółowo określone".

Czwarta Poprawka ma kluczowe znaczenie dla pracy funkcjonariuszy organów ochrony porządku publicznego w USA. Jednak technologia umożliwiła wykorzystanie luk prawnych w interpretacji Czwartej Poprawki. Te najważniejsze dotyczą:

- **Przestrzeni publicznej.** Czwarta poprawka chroni tylko „osoby, mieszkania, dokumenty i mienie. Tak zinterpretował to Sąd Najwyższy[11], co oznacza, iż nieuzasadnione jest żądanie ochrony prywatności przez jednostki znajdujące się w przestrzeni publicznej. Technologia ograniczyła zakres podlegający ochronie – umożliwiając nadzór nad komputerami, z których korzystamy w domu i oblatywanie naszych ogródków przez drony.
- **Doktryny strony trzeciej.** Sąd Najwyższy usankcjonował tzw. doktrynę strony trzeciej[12] [ang. *third-party doctrine*], która mówi

o tym, iż jednostki nie powinny oczekiwać ochrony poufności informacji, którą dzielą się z osobami trzecimi – na przykład bankami czy operatorami telekomunikacyjnymi. W efekcie, nawet dane wrażliwe[13] przechowywane przez tzw. stronę trzecią, takie jak e-maile, mogą zostać pozyskane bez stosownego nakazu.

- **Metadanych.** Metadane to dane na temat danych[14] – na przykład koperta zawierająca list może być uważana za element metadanych. W tym przypadku treść listu oznacza dane. Sądy tradycyjnie przyznają mniejszą ochronę metadanym niż samym danym. Na przykład urząd pocztowy może wykonać fotografię koperty waszego listu bez stosownego nakazu, nie może jednak bez niego otworzyć koperty. W erze cyfrowej metadane[15] mogą jednak ujawniać bardzo wiele – to na przykład wszystkie numery telefonów, z którymi się kontaktowaliście, adresy e-mail ludzi, z którymi prowadziliście korespondencję, oraz dane o waszej lokalizacji.
- **Przeszukań na granicach.** Sądy w swych orzeczeniach usankcjonowały ów wyjątek od Czwartej Poprawki, jaki stanowi przeszukanie na granicy[16]. Pozwala to rządowi prowadzić przeszukania na granicach bez konieczności uzyskiwania nakazu. W erze elektronicznej oznacza to, że agenci celni mogą – i często tak robią – pobrać całą zawartość telefonu lub komputera jednostki na granicy. Amerykańskie służby celne twierdzą, że przeprowadzają około piętnastu przeszukań sprzętu elektronicznego dziennie. W marcu 2013 roku Sąd Apelacyjny USA dla Dziewiątego Okręgu w Kalifornii ustanowił nowe ograniczenia dotyczące przeszukań sprzętu elektronicznego na granicach, orzekając w sprawie Stany Zjednoczone kontra Cotterman. Sąd uznał, że do policyjnego przeszukania, z użyciem oprogramowania do analizy zaszyfrowanych lub usuniętych z danego urządzenia danych, powinno być wymagane co najmniej uzasadnione podejrzenie prowadzenia działalności przestępczej przez przeszukiwanego. Tego typu czynność różni się bowiem od bardziej ogólnej kontroli, polegającej na przejrzeniu dokumentów, zdjęć czy innych plików.

W erze cyfrowej owe luki prawne stały się wystarczająco duże, by umożliwić prowadzenie nieuzasadnionych rewizji, podobnych do tych,

które wzbudziły gniew amerykańskich Ojców Założycieli.

* * *

Amerykańscy prezydenci byli bardzo ostrożni w przekraczaniu granic wytyczonych przez Czwartą Poprawkę. W roku 1981, gdy prezydent Ronald Reagan usankcjonował funkcjonowanie krajowego szpiegostwa[17] w poszukiwaniu sowieckich agentów, nakazał organizacjom wywiadowczym, by „na terenie Stanów Zjednoczonych lub wobec Amerykanów przebywających za granicą" korzystały z „najmniej inwazyjnych metod pozyskiwania informacji". Przez całe lata nakaz Reagana interpretowano w sposób następujący: działania szpiegowskie wewnątrz kraju powinny być prowadzone ostrożnie i tylko w uzasadnionych przypadkach.

Jednak po 11 września 2001 roku, zniesiono wymóg istnienia jakichkolwiek podejrzeń wobec osoby inwigilowanej przed podjęciem jakichkolwiek działań o charakterze wywiadowczym, niezależnie od intencji i celu tych działań. Dokumenty, które ujawnił współpracownik NSA Edward Snowden[18], odmalowują dramatyczny obraz tego, jak jedna decyzja podjęta tuż po atakach, odtworzyła tamę stanowiącą zabezpieczenie dla działalności potężnych krajowych dragnetów. Według szkicu raportu Inspektora Generalnego z 2009 roku, który przeciekł do wiadomości publicznej, NSA rozpoczęła szpiegowanie swych obywateli 14 września 2001 roku, w trzy dni po atakach, gdy dyrektor agencji, Michael Hayden, zatwierdził procedurę przechwytywania wszystkich amerykańskich połączeń telefonicznych kierowanych na numery (lub połączenia przychodzące od tych numerów) zidentyfikowane jako należące do terrorystów znajdujących się w Afganistanie bez zgody sądu. 26 września Hayden rozszerzył swój rozkaz o wszelkie możliwe połączenia z numerami z Afganistanu.

Wkrótce jednak Hayden zapragnął jeszcze większej ilości danych. Wierzył, że istnieje jakaś „międzynarodowa luka", czyli obszar danych znajdujący się pomiędzy zasięgiem działań NSA, poszukującej informacji zagranicą, a zasięgiem Federalnego Biura Śledczego (Federal Bureau of Investigation, FBI), które monitoruje sytuację w kraju. Nikt bowiem nie obserwował komunikacji przychodzącej do USA, inicjowanej zagranicą. Hayden zaczął więc pracować nad tym z wiceprezydentem Stanów

Zjednoczonych Dickiem Cheneyem. Ten poprosił swego radcę prawnego, by pomógł mu napisać notatkę służbową, która umożliwiłaby NSA wypełnić ową międzynarodową lukę. 4 października 2001 roku prezydent George W. Bush wydał memorandum zatytułowane „Authorization for specified electronic surveillance activities during a limited period to detect and prevent acts of terrorism within the United States". Memorandum pozwalało Haydenowi kontynuować namierzanie komunikacji pomiędzy Afganistanem i Stanami Zjednoczonymi bez konieczności uzyskania zgody Sądu Nadzoru Wywiadu Stanów Zjednoczonych (Foreign Intelligence Surveillance Court), który zwykle sprawuje kontrolę nad przypadkami elektronicznego nadzoru mieszkańców Stanów Zjednoczonych. Prezydent wydał zgodę na realizowanie programu przez trzydzieści dni.

W tamtych dniach zdawało się to być zrozumiałym środkiem przeciwdziałania rozwojowi kryzysu. W czasach, gdy terroryści mogli już maskować swoje ruchy w internecie, wykorzystując do komunikowania się serwery z różnych części świata, wyodrębnianie komunikacji amerykańskiej i międzynarodowej nastręczało problemów. Rozkaz pozwolił NSA chwilowo od tego odetchnąć – przynajmniej na czas kryzysu.

Jednak ostatecznie ten bardzo wąsko zakreślony przez Haydena, krótkoterminowy, program rozrósł się do szeroko zakrojonego szpiegostwa na terenie kraju. Obowiązujący początkowo przez miesiąc rozkaz był permanentnie odnawiany, a zasięg działań coraz bardziej rozszerzany. Po roku wykraczał już poza akty komunikacji pomiędzy USA i Afganistanem. NSA posługiwało się prezydenckim rozkazem, aby usprawiedliwić przechwytywanie e-maili i połączeń telefonicznych tysięcy celów naraz. Zaczęto także pozyskiwać hurtowe ilości danych o połączeniach zamiejscowych i międzynarodowych, by móc prowadzić poszukiwania metodą łańcuchową [ang. *chaining*] – polegającą na znajdowaniu osoby, która dzwoniła do innej osoby, która z kolei kontaktowała się z kimś podejrzanym o działalność terrorystyczną. Do tego jeszcze NSA zaczęła zbierać dane dotyczące ruchu w internecie (do kogo mailowaliście, jakie strony internetowe przeglądaliście) pochodzącego z tych źródeł, które „większość komunikacji prowadziły z zagranicznymi źródłami" i stwarzały „znaczne prawdopodobieństwo" przechwycenia działalności internetowej terrorystów.

By móc gromadzić wszystkie te dane, NSA zaczęło zabiegać o współpracę z dostawcami internetu i spółek telekomunikacyjnych. Jak

czytamy w raporcie, NSA dotarła do siedmiu firm (których nazw nie ujawniono). Trzy z nich odmówiły współpracy.

W 2005 roku dziennik „The New York Times" ujawnił[19] fakt istnienia programu polegającego na bezprawnym zbieraniu danych o połączeniach obywateli, opisując go jako istotną zmianę w praktyce wywiadowczej. Szeroki zasięg programu wyszedł na jaw[20] kilka miesięcy później, gdy emerytowany pracownik techniczny firmy AT&T, Mark Klein, podał do wiadomości publicznej, że NSA zainstalowała w tajnym pokoju biura AT&T w San Francisco narzędzia, które pozwalały przechwytywać całą komunikację przechodzącą przez tę część sieci. „To infrastruktura rodem z Orwellowskiego państwa policyjnego. Należy ją unieszkodliwić"[21], oświadczył Klein.

Następnie, w maju 2006 roku, dziennik „USA Today" poinformował w jednym z artykułów[22], że firmy AT&T, Verizon oraz BellSouth zaczęły dostarczać NSA danych dotyczących połączeń telefonicznych swych klientów tuż po atakach 11 września. „To największa baza danych, jaką zbudowano na świecie", ujawniał w artykule pragnący zachować anonimowość urzędnik.

Wobec presji ze strony społeczeństwa, prezydent Bush, na krótko zamknął pewne części programu[23]. Jednak w 2008 roku podpisał nowelizację Ustawy o nadzorze wywiadu [Foreign Intelligence Surveillance Act, FISA], która go przywracała i legalizowała, a także chroniła dostawców usług telekomunikacyjnych przed odpowiedzialnością za naruszenia tajemnicy korespondencji ich klientów, których się dopuściły, uczestnicząc we wcześniejszym, prawdopodobnie nielegalnym, procederze.

Poprawki do ustawy FISA ustanawiały nową grupę nakazów rewizji, które pozwalały rządowi przechwytywanie treści komunikacji bez konieczności uzyskania choćby nazwiska osoby będącej celem. Oznaczały więc kontynuację szerokiego przemiatania, które prowadzono już wcześniej w ramach bezprawnego programu zbierania danych o połączeniach telefonicznych. Tym razem jednak algorytm, który miał być stosowany wobec podejrzanego celu, wymagał zgody sądu. Program zwany PRISM[24], ujawniony później przez Snowdena, opisywał spółki internetowe, które stosowały się do nakazów algorytmicznych rewizji. Okazuje się, że w trakcie niejawnej rozprawy sądowej portal Yahoo! podjął walkę o uznanie jednego z takich nakazów za niekonstytucyjny[25], jednak

przegrał i został zmuszony do stosowania się do niego pod rygorem stwierdzenia niewykonania postanowienia sądu.

Co zdumiewające, bezprawne zbieranie danych o połączeniach telefonicznych okazało się jednym z tych programów NSA, które miały bardziej ograniczony zasięg, jako że w jego ramach przechwytywano wyłącznie informacje o komunikacji wychodzącej z USA do podmiotów zagranicznych. Znacznie głębszą inwigilację stanowiły te działania NSA, które nakierowane były na zbieranie wielkich ilości danych o połączeniach telefonicznych i ruchu internetowym w samych Stanach Zjednoczonych[26]. Agencja twierdziła, iż ponieważ owo przemiatanie danych dotyczących krajowych połączeń telefonicznych i ruchu internetowego dotyczyło w istocie „metadanych", działania te nie naruszały prawa do prywatności Amerykanów.

Snowden ujawnił tajny nakaz sądowy[27], który zobowiązywał firmę Verizon do codziennego przekazywania NSA danych dotyczących połączeń telefonicznych. Wkrótce potem senator z Kalifornii, Dianne Feinstein, potwierdziła[28], że przez siedem lat NSA zbierała dane o krajowych i międzynarodowych połączeniach telefonicznych od największych spółek telekomunikacyjnych.

Snowden ujawnił także notatkę z 2007 roku autorstwa Kennetha Wainsteina, prawnika z Departamentu Sprawiedliwości, który domagał się, by NSA otrzymało uprawnienia do gromadzenia jeszcze większej ilości danych o ruchu internetowym na terenie USA[29]. „Z wykorzystaniem algorytmów komputerowych NSA tworzy łańcuch kontaktów, prowadzących do komunikujących się z sobą podmiotów", pisał Wainstein. „Obecna praktyka nakazuje NSA zaprzestać działań, gdy w łańcuchu pojawia się numer telefonu lub adres należący do obywatela USA". Następnie wnioskował do prokuratora generalnego o zgodę na „budowanie łańcuchów kontaktów" rezydentów Stanów Zjednoczonych.

Wydaje się, że jego życzenie szybko się spełniło. Administracja Obamy przyznała, że program śledzenia ruchu w internecie zakończył się w 2011 roku i nie został wznowiony[30]. Istnieje jednak prawdopodobieństwo, że NSA wciąż śledzi krajowy ruch internetowy, pod innym pretekstem.

Niezależnie od tego, sensacyjne informacje, które ujawnił Snowden, potwierdziły to, czego wielu przez długi czas się domyślało: wąski, obliczony na funkcjonowanie przez miesiąc dragnet, obejmujący

komunikację pomiędzy Stanami Zjednoczonymi a Afganistanem, rozrósł się w potężny dragnet krajowy.

* * *

Po 11 września 2001 roku, olbrzymie, uruchamiane pospiesznie kwoty mające służyć przeciwdziałaniu terroryzmowi[31], napędzały powstawanie służących inwigilacji dragnetów, zarówno na poziomie krajowym jak i lokalnym. Budżety federalnej agencji wywiadowczej rosły z ok. 27 mld dolarów tuż przed atakami do 75 mld dolarów w 2013 roku. Część tych środków płynęła do poszczególnych stanów w postaci grantów.

Zastanówcie się nad działaniami Departamentu Bezpieczeństwa Krajowego (Department of Homeland Security, DHS). Począwszy od 11 września 2001 roku resort ten rozdzielił[32] ponad 7 mld dolarów w postaci grantów na ochronę i walkę z terroryzmem[33] na obszarach charakteryzujących się „wysokim stopniem zagrożenia i dużą gęstością zaludnienia". Granty o wartości ponad 50 mln dolarów od DHS[34] zostały rozdzielone między lokalne organy ścigania, w celu dofinansowania zakupu zautomatyzowanych czytników tablic rejestracyjnych pojazdów. Dzięki nim, w skali dotąd niespotykanej, służby te mogły kontrolować przemieszczanie się obywateli. Departement dofinansował[35] również „centra fuzyjne", tworzone niemal w każdym stanie, które miały za zadanie przetwarzanie danych pochodzących z różnych instytucji – a często także od podmiotów pośredniczących w handlu danymi – w poszukiwaniu sygnałów, które mogłyby pomóc zapobiec przyszłym aktom terroryzmu. Lokalna policja zaczęła coraz częściej śledzić ludzi[36], wykorzystując do tego sygnały wysyłane przez ich telefony komórkowe.

Jednocześnie coraz powszechniejsze stało się prowadzenie śledztw bez uzasadnionego podejrzenia przestępstwa. W 2008 roku prokurator generalny wprowadził nowe wytyczne[37], które pozwoliły Federalnemu Biuru Śledczemu (Federal Bureau of Investigation, FBI), wszczynać postępowania bez podania „konkretnej, mającej odzwierciedlenie w ustaleniach faktycznych, kwalifikacji prawnej czynu", którego miał dopuścić się obiekt obserwacji. Nowe przepisy pozwalały FBI „otrzymywać informacje o jednostkach, grupach i organizacjach, które mogą być przedmiotem zainteresowania śledczych, zarówno dlatego,

że mogą być zaangażowane w działalność o charakterze przestępczym lub zagrażającą bezpieczeństwu narodowemu, jak i dlatego, że mogą one być celem ataku bądź ofiarami działań o takim charakterze".

Natomiast w roku 2012 Departament Sprawiedliwości upoważnił[38] Krajowe Centrum ds. Antyterroryzmu (National Counterterrorism Center) do wykonania kopii wszystkich rządowych baz danych zawierających informacje o obywatelach USA – danych dotyczących lotów samolotowych, list pracowników kasyn, nazwisk Amerykanów goszczących studentów przebywających na wymianie językowej – i przetwarzania ich w celu wykrycia podejrzanych zachowań.

Wcześniej agencji nie wolno było przechowywać informacji o rezydentach amerykańskich, chyba, że byli oni podejrzani o działalność terrorystyczną lub mieli związek z prowadzonym postępowaniem.

Dragnety ustanawiane w warunkach braku uzasadnionego podejrzenia popełnienia przestępstwa stały się nową normą.

* * *

Ataki terrorystyczne z 2001 roku zapoczątkowały także erę dragnetów w Dolinie Krzemowej.

Jeszcze do późnych lat 90. branża oprogramowania, oferująca produkty klientom indywidualnym, zaliczana była do handlu detalicznego. Programy komputerowe sprzedawane było w zawiniętych w folię pudełkach, ustawianych na półkach sklepowych. Oczywiście, przedsiębiorstwa kupowały także hurtowo oprogramowanie dla jednostek przemysłowych. Jednak rynek popularny – do którego należały głównie gry i narzędzia do pracy biurowej – był rynkiem detalicznym.

Internet dosłownie wysadził w powietrze biznes programów komputerowych. Pierwszym prawdziwym elementem oprogramowania internetowego była przeglądarka stron www o nazwie Netscape Navigator, wprowadzona w 1994 roku. Prospekt emisyjny prezentujący pierwszą oferowaną dla masowego rynku przeglądarkę sprawił, że w tzw. pierwszej ofercie publicznej Netscape osiągnął wręcz kosmiczną wycenę. Cena akcji poszybowała w dniu debiutu spółki[39], a przed zamknięciem giełdy, za jeden walor płacono czterokrotność kwoty, jaką ustalono w ofercie. Majątek współtwórcy Netscape'a Marka Andreessena, wówczas zaledwie dwudziestoczterolatka, nagle osiągnął wartość 171 mln dolarów.

W kolejnym roku Andreessen trafił na okładkę magazynu „Time”[40] – sfotografowany boso, za to w koronie, obok podpisu: „Złoci maniacy komputerowi”. Zysków jednak nie zrealizowano. Firma Miscrosoft zaczęła dołączać do programu operacyjnego Windows 95 bezpłatną przeglądarkę o nazwie Internet Explorer. W efekcie, Netscape nie mógł pobierać opłat za swoje oprogramowanie. W 1998 roku Departament Sprawiedliwości[41] oraz prokuratorzy generalni dwudziestu siedmiu amerykańskich stanów i prokurator generalny dla Dystryktu Kolumbii, pozwali Microsoft, zarzucając firmie, że stosuje praktyki monopolistyczne, pakietując Internet Explorer z Windowsem 95. Do 2002 roku, kiedy to Microsoft podpisał ugody sądowe[42], mleko już się rozlało. W 1998 roku Internet Explorer prześcignął Netscape[43] w udziale w rynku, a w 2008 roku oficjalnie zaprzestano prac nad Netscape’em[44].

Pierwsze prawdziwie masowe oprogramowanie zostało już stworzone. Tylko, że dotąd nie dało się na nim zarabiać. Wniosek był oczywisty: detaliczny rynek programów komputerowych skończył się. Technologia potrzebuje jednak oprogramowania. W jaki sposób zamierzano finansować jego rozwój? Początkowo wydawało się, że odpowiedzią na to pytanie może być branża reklamowa. Pod koniec lat 90. Dolina Krzemowa była dosłownie zalana przedsięwzięciami z branży dot-comów. Wiele z nich zakładało, że zapłatą za ich starania będą przychody z rynku reklamowego. Jednak w 2000 roku pękła bańka spekulacyjna. Kapitalizacja Yahoo!, którego przychody pochodziły głównie z reklamy internetowej[45], spadła z 113,9 mld dolarów na początku 2000 roku do zaledwie 7,9 mld dolarów rok później.

Jest wiedzą powszechną, że reklama internetowa nie sprawdziła się jako podstawowe źródło finansowania. „Jeszcze dwa lata temu prawie wszyscy reklamodawcy przekonywali: «Muszę być w internecie»[46]. Dziś wycofują się z tego: «Czy naprawdę promowanie tej marki w internecie jest uzasadnione?»”, komentował w listopadzie 2001 roku Pat McGrath, prezes agencji reklamowej Arnold McGrath. Podobne głosy dało się słyszeć w całej branży. Najzwięźlej podsumowała to Wendy Taylor, redaktor magazynu „Ziff Davis Smart Business”: „Reklama internetowa się skończyła”[47].

Branży, która posiadała najlepsze w historii narzędzia do pomiaru wielkości jej odbiorców, zarzucano, że nie oferuje żadnych danych, które mogłyby udowodnić skuteczność jej usług. Firmy internetowe zaczęły

szukać lepszych skal porównawczych. Doskonała technologia umożliwiająca śledzenie ruchu internetowego, zwana „ciasteczkami" [ang. *cookies*] umożliwiała podążanie za użytkownikiem internetu, strona za stroną. Nie było jednak wiadomo, czy jest ona zgodna z prawem.

W 2000 roku wniesiony został pozew zbiorowy[48] przeciwko firmie DoubleClick, której zarzucono instalowanie „ciasteczek" na komputerach użytkowników stron internetowych. Powodowie twierdzili, że narusza to ich prawo do ochrony przed podsłuchiwaniem, hakowaniem i elektroniczną inwigilacją. Rok później sędzia Sądu Dystryktowego dla Południowego Dystryktu Nowego Jorku, Naomi Reice Buchwald, orzekła, iż działania DoubleClick nie były nielegalne, ponieważ administratorzy owych stron internetowych zezwolili firmie na instalowanie „ciasteczek" na komputerach odwiedzających je osób. W uzasadnieniu napisała, że „ustalono, iż powiązane z DoubleClick witryny internetowe są stronami w procesie komunikacji z powodami, i że zgoda, której udzieliły one firmie DoubleClick na przechwytywanie tej komunikacji, jest wystarczająca, by uzasadnić takie jej działania". Decyzja sędzi otworzyła drogę korporacyjnej internetowej inwigilacji: gdy dana osoba odwiedza stronę internetową, administrator tej strony ma prawo udzielić innemu podmiotowi zgody na przechwytywanie danych o odwiedzającym.

Zatem Dolina Krzemowa wypracowała w końcu swój model biznesowy. Jest on oparty na śledzeniu.

* * *

Oczywiście firmy od dawna zbierały dane na temat swych klientów i pracowników. Jednak kupowanie i sprzedawanie danych osobowych urosło do rozmiarów branży dopiero, gdy pojawiły się nowoczesne komputery.

W 1971 roku szef Vinoda Gupty poprosił go, by ten przygotował listę wszystkich działających w kraju sprzedawców domów na kółkach. Gupta, imigrant z Indii, który właśnie ukończył studia w dziedzinie administracji biznesowej na Uniwersytecie Nebraski[49], przysiadł nad stertą książek telefonicznych zawierających dane przedsiębiorstw i zaczął tworzyć swoje własne zestawienie. Wkrótce zdał sobie sprawę z tego, że musi istnieć jakiś lepszy sposób na opracowywanie list sprzedażowych. W 1972 roku założył firmę o nazwie American Business Information, która wykorzystywała

dane z tzw. żółtych stron i katalogów, do tworzenia dedykowanych list dla sprzedawców. Spółka, która dziś znana jest jako Infogroup, wkrótce rozszerzyła obszar zainteresowań o dane abonentów indywidualnych. Zaczęła kupować je od profesjonalnych stowarzyszeń oraz zbierać każdego rodzaju dostępne publicznie informacje – od danych dotyczących praw jazdy czy kart do głosowania po wiadomości z postępowań sądowych.

„Możemy tak naprawdę stworzyć dowolną listę[50]. Jeśli potrzebujecie zestawienia leworęcznych golfistów albo leworęcznych rybaków, czy też rybaków łowiących na muszkę lub posiadaczy psów, możemy je wykonać", mówił później Gupta.

W skali całego kraju mierzyła się z tym samym wyzwaniem inna firma, mająca siedzibę w Conway w stanie Arkansas. W 1969 roku Charles Ward, lokalny przedsiębiorca, aktywny działacz Partii Demokratycznej, założył małą spółkę[51] o nazwie Demographics Inc., by wspierać kandydatów w prowadzeniu kampanii wyborczych z wykorzystaniem bezpośredniej korespondencji. Zanim przeniosła się w inne niż polityka obszary, jego firma pomagała Dale'owi Bumpersowi w wyścigu o fotel gubernatora stanu Arkansas oraz Lloydowi Bentsenowi w jego – zakończonym przegraną – starcie w wyborach prezydenckich[*7]. W 1989 roku firma zmieniła swą nazwę na Acxiom.

Axciom rósł w latach 90., ponieważ biznes potrzebował spółek mających doświadczenie w pracy z programami komputerowymi do zarządzania danymi ich klientów. Pomiędzy rokiem 1993 a 1998 przychody spółki wzrosły czterokrotnie[52] – od 91 mln dolarów do 402 mln dolarów. „Dane zawsze były obecne w biznesie. Dziś po prostu, dzięki technologii, możemy mieć do nich lepszy dostęp", mówił w wywiadzie dla dziennika „Washington Post" w 1998 roku prezes firmy, Donald Hinman. Skarby w postaci danych napędzały nowe przedsięwzięcia. Wystawcy kart kredytowych Capital One oraz Discover[53] znaleźli sposób na podzielenie ludności na kawałki – segmentację według potencjału przychodowego. To pozwoliło im docierać do ludzi za pomocą celowanych kampanii korespondencyjnych. Sprzedaż danych stała się lukratywnym biznesem dla władz na wszystkich możliwych poziomach. Tylko stan Floryda zarabia około 62 mln dolarów rocznie[54] na sprzedawaniu danych o wystawianych kierowcom prawach jazdy. Amerykańska poczta generuje około 9,5 mln dolarów przychodów[55] z udzielania firmom takim jak Acxiom dostępu do danych Krajowej Zmiany Adresu (National Change of

Address).

W pierwszej dekadzie XXI, gdy internet stał się wszechobecny, sprzedawcy[56] zaczęli interesować się „bardziej świeżymi" danymi, zdradzającymi choćby to, jakie strony odwiedzają ludzie korzystający z sieci. Dział prawny DoubleClick dał początek nowej branży, koncentrującą się na podążaniu za każdym kliknięciem użytkownika stron www. W 2007 roku wszyscy giganci internetowi dosłownie „wskoczyli" w biznes polegający na śledzeniu klientów. Przedsiębiorstwo AOL zakupiło firmę specjalizującą się w profilowaniu klientów o nazwie TACODA za 275 mln dolarów[57]. Google zapłacił 3,1 mld dolarów za DoubleClick[58], a Microsoft – 6 mld dolarów za spółkę reklamy internetowej aQuantive[59]. Wszystkie te firmy zaczęły tworzyć profile użytkowników sieci internetowej.

Pośrednicy w handlu wielkimi zbiorami danych [ang. *big data*] zareagowali natychmiastowo. Acxiom, wraz z innymi tego typu podmiotami[60], zaczął pracować nad połączeniem swoich zasobów z danymi o ruchu internetowym, by umożliwić reklamodawcom docieranie z ich komunikatami do klientów w sposób tak precyzyjny, jak tradycyjne kampanie korespondencyjne. Jednocześnie Acxiom zaczął sprzedawać dane firmom takim jak Facebook, które pragnęły zintensyfikować śledzenie użytkowników[61].

Śledzenie w sieci napędzało także rozwój nowej branży: handlu danymi. Na giełdach podobnych do tych, które znamy z rynku akcji, reklamodawcy zaczęli kupować i sprzedawać profile klientów w ramach transakcji dokonywanych w przeciągu milisekund. Wygląda to tak: kiedy przeglądacie ogłoszenie o sprzedaży kamery cyfrowej w serwisie eBay[62], na stronie internetowej zostaje zagnieżdżony kod z giełdy danych, na przykład BlueKai. Gdy BlueKai dostaje informację, że znajdujecie się na tej stronie, natychmiast zaczyna oferować wasze „ciasteczka" tym reklamodawcom, którzy chcą trafić ze swym przekazem do potencjalnych nabywców kamer. Ten, kto zaoferuje najwięcej, wygrywa prawo do wyświetlenia reklam kamer cyfrowych na kolejnej stronie internetowej, którą odwiedzicie. To dlatego reklamy *online* zdają się was śledzić.

W dużej mierze to właśnie dzięki śledzeniu rynek reklamy internetowej[63] rośnie tak szybko. Przychody branży wzrosły z 7,3 mld dolarów w 2003 roku do 36,6 mld dolarów w 2012 roku. Jest to dla branży

tak ważne, że w 2013 roku Randall Rothenberg, przewodniczący Związku Pracodawców Branży Internetowej (Interactive Advertising Bureau, IAB) stwierdził, że gdyby podmioty rynku reklamy internetowej utraciły możliwość śledzenia ludzi, „wyparowałyby z niego miliardy dolarów i setki tysięcy miejsc pracy”[64].

Członkini Komisji Europejskiej, Meglena Kunewa, świetnie podsumowała to w 2009 roku: „Dane osobowe są dla internetu tym, czym ropa naftowa dla rynku energii; to także nowa waluta cyfrowego świata”[65].

* * *

Gdybyście mieli zaproponować klasyfikację podmiotów, które was śledzą, mogłaby przedstawiać się następująco:

RZĄDY

- Zbieracze okazjonalni. Instytucje, które zbierają dane w toku prowadzenia działalności, takie jak stanowe wydziały komunikacji czy urzędy podatkowe, ale w rynek danych osobowych nie są zaangażowane bezpośrednio.
- Śledczy. Urzędy, które zbierają dane na temat osób mających status podejrzanych w postępowaniach prowadzonych przez organy ścigania, takie jak FBI czy lokalna policja.
- Analitycy danych. Nowa grupa urzędów, która zbiera i analizuje dane pochodzące od agencji rządowych i prywatnych brokerów danych, takich jak stanowe centra fuzyjne czy Krajowe Centrum ds. Antyterroryzmu.
- Wywiad. Urzędy takie jak NSA, które powinny się zajmować szpiegowaniem za granicą, jednak zaczęły interesować się dodatkowo szpiegostwem wewnętrznym.

KORPORACJE

- Zbieracze okazjonalni. To zasadniczo wszystkie przedsiębiorstwa, które zbierają dane osobowe w toku prowadzenia działalności – począwszy od lokalnych pralni przez banki po dostawców usług

telekomunikacyjnych.

- „Freestylowcy". Są to zwykle firmy z rynku oprogramowania, takie jak Google czy Facebook, które dostarczają bezpłatne usługi, a zarabiają na danych swych klientów – zwykle sprzedając dostęp do tych danych specjalistom do spraw marketingu.
- Marketingowcy. Rozwój dyscypliny jaką jest śledzenie w sieci jako podstawy rynku reklamy cyfrowej, pchnął marketingowców przede wszystkim ku rynkowi danych.
- Brokerzy danych. To firmy, które kupują dane od okazjonalnych zbieraczy rządowych i korporacyjnych, analizują je, a następnie odsprzedają. Niektóre z nich, takie jak Acxiom, sprzedają je głównie do biznesu. Inne, takie jak Intelius, sprzedają je podmiotom indywidualnym.
- Giełdy danych. Marketingowcy oraz brokerzy danych handlują informacjami z coraz większą intensywnością, na funkcjonujących w czasie rzeczywistym parkietach, które przypominają giełdy papierów wartościowych.

JEDNOSTKI

- Zdemokratyzowane dragnety. Technologia stała się wystarczająco tania, by każdy mógł oddawać się śledzeniu na własny użytek, za pomocą narzędzi takich jak kamerka na desce rozdzielczej, samodzielnie skonstruowane drony czy okulary Google'a zawierające małe kamerki, umożliwiające robienie zdjęć i kręcenie filmików.

Ci, którzy śledzą, są ze sobą głęboko powiązani. Dane rządowe stanowią krwiobieg dla korporacyjnych brokerów danych. Natomiast rządowe dragnety działają w oparciu o informacje pozyskiwane przez sektor prywatny.

Zwróćcie uwagę na taki przykład: głosowanie w wyborach. Aby zarejestrować swój głos[66], obywatel musi wypełnić formularz, który zwykle zawiera pytania o nazwisko, adres i, w prawie wszystkich stanach, datę urodzenia. Jednak niewielu oddających głos zdaje sobie sprawę z tego, że listy te są sprzedawane korporacyjnym brokerom danych. Badanie przeprowadzone w 2011 roku pokazało[67], że listy głosujących z całego stanu sprzedano za ledwie 30 dolarów w Kalifornii i aż 6,050

dolarów w Georgii.

Korporacyjni brokerzy danych łączą dane o głosujących z innymi, tworząc w ten sposób bogate w informacje profile jednostek. Na przykład firma brokerska Aristotle Inc. chwali się bazą 190 milionów nazwisk wyborców[68], które może posegregować według ponad „pięciuset kryteriów konsumenckich", takich jak ich ocena kredytowa[69] czy wielkość posiadanego kredytu hipotecznego.

Zgadnijcie, kto kupuje od firmy Aristotle tak wzbogacone dane? Politycy, którzy niekiedy wykorzystują do tego rządowe pieniądze. Firma ekscytuje się[70], że „każdy amerykański prezydent – zarówno wywodzący się z Demokratów jak i z Republikanów – od Reagana przez Obamę, wykorzystywał produkty i usługi Aristotle'a". W swej śmiałej pracy dyplomowej z 2012 roku[71], studentka Uniwersytetu Harvarda, Melissa Oppenheim, zwróciła uwagę, że 51 członków amerykańskiej Izby Reprezentantów rzeczywiście kupowało dane od Aristotle'a, przeznaczając na to służbowe środki. Te informacje miały im pomóc zrozumieć, kim są ich wyborcy[72]: w jakim wieku mają dzieci, czy prenumerują czasopisma religijne albo posiadają licencję łowiecką. W ten sposób dane stale znajdują się w obiegu[73]. Oppenheim nazywa to zjawisko „ciemnym kręgiem danych". Rząd wymaga od swych obywateli, by tworzyli zbiory danych, a następnie odsprzedaje je prywatnym podmiotom, które „piorą" je i odsprzedają je z powrotem rządowi. Z ciemnym kręgiem danych mamy do czynienia praktycznie w przypadku każdego rodzaju informacji. Dane z praw jazdy są przemiatane[74] do raportów LexisNexis, które następnie wzbogacane są innego rodzaju informacjami, a potem sprzedawane Departamentowi Bezpieczeństwa Krajowego. Dane o sprzedaży obciążonych hipoteką nieruchomości są przygotowywane w stanowych sądach[75], a następnie opracowywane przez brokerów takich jak CoreLogic, które sprzedają pakiety danych o nieruchomościach[76] swym klientom – także rządowi.

Z jeszcze ciemniejszym kręgiem danych mamy do czynienia w tajnym Sądzie Nadzoru Wywiadu Stanów Zjednoczonych – w toczących się przed nim postępowaniach rząd może bowiem zażądać, by sektor prywatny udzielił mu informacji o klientach. To w takich okolicznościach giganci typu Google, Yahoo!, AT&T, Verizon czy Microsoft zostali zmuszeni przekazać dane o swych klientach agencji NSA.

Jest smutną rzeczywistością, że dragnety korporacyjne i rządowe są ze sobą nierozerwalnie złączone. Jedne nie istnieją bez drugich.

* * *

Bill Binney zapłacił za wypowiadanie się przeciwko dragnetom zastawianym przez NSA. Gdy jeszcze pracował w agencji[77], przygotował coś, co, jak wierzył, było dragnetem, który uwzględniał prawo do prywatności jednostek i chronił je. Nazywało się to ThinThread i było inteligentnym programem, który przechwytywał tony danych z połączeń telefonicznych i internetowych, szyfrował je oraz analizował pod kątem występowania określonych wzorców. Dane mogły zostać odszyfrowane wyłącznie, gdy program napotkał na określone zagrożenie, a sąd zatwierdził nakaz przeszukania – odszyfrowanie danych.

Nie udało mu się jednak wdrożyć programu na dobre. Po kilku latach wewnętrznych batalii, w trakcie których Binney i jego koledzy zgłaszali się z prośbą o pomoc wprost do liderów partyjnych, szefowie NSA ostatecznie pozbawili program ThinThread swego poparcia. Jednym z powodów było to, że w erze, która poprzedzała ataki z 11 września, prawnicy NSA obawiali się[78], iż ThinThread będzie naruszał prawo do prywatności amerykańskich obywateli. Umożliwiał on przecież zbieranie danych dotyczących krajowej komunikacji, mimo iż były one zaszyfrowane. Drugim powodem było to[79], że dyrektor NSA Michael Hayden postanowił wesprzeć inny, znacznie zresztą droższy program, Trailblazer, stworzony przez prywatnego dostawcę, który także miał służyć analizowaniu morza danych pozostających w dyspozycji NSA. Ten jednak nie szyfrował danych. Z Trailblazera ostatecznie zrezygnowano, gdy w istotny sposób przekroczony został budżet i doszło do wielu technicznych problemów.

W 2002 roku kolega Binneya[80], Kirk Wiebe, który pracował z nim nad ThinThread, skontaktował się z inspektorem generalnym Departamentu Obrony, by złożyć raport na temat tego, co w jego przekonaniu stanowiło proceder „marnotrastwa, malwersacji i pogwałcenia praw" przez NSA. W raporcie inspektora generalnego[81], który powstał ostatecznie w 2005 roku, choć był on mocno okrojony, w pewnym stopniu zrehabilitowano ThinThread.

W roku 2006 gazeta „Baltimore Sun" opublikowała artykuł[82]

o wojnach wokół ThinThread. „NSA odrzuciło system, który przesiewał dane o połączeniach telefonicznych w sposób legalny" – brzmiał nagłówek. 26 lipca 2007 roku FBI wkroczyło do domu Binneya[83], położonego na jednym z przedmieść w stanie Maryland. Binney brał właśnie prysznic. „Jeden z tych facetów wszedł do łazienki i wycelował we mnie broń. Powiedziałem więc: «Czy sądzisz, że mógłbym coś na siebie narzucić?»", wspominał[84]. Także Wiebe, który – podobnie jak Binney – przeszedł na emeryturę w 2001 roku, miał „nalot" na dom[85]. Żaden z nich ostatecznie nie został jednak oskarżony o popełnienie przestępstwa.

28 listopada 2007 roku FBI wkroczyła[86] też do domu innego zwolennika ThinThread, Thomasa Drake'a, jednego z wysokich rangą kierowników NSA, który – anonimowo – współpracował z Binneyem i Wiebe'em przy sprawie donosu do inspektora generalnego. Agenci zajęli dokumenty, komputery i dyski należące do Drake'a. Twierdzili też, że w jego piwnicy znaleźli tajne akta. Dwa i pół roku później postawiono go w stan oskarżenia[87] – zarzucając mu naruszenie ustawy o szpiegostwie (Espionage Act) poprzez umyślne przetrzymywanie tajnych dokumentów.

W wyniku prokuratorskiego postępowania, Drake popadł w ruinę[88]. Brakowało mu jeszcze pięć i pół roku do emerytury w NSA. Stracił uprawnienia do przyszłego świadczenia w wysokości 60 tys. dolarów rocznie. Obciążył dom drugą hipoteką i wybrał większość środków zgromadzonych w planie emerytalnym, by móc się utrzymać. Wiadomo było, że nie zatrudni się już w wywiadzie. Zaczął więc pracować w sklepie Apple. Po wydaniu przeszło 82 tys. dolarów na opłaty sądowe[89], został uznany za wystarczająco biednego, by pozwolono mu skorzystać z usług obrońcy z urzędu. W 2011 roku, po całej fali artykułów prasowych o sprawie Drake'a[90], rząd zaproponował wycofanie wszystkich dziesięciu zarzutów, jakie wobec niego sformułował, pod warunkiem, że Drake przyzna się do popełnienia występku, jakim było „przekroczenie granic dozwolonego wykorzystania rządowego komputera". Sędzia sądu dystryktowego Richard D. Bennett określił w orzeczeniu[91] dwuipółletni okres, w którym rząd przygotowywał akt oskarżenia, czymś „nie do przyjęcia". „Jednym z podstawowych założeń Karty Praw, ustanowionej w tym kraju, było to, by jego obywatele nie byli narażeni na działania ludzi, którzy pukają do ich drzwi w imieniu władzy i wchodzą do ich domów", napisał sędzia. „A gdy nawet tak się stanie,

by sprawy wyjaśniane były możliwie szybko".

Sędzia Bennett nie skrytykował rządu otwarcie za nadużycie władzy celem spacyfikowania sygnalisty [ang. *whistle-blower*]. Wymierzył jednak Drake'owi najniższą możliwą karę – wyrok w zawieszeniu na rok i dwadzieścia godzin prac społecznych na miesiąc. Drake nie został ukarany grzywną. Kończąc odczytywanie orzeczenia, sędzia zwrócił się do niego: „Życzę ci dużo szczęścia w twoim dalszym życiu".

Przed skazaniem Drake'a, Binney, Drake oraz Wiebe starali się reformować agencję od środka. Jednak, gdy termin procesu Drake'a był coraz bliżej, postanowili dotrzeć do szerszej publiczności. Po tym jak Drake został oczyszczony z zarzutów, stali się pełnoetatowymi krytykami NSA, udzielając w ostrym tonie wywiadów tytułom prasowym i ostrzegając przed władzą niekontrolowanej agencji, która posiada informacje na temat nas wszystkich.

Gdy po raz pierwszy spotkałam Binneya[92], od razu powiedział mi, że ilość danych zgromadzonych przez NSA przekracza „o całe rzędy wielkości" to, co udało się pozyskać najbardziej opresyjnym reżimom tajnych policji Gestapo, Stasi czy KGB.

Jak stwierdził: „Gromadzenie przez rząd tak wielkich ilości informacji o obywatelach stanowi dla nas prawdziwe zagrożenie. Daje mu to władzę nad każdym z nas"[93].

3

POD NADZOREM

Nadzór, sam w sobie, nie jest czymś potwornym.

Rodzice pilnują swoich dzieci, aby te nie zrobiły sobie krzywdy. Policjanci monitorują ludność, by łapać kryminalistów. Firmy kontrolują swoich pracowników, aby wykryć złodziei i oszustów. Dziennikarze patrzą na ręce potężnym instytucjom, by ujawniać ich nadużycia.

Jednak we współczesnej erze dragnetów mamy do czynienia z nowym typem nadzoru: w warunkach braku jakichkolwiek podejrzeń, skomputeryzowanym, bezosobowym i zakrojonym na szeroką skalę. Niektórzy wierzą, że ten rodzaj inwigilacji zapewni społeczeństwu większe bezpieczeństwo. Inni są przekonani, że przyczyni się do stworzenia państwa policyjnego.

By zrozumieć, jak mógłby wyglądać najgorszy scenariusz, odwiedziłam najlepiej zachowane archiwum inwigilacji sprzed ery cyfrowej, jakie istnieje na świecie: archiwum Stasi w Berlinie. Chciałam porównać dokumenty posiadane przez Stasi, tajną policję polityczną w NRD, do informacji, które dziś gromadzą podmioty rynku i rządy w trakcie prowadzenia działań o charakterze inwigilacji.

Tajne służby Stasi prowadziły działania w olbrzymiej, niespotykanej w dziejach świata, skali[1], jeśli przeliczyć ich koszt na mieszkańca. W ramach tego represyjnego systemu, zgromadzono dokumenty o 4 milionach obywateli NRD[2], co stanowiło około jednej czwartej całkowitej liczby ludności tego kraju[3], wynoszącej 16,7 miliona. Stasi nie miała do dyspozycji dzisiejszej technologii. Musiała otwierać listy i bezpośrednio podsłuchiwać rozmowy telefoniczne. Miała jednak rozbudowaną sieć informatorów. W 1989 roku praktycznie co piąty

mieszkaniec Niemiec Wschodnich[4] w wieku od osiemnastu do osiemdziesięciu lat w jakimś zakresie pracował dla Stasi.

Kiedy reżim w Niemczech Wschodnich zaczął chylić się ku upadkowi w listopadzie 1989 roku, oficerowie Stasi zaczęli likwidować akta osobowe obywateli. Mieszkańcy, oburzeni faktem, że niszczone są świadectwa opresyjności ustroju, szturmowali siedzibę tajnej policji, by zatrzymać proces niszczenia dokumentów. W konsekwencji współcześni obywatele mają dostęp do dokumentów na ich temat. Badacze natomiast mogą przeglądać niektóre pliki, z których usunięto nazwiska monitorowanych osób.

Podczas mojej podróży do Berlina w 2011 roku, odwiedziłam archiwum Stasi – znane dziś jako urząd Pełnomocnika Federalnego do spraw Materiałów Państwowej Służby Bezpieczeństwa NRD – które zlokalizowane jest, dość zresztą niestosownie, w radośnie wyglądającym, szklanym budynku biurowym w samym sercu miasta.

Günter Bormann, administrator dokumentów Stasi przydzielony na moją prośbę, od razu zachwycił się moim pomysłem porównania współczesnych metod inwigilacji do tych z czasów NRD. Kiedy wypełniałam dokumenty, zapytał co może o mnie wiedzieć typowy zachodni zbieracz danych. Spytałam więc, czy mogę użyć jego komputera, aby pokazać mu choć odrobinę tego, co mówi na mój temat internet.

Zalogowałam się do konta Gmail, weszłam w ustawienia, w ramach których Google pozwala zobaczyć moje wcześniejsze wyszukiwania, wliczając w to książki i zdjęcia, które przeglądałam. Wyświetliłam także listę dziewięćdziesięciu trzech osób, z którymi wymieniałam e-maile albo porozumiewałam się przez komunikator.

Stojący nade mną Bormann był pod wrażeniem. Przyznał, że odwzorowywanie powiązań społecznych było „bardzo trudne dla Stasi". Usiadł przy stole konferencyjnym i zaczął kreślić koła wraz z wiążącymi je liniami. „Agenci próbowali tworzyć schematy sieci społecznych"[5], jednak nawet z pomocą wszystkich informatorów, ciężko im było przygotować solidny schemat.

Zainspirowana, weszłam na swój profil na LinkedIn, gdzie miałam zainstalowaną specjalną wtyczkę, która pozwalała zobaczyć wizualizację mojej sieci społecznej. Był to piękny graf, składający się z ponad dwustu punktów, połączonych ze sobą kolorowymi liniami. Wszyscy moi znajomi z pracy w Nowym Jorku byli zgromadzeni w jednym, oznaczonym

na żółto, rogu, inni koledzy z mediów mieścili się w niebieskiej części, natomiast moje kontakty z czasów, gdy żyłam w Kalifornii, wyodrębnione zostały na przeciwległym krańcu grafu i oznaczone kolorem pomarańczowym z szarymi kropkami.

Wydawało się, że Bormann jest pod coraz większym wrażeniem: „Stasi by to pokochała".

* * *

Trzy miesiące później, na moje biurko w Nowym Jorku dotarła paczka dokumentów. Zawierała setki stron, a pomiędzy nimi dwa zestawy akt w języku niemieckim. Po krótkich poszukiwaniach, znalazłam kilku ekspertów ds. Stasi, którzy mieli mi pomóc przetłumaczyć i zrozumieć te dokumenty.

Szokujące było, jak toporne były dawniej metody inwigilacji. „Podstawową technologię śledczą stanowiły listy, telefony i informatorzy"[6], powiedział Gary Bruce, profesor na Uniwersytecie w Waterloo i autor książki *The Firm: The Inside Story of the Stasi*.

Pierwsze akta dokumentowały inwigilację niższego stopnia, zwaną imforgang, która polegała na zrekrutowaniu nieokreślonego celu do współpracy w charakterze informatora. (Nazwiska celów były zmienione; dane agentów Stasi i informatorów już nie). W tym przypadku, Stasi obserwowała dość „nudnego" ucznia szkoły średniej[7], żyjącego z matką i siostrą w zwyczajnym mieszkaniu. Tajna policja otrzymała raport na jego temat od dyrektora szkoły i klubu, którego był członkiem.

Stasi nie posiadała o nim wielu informacji. Widziałam bardziej rozbudowane profile na Facebooku. Mimo to, chciano go zwerbować jako informatora. Odrzucił ich propozycję, powołując się na bliżej nieokreślone problemy zdrowotne. Miał szczęście, ponieważ był młody i wiódł uporządkowane życie. Większość osób, które Stasi zamierzało pozyskać do współpracy, nie mogło odmówić, bowiem natychmiast przedstawiano im dowody na popełnione przez nie drobne wykroczenia – choćby oglądanie zachodnioniemieckiej telewizji.

Drugie akta zwierały informacje na temat operacji śledczej znanej jako OPK[8] – od Operative Personenkontrolle. Dotyczyły autora zaangażowanej, opozycyjnej poezji. Operacja była prowadzona raczej w średniej[9] skali: Stasi wypuściła przeciwko niemu trzech informatorów,

ale nie otwierała jego korespondencji przy użyciu pary ani nie podsłuchiwała jego rozmów telefonicznych.

Oficerowie Stasi otrzymywali dodatki za prowadzenie OPK[10], a jeszcze większa nagroda czekała na nich, jeśli operacja się powiodła, przyczyniając się do aresztowania albo pozyskania nowego informatora. Ostatecznie, działania OPK wobec poety okazały się bezowocne[11]: reżim upadł zanim tajna policja mogła podjąć jakiekolwiek kroki przeciwko niemu.

Sześć miesięcy później otrzymałam mniejszą przesyłkę. Zawierała zaledwie piętnaście stron, dokumentujących charakterystyczną dla Stasi metodę inwigilacji, o której chciałam dowiedzieć się więcej.

Jedne akta[12] zawierały informacje o wszelkich ruchach podejmowanych w ciągu dwóch dni przez pewnego czterdzistodwulatka. Miało to miejsce 28 i 29 września 1979 roku. Agenci obserwowali go, gdy oddawał pranie, pakował do auta rolki tapety oraz wiózł w samochodzie dziecko, „przestrzegając ograniczeń prędkości", zatrzymując się po gaz, a potem dostarczył tapetę do bloku mieszkalnego. Stasi śledziła samochód także wtedy, gdy jechała nim kobieta, odwożąc dziecko z powrotem do Berlina.

„Obserwowani byli niezwykle roztropni (...)", napisał w raporcie oficer Stasi, podpułkownik Fritsch. „Najpewniej (...) [zostali] uprzedzeni (...), że w pobliżu prowadzone są działania".

Agent prawdopodobnie zaczął śledzić swój cel około 16.15 w piątek popołudniu. O 21.38 obserwowany wrócił do swojego mieszkania i wyłączył światła. Agent spędził całą noc na inwigilacji i przekazał zadanie innemu oficerowi o godzinie 7.00 w sobotę rano. Ten najpewniej śledził cel do 22.00. Z dzisiejszej perspektywy, nakład pracy wydaje się olbrzymi w stosunku do ilości pozyskanych informacji.

Drugie akta[13] zawierały odręcznie narysowaną sieć kontaktów. Na jednej kartce papieru agenci umieścili czterdzieści sześć relacji łączących cel ich obserwacji z różnymi ludźmi („ciotka", „Przypadek operacyjny Jentzsch", zapewne Bernd Jentzsch, poeta z NRD, który uciekł na Zachód w 1976 roku) i miejscami („kościół"). Oznaczyli także metody kontaktu („pocztą, przez telefon, spotkanie na Węgrzech").

To było zdumiewające. Dokument opisywał niespełna 25 proc. moich kontaktów z LinkedIn, których miałam nieco ponad 200. Jednak zdawały się one bardzie przydatne dla śledztwa niż moja rozległa sieć społeczna.

Stasi zapewne prowadziła monitoring wszystkich osób z grafu[14], jak twierdzi Gary Bruce. Były one określane jako „jednostki drugorzędne".

„Nie musiałaś prowadzić działalności opozycyjnej, aby trafić do raportów Stasi”, dodaje.

Problem polegał na tym, że dokumenty Stasi[15], bez względu na ich objętość, mogły wpłynąć na to, czy osoba dostała awans, czy została zdegradowana, ile czekała na samochód lub mieszkanie, a także na to, czy wniosek o zgodę na odwiedzenie bliskich na Zachodzie zostanie rozpatrzony pozytywnie. W konsekwencji, choć Stasi posiadała papiery na jedną czwartą populacji, strach przed możliwością bycia przez nią namierzanym, był wszechobecny.

W ankiecie z 1990 roku, tuż po upadku komunizmu, 72,6 proc. obywateli byłego NRD opisało doświadczenia związane z komunizmem jako „totalną inwigilację”. W 1992 roku, 43 proc. respondentów pytanych, czy zgadzają się z tezą, iż w tamtych czasach: „Można było się czuć śledzonym. Nikomu nie można było ufać”, odpowiedziało: „To prawda, dokładnie tak było”.

W ramach badania[16] poświęconego psychologicznym skutkom inwigilacji prowadzonej przez Stasi, Babett Bauer przeprowadziła wywiady z około trzydziestoma osobami, które miały bezpośrednie doświadczenia z tajną policją. Odkryła, że strach przed kolejnym spotkaniem ze Stasi prowadził do tego, że ludzie albo przeistaczali się we wzorowych obywateli, albo w wyrzutki społeczeństwa. Bauer doszła do wniosku, że osoby, które miały do czynienia ze Stasi utożsamiały represje z „obrażeniami na ciele i odruchami bezwarunkowymi”.

* * *

Represyjna siła obserwacji była ideą założycielską panoptykonu[17] – modelu więzienia zaproponowanego przez Jeremy’ego Benthama w 1787 roku. Zakładał, że doskonałe więzienie pozwoli więźniom wierzyć, że są stale monitorowani, a obserwatorom pozostać niewidocznymi. Zaprojektował okrągły budynek więzienia z wieżą strażniczą w środku. Projekt ten jednak nie został zrealizowany za jego życia.

W 1975 roku, francuski filozof Michel Foucault[18] spopularyzował ideę Benthama, opisując panoptykon jako „kapitalne” narzędzie władzy. „Dlatego to Bentham przyjął, że władza ma być widzialna i nieweryfikowalna. Widzialna – więzień będzie miał nieustannie przed oczyma wyniosłą sylwetkę wieży centralnej, skąd się go szpieguje. Nieweryfikowalna – więzień nigdy nie powinien wiedzieć, czy jest

obecnie obserwowany, ale ma być pewien, że zawsze może tak być”[*8], napisał w swojej książce *Nadzorować i karać. Narodziny więzienia*.

Obecnie żyjemy w świecie rozległej inwigilacji, więc określenie „niepokojącej świadomości” powinno odzwierciedlać zbiorowy stan naszego umysłu. Wydaje się jednak, że Foucault miał tylko częściowo rację. Jak odkryła w trakcie licznych rozmów Babett Bauer, ludzie radzą sobie z inwigilacją, zmieniając swoje zachowanie i stając się coraz bardziej zlęknieni.

W 2011 roku fińscy naukowcy zainstalowali[19] w dziesięciu domach rozbudowany sprzęt monitorujący, w tym kamery wideo, mikrofony i urządzenia monitorujące komputery, smartfony czy telewizję. Miały pozostać rozstawione w ten sposób przez rok. Badacze chcieli przyjrzeć się długofalowym skutkom wszechobecnej inwigilacji. Odkryli, że uczestnicy eksperymentu (bez wątpienia wolontariusze) „stopniowo przyzwyczajali się do monitoringu”. Ich reakcje były jednak różne. Jeden zrezygnował po sześciu miesiącach, twierdząc, że nieustanny nadzór zniechęcił go do używania komputera i wpłynął negatywnie na niego bądź na jego relacje z ludźmi. (Badacze nie ujawnili płci, ani nie podawali do wiadomości szczegółów ułatwiających identyfikację uczestników).

Mimo, że badani wiedzieli, że dane z monitoringu ujawniane są wyłącznie naukowcom, i mimo że mogli wyłączyć system w dowolnym momencie, nadal uważali, że inwigilacja jest źródłem „irytacji, niepokoju, rozgoryczenia, a nawet złości”. Najbardziej znienawidzone były ekrany komputera i kamery wideo (które, jak przyznało dwóch uczestników, były przez nich regularnie wyłączane).

Większość badanych zmieniło swój sposób działania. Ludzie ci stali się bardziej ostrożni, w szczególności tam, gdzie się rozbierali (kamery nie były umieszczone w łazienkach i sypialniach) i gdzie prowadzili poufne rozmowy.

„Dwoje uczestników zaczęło spędzać więcej czasu w sypialni, która nie miała zainstalowanych mikrofonów. Dwoje innych przyznało, że w celu przedyskutowania spraw osobistych spotykało się w kawiarni. Jeden wspomniał, że unikał zapraszania do domu wielu osób”, napisali autorzy badania.

Główny autor projektu[20], naukowiec pracujący w dziedzinie informatyki, Antti Oulasvirta wyjaśnił, że choć w ciągu trzech miesięcy udało się rozwiać nadmierne wątpliwości uczestników co do kwestii

prywatności, to jednak ludzie wyraźnie dostosowali swoje zachowanie do sytuacji. *Status quo* łatwo jednak było zburzyć. „Zmiany, które wprowadzaliśmy, zawsze sprawiały, że sytuacja stawała się napięta. Jakiekolwiek nieprzewidziane wydarzenia towarzyskie ujawniały zupełnie nowe praktyki, podważały je, a czasami zapobiegały ich pojawieniu się".

* * *

Inny sposób radzenia sobie z wszechobecną inwigilacją[21] przedstawia autor książek *science fiction*, David Brin, w swojej proroczej publikacji z 1998 roku pod tytułem *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*?

Książka zaczyna się „przypowieścią o dwóch miastach". Każde z nich ma zainstalowane kamery „na latarniach, dachach i znakach drogowych". W pierwszym mieście, wszystkie obrazy przesyłane są do komisariatu policji. W drugim mieście, każdy obywatel ma dostęp do rejestru z kamery za pośrednictwem telewizji zainstalowanej w zegarku.

W obu miastach nie ma przestępczości. Pierwsze jest jednak państwem policyjnym, a drugie cieszy się pewną wolnością: „Osoba spacerująca późnym wieczorem może się upewnić, czy nikt nie czyha za rogiem (...) Niespokojny rodzic skanuje otoczenie, aby sprawdzić, w którą stronę powędrowało dziecko (...) Sklepowy złodziej ostrożnie trafia do aresztu (...), ponieważ kierujący zatrzymaniem policjant wie, że cały proces jest skrupulatnie rejestrowany".

Brin przekonywująco dowodzi, że rozpowszechnienie kamer i innych technologii śledczych jest nieuniknionym rezultatem rozwoju technologii. Jednak kluczową kwestią jest to, kto kontroluje kamery? Uważa, że wzajemny monitoring, polegający na tym, że obywatele i państwo wzajemnie się obserwują, może sprawić, że wszechobecny nadzór nie będzie miał charakteru opresji, a związany będzie ze współdzieloną odpowiedzialnością. Istnieją argumenty na poparcie tej tezy.

Podczas zimnej wojny, wzajemny nadzór odgrywał istotną rolę. Miał zapobiegać sytuacji, w której Stany Zjednoczone i Związek Sowiecki rzuciłyby przeciwko sobie bomby atomowe.

Po tym jak w 1957 roku Związek Radziecki wystrzelił na orbitę satelitę o nazwie Sputnik, Amerykę sparaliżował strach przed możliwościami ZSRR i ich potencjalnymi skutkami. W 1958, senator John F. Kennedy ogłosił[22],

że USA nie nadążają za Sowietami, przewidując, że „do 1960 roku, Stany Zjednoczone stracą (...) swoją przewagę w nuklearnym potencjale uderzeniowym".

Trwało to jednak do czasu. Już wkrótce Stany Zjednoczone wysłały satelitów rozpoznawczych[23], które pozwoliły im ustalić różnicę pomiędzy USA i ZSRR w liczbie posiadanych przez nie pocisków antyrakietowych. Przechwycone obrazy potwierdziły[24], że sytuacja jest zgoła inna: w 1961 roku Sowieci dysponowali raptem czterema międzykontynentalnymi pociskami balistycznymi[25]. Zapasy amerykańskie liczyły sto siedemdziesiąt pocisków.

Mimo to, Stanom Zjednoczonym nie udało się dostrzec, że latem 1962 roku ZSRR rozstawiła rakietowe pociski balistyczne średniego zasięgu na Kubie. Była to porażka wywiadu amerykańskiego, która doprowadziła USA i ZSRR na granicę wojny atomowej. W konsekwencji, istotną częścią zimnowojennego wyścigu stało się konstruowanie coraz lepszych satelitów rozpoznawczych.

W 1972 roku Stany Zjednoczone i Związek Radziecki[26] skodyfikowały swoje działania szpiegowskie w traktacie ABM (ang. *Anti-Ballistic Missile Treaty*), w którym obie strony zobowiązały się korzystać z „narodowych środków technicznych" w celu wzajemnej weryfikacji przestrzegania postanowień porozumienia. Sześć lat później Prezydent Jimmy Carter podkreślił[27] znaczenie satelitów szpiegowskich w Centrum Kosmicznym im. Johna F. Kennedy'ego. „Satelity rozpoznawcze stały się istotnym czynnikiem stabilizującym w relacjach międzynarodowych w zakresie monitoringu realizacji porozumień odnoszących się do kontroli zbrojeń".

W istocie, nadmierna inwigilacja może skutecznie wpływać na zmianę ludzkiego zachowania. Kolejne badania dowodzą, że zwykła sugestia o byciu obserwowanym powoduje, że ludzie stają się bardziej chętni do współpracy, nawet jeśli monitoring już ustał.

Według Ryana Calo z Uniwersytetu Waszyngtońskiego, przeświadczenie, że ktoś nam towarzyszy, uruchamia stan „psychologicznego podniecenia", nawet jeśli nie jest to ktoś z krwi i kości. Ci uczestnicy jednego z badań[28], którym przedstawiono zdjęcie wielookiego robota, przekazali w symulacji komputerowej o 30 proc. więcej pieniędzy do funduszu gminy niż ci, którzy nie czuli się obserwowani.

W 2011 roku badacze z Uniwersytetu Newcastle w Wielkiej Brytanii

zawiesili w wybranych losowo punktach uczelnianej kawiarni plakaty z wielkimi oczami, znajdującymi na poziomie wzroku odbiorcy[29]. W ciągu trzydziestu dwóch dni, podczas których prowadzili obserwację, odkryli, że w bezpośredniej bliskości plakatu ludzie dwa razy chętniej niż zwykle sprzątali po sobie po posiłku. W następnym roku, podobna grupa badaczy z tego uniwersytetu rozwiesiła koło stojaków rowerowych tabliczki z informacją: „Złodzieje rowerów! Obserwujemy was”[30]. Nadruk tekstowy widniał nad fotografią przedstawiającą ludzkie oczy. Przypadki kradzieży rowerów zostały ograniczone o 62 proc. w miejscach, w których zawisły tabliczki. Tam, gdzie ich nie było, liczba kradzieży wzrosła o 65 procent. To sugeruje, że złodzieje przenieśli się do bardziej „bezpiecznych” miejscówek. „Skuteczność tej niezwykle taniej i prostej metody pokazuje, że z wykorzystania psychologii nadzoru mogą płynąć istotne korzyści w postaci ograniczenia przestępczości, i to nawet przy faktycznym braku nadzoru”, podsumowali badacze.

Teatr inwigilacji – pozorna obecność obserwacji, z udziałem podobnych do ludzkich oczu albo robotów – wydaje się pozytywnie wpływać na to, w jaki sposób ludzie odnoszą się do siebie. Wciąż nie wiadomo jednak, czy monitoring z wykorzystaniem kamer rzeczywiście przyczynia się do zwalczania przestępczości.

Przeprowadzona w 2008 roku przez Kalifornijskie Biuro Badawcze (California Research Bureau, CRB)[31] analiza czterdziestu czterech badań nad wpływem monitoringu z użyciem kamer przemysłowych na poziom przestępczości, wykazała, że wyniki 43 proc. badań sugerowały, że wpływ ten nie istnieje, podczas gdy wyniki 41 proc. mówiły o wyraźnym, dającym się zaobserwować statystycznie, zmniejszeniu poziomu przestępczości.

W 2011 roku Urban Institute przyjrzał się[32] systemom monitoringu w Baltimore, Chicago oraz Waszyngtonie. Uzyskane wyniki były w podobny sposób sprzeczne ze sobą. Badacze odkryli, że w Baltimore system pięciuset kamer obsługiwanych całą dobę przez zespół wyszkolonych, emerytowanych policjantów, doprowadził do 35-procentowego spadku liczby dokonywanych przestępstw w skali miesiąca, w jednej tylko dzielnicy. W innych dzielnicach, wykorzystywanie kamer przyniosło słabszy efekt. Podobnie było w Chicago, gdzie funkcjonuje wart wiele milionów dolarów program monitoringu, do którego należy osiem tysięcy kamer. W Urban Institute zwrócono uwagę, że kamery przyczyniły

się do 12-procentowego spadku przestępczości w chicagowskim Humboldt Park, jednak nie miały zauważalnego wpływu na liczbę przestępstw popełnianych w West Garfield Park. I wreszcie w Waszyngtonie również nie wykazano jakiegokolwiek wpływu kamer monitoringu na statystyki dotyczące przestępczości.

Jednym z powodów owej sprzeczności wyników może być fakt, że na spadek przestępczości wpływa wiele rożnych czynników. Trudno jest wyodrębnić jeden czynnik – na przykład istnienie kamer monitoringu – pominąwszy inne, takie jak zwiększenie liczby policyjnych patroli czy zmodernizowanie oświetlenia ulicznego.

W 2004 roku Leon Hempel i Eric Töpfer z Centrum Technologii i Społeczeństwa w Berlinie, przeanalizowali badania dotyczące wykorzystania systemów kamer przemysłowych w Europie i odkryli, że w wielu przypadkach nie uwzględniono w nich grup kontrolnych, dzięki którym można by porównać wskaźniki przestępczości na obszarach z zainstalowanymi kamerami z tymi na szerszych obszarach, które nie podlegają monitoringowi. Brakowało także analizy możliwości przemieszczenia się przestępczości z jednego obszaru na inne.

Tych kilka badań, które uwzględniły wyniki z grup kontrolnych, nie potwierdza jednoznacznie tezy, że kamery mogą zapobiegać przestępczości. Kolejne badanie Urban Institute z 2011 roku poświęcone wpływowi kamer monitoringu na liczbę przestępstw popełnianych na parkingach[33] – z wykorzystaniem metody opartej na losowych grupach kontrolnych – także wykazało, że istnienie kamer nie czyni większej różnicy. Porównano roczne statystyki przestępczości związanej z samochodami na dwudziestu pięciu parkingach przy stacjach metra w Waszyngtonie, na których były zainstalowane kamery z czujnikami ruchu, z danymi o liczbie incydentów na dwudziestu pięciu parkingach „kontrolnych", na których nie było kamer. Choć w tym pierwszym przypadku tak naprawdę były to stałe kamery cyfrowe, prowadzący badanie umieścili na nich znaki sugerujące, że monitoring obejmuje maksymalnie szeroki obszar i jest permanentny. Tymczasem wykazano, że „kamery nie miały żadnego znaczącego wpływu na poziom przestępczości".

Istnieją dowody na to, że zwykłe latarnie uliczne mogą w pewnym stopniu zniechęcać do popełniania przestępstw. W 2004 roku kryminolodzy Brandon Welsh i David Farrington[34] przeanalizowani trzydzieści dwa badania przeprowadzone w Stanach Zjednoczonych,

Kanadzie i Wielkiej Brytanii, by sprawdzić czy kamery przemysłowe zmniejszały przestępczość skuteczniej niż uliczne latarnie. Wniosek był następujący: oba czynniki okazały się skuteczne w zwalczaniu przestępczości dotyczącej nieruchomości, żaden jednak nie był efektywny w przypadku brutalnych napaści. Badacze stwierdzili, że zarówno kamery jak i latarnie uliczne „działają jako katalizatory spadku przestępczości poprzez zmianę percepcji, postaw i zachowań mieszkańców oraz potencjalnych sprawców".

Badacze z Urban Institute zasugerowali także[35], że kamery są skuteczne tylko wtedy, gdy zapisy z nich pochodzące są aktywnie wykorzystywane przez funkcjonariuszy organów ścigania, którzy mogą szybko działać dzięki zdobytym poprzez nie informacjom. „Technologia jest tylko tak dobra, jak sposób jej wykorzystania".

Innymi słowy, kamery wpływają na ludzkie zachowania wyłącznie wtedy, gdy ludzie są pewni, że po drugiej strony obiektywu ktoś ich obserwuje.

* * *

Nie jest także pewne, że cyfrowa inwigilacja polegająca na analizie danych, pomaga powstrzymywać terrorystów przed kolejnym uderzeniem.

Ostatecznie, wiele planów zamachów uszło uwadze dragnetów. Od czasu zamachów 11 września 2001 roku, podjęto całą serię prób. Do tych o największym znaczeniu zaliczamy:

- **„Shoe Bomber".** W 2001 roku Richard Colvin Reid[36] usiłował bez powodzenia zdetonować bombę ukrytą w swoim bucie podczas lotu samolotem z Paryża do Miami.
- **Strzelec z lotniska LAX.** W 2002 roku Egipcjanin Hesham Mohamed Hadayet[37] otworzył ogień przy stoisku biletowym linii El Al na Międzynarodowym Lotnisku w Los Angeles, zabijając dwie osoby i raniąc wiele innych.
- **Strzelec z Fort Hood.** W 2009 roku major Armii Amerykańskiej Nidal Malik Hasan[38] wkroczył do baraków w Fort Hood w Teksasie, wskoczył na biurko, krzyknął „Allahu Akbar" i otworzył ogień z dwóch pistoletów. Zabił trzynaście osób i zranił czterdzieści trzy

kolejne.

- **„Majtkowy zamachowiec”.** W Wigilię Bożego Narodzenia 2009 roku Umar Farouk Abdulmutallab[39] usiłował zdetonować ładunki wybuchowe zaszyte w bieliźnie podczas lotu z Detroit do Amsterdamu. Urządzenie nie wybuchło, ale zwyczajnie zapaliło się, raniąc Abdulmutallaba i dwóch innych pasażerów.
- **Zamachowiec z Times Square.** W 2010 roku Faisal Shahzad[40], który szkolił się z terrorystami w Pakistanie, usiłował bez powodzenia zdetonować bombę w samochodzie na nowojorskim Times Square.
- **Zamachowcy z maratonu w Bostonie.** W 2013 roku Tamerlan i Dżochar Carnajewowie[41] umieścili domowej roboty bomby nieopodal mety maratonu w Bostonie. Eksplozje zraniły setki ludzi oraz zabiły trzy, w tym ośmioletniego chłopca.

Zwolennicy inwigilacji wskazują, że rzeczone statystyki nie uwzględniają ataków, którym udało się zapobiec – zaś wiele z nich pozostaje tajemnicą. Po raz pierwszy mamy jednak choć garść dowodów na to, że jakieś ataki zostały powstrzymane.

Gdy pojawiły się pierwsze przecieki pochodzące od Snowdena[42], generał Keith Alexander, dyrektor Agencji Bezpieczeństwa Krajowego (NSA), ujawnił, że budzące tyle kontrowersji, telefoniczne i internetowe dragnety „przyczyniły się do lepszego zrozumienia, a w konsekwencji unieszkodliwienia przełomowych innowacji w dziedzinie ataków terrorystycznych” aż w pięćdziesięciu czterech sprawach.

Nie opisał tych spraw dokładnie. Wspomniał jednak, że większość z nich dotyczyła zagranicy. Podkreślił jednak sprawę Najibullaha Zaziego. Mężczyzna został aresztowany w 2009 roku[43], dosłownie na kilka dni przed planowaną przez niego i jego znajomych serią samobójczych ataków w nowojorskim metrze.

Według Alexandra, Zazi wpadł w sidła w ramach „Operacji High-Rise”[44]. NSA odnalazło maile wysłane przez Zaziego wśród licznych wiadomości elektronicznych przesyłanych pomiędzy Stanami Zjednoczonymi a Pakistanem. Agencja monitorowała za pomocą dragnetu stworzonego w ramach programu PRISM, przemiatającego e-maile przychodzące do Stanów Zjednoczonych z zagranicznych źródeł.

Pośród korespondencji, NSA znalazła numer telefonu. Wykorzystano

wówczas dragnet ustanowiony na mocy ustawy Patriot Act[*9], przemiatający wszystkie połączenia realizowane z obszaru Stanów Zjednoczonych, w celu zlokalizowania wszystkich innych numerów, z którymi łączył się ten znaleziony. „Odkryliśmy, że Zazi rozmawiał z człowiekiem w Nowym Jorku, który miał powiązania z innymi członkami siatki terrorystycznej, „poinformował generał Alexander.

Kiedy powiadomiono Federalne Biuro Śledcze (FBI), jego agenci użyli tradycyjnych technik ścigania[45]. Śledzono Zaziego podczas podróży z jego domu w Kolorado do Nowego Jorku. Kiedy dotarł na miejsce, FBI poprosiło władze portowe by zatrzymały podejrzanego przy wjeździe na most Jerzego Waszyngtona, ale niczego nie znaleziono w jego samochodzie. Zaziemu pozwolono jechać dalej, jednak wyraźnie nadzór go spłoszył. Parę dni później poleciał z powrotem do Denver[46], nie wdrażając swojego planu w życie.

Został aresztowany w Kolorado[47], a po pewnym czasie przyznał się do stawianych mu zarzutów, wśród których wymienić można spiskowanie w celu użycia broni masowego rażenia oraz udzielanie finansowego wsparcia Al-Kaidzie. Nie został jeszcze skazany.

Nie jest jednak pewne czy rząd potrzebował dragnetów, by złapać Zaziego. Jeśli utrzymywał on kontakt e-mailowy z terrorystami będącymi pod nadzorem, nakaz przeszukania wystarczyłby do przechwycenia jego korespondencji. Podobnie z numerem telefonu – kiedy zostałby zidentyfikowany, sędzia najpewniej zgodziłby się na udostępnienie jego bilingów.

Zapytany przez Senat, czy wykorzystanie dragnetów było „kluczowe" dla schwytania Zaziego, generał Alexander udzielił wymijającej odpowiedzi[48]. Powiedział, że bilingi *nie* były kluczowe, nie wspomniał zaś nic o znaczeniu dragnetów przemiatających e-maile. Nawet prezydent Obama formułował ambiwalentne wypowiedzi[49], gdy opisywał wykorzystanie dargnetów NSA w polowaniu na Zaziego. „Mogliśmy go złapać w jakiś inny sposób", powiedział w wywiadzie telewizyjnym przeprowadzonym przez Charliego Rose'a. „Jednak na krańcach rozkładu prawdopodobieństwa, zwiększamy nasze szanse na zapobieżenie tego typu katastrofom dzięki użyciu tych programów".

Czy masowa inwigilacja jest tego warta, jeśli nawet jej najzagorzalsi obrońcy mogą wyłącznie powiedzieć, że „przyczynia się ona do zrozumienia" przypadków „o krańcowym prawdopodobieństwie"?

* * *

Dragnety to broń obosieczna. Gdy agencje wywiadowcze znajdują trop, ale nie sprawdzają go dokładnie, często obarcza się je winą za dopuszczenie do ataku. Tak było w przypadkach „majtkowego zamachowca", strzelca z Fort Hood czy zamachowców z maratonu w Bostonie. Wszyscy sprawcy zostali zidentyfikowani jako potencjalni sprawcy zagrożenia terrorystycznego jeszcze zanim doszło do ataków.

W swojej książce pod tytułem *Enemies Within: Inside the NYPD's Secret Spying Unit and bin Laden's Final Plot Against America*, dziennikarze Matt Apuzzo i Adam Goldman opisują[50], krok po kroku, kompromitację nowojorskiej policji, której – pomimo prowadzenia masowej inwigilacji muzułmanów – nie udało się złapać Najibullaha Zaziego i jego przyjaciół, gdy w dzielnicy Queens knuli swój terrorystyczny spisek. Policyjni „węszyciele" sprawdzili restauracje w okolicy miejsca zamieszkania Zaziego, jego meczet a nawet biuro podróży, w którym kupował bilety lotnicze do Pakistanu. „Po latach węszenia, nowojorska policja wiedziała, gdzie są nowojorscy muzułmanie, ale nie miała pojęcia, gdzie są terroryści", napisali Apuzzo i Goldman.

Ojciec Umara Farouka Abdulmutallaba[51], „majtkowego zamachowca", ostrzegał amerykańską ambasadę w Nigerii przez radykalnymi poglądami swego syna, a także informował o jego zniknięciu i możliwej podróży do Jemenu. Śledztwo prowadzone na zlecenie Białego Domu[52] wykazało, że „liczne agencje" weszły w posiadanie informacji na temat Abdulmutallaba przed planowanym atakiem, ale nie umieściły go na swoich listach obserwacyjnych.

Biuro terenowe FBI monitorowało korespondencję strzelca z Fort Hood[53], Nidala Malika Hassana, z radykalnym klerykiem islamskim Anwarem al-Awlakim, jednak nie podjęło działań, dopóki nie otworzył ognia w bazie wojskowej. Z kolei przyszły zamachowiec z maratonu w Bostonie, Tamerlan Carnajew, znalazł się w bazie danych Krajowego Centrum ds. Antyterroryzmu (National Counterterrorism Center) co najmniej na rok przed atakiem[54].

Niektóre badania sugerują, że gromadzenie olbrzymich ilości danych po prostu nie może zwiększyć zdolności przewidywania tak rzadkich wydarzeń, jakimi są zamachy terrorystyczne. Opublikowana w 2006 roku

praca autorstwa Jeffa Jonasa[55], naukowca z IBM, oraz Jima Harpera, dyrektora ds. polityki informacyjnej w Cato Institute, zawiera konkluzję, że przypadki terroryzmu nie są wystarczająco powszechne, by prawodpodobieństwo ich wystąpienia dało się „wykopać" w olbrzymich zbiorach danych.

Przecież Zazi kupował zmywacz do paznokci, żeby zbudować ładunek wybuchowy na podstawie acetonu, Abdulmutallab zaszywał materiały wybuchowe w bieliźnie, zaś Hasan wysyłał maile do swojego idola al-Awlakiego. Każde z tych zdarzeń miało swoją charakterystykę. Dla porównania, analizowanie danych w poszukiwaniu pewnych schematów działania, jest skuteczne w zwalczaniu przestępstw takich jak kradzież numerów kart kredytowych czy ubezpieczeń. Wystawcy kart kredytowych tworzą „czerwone flagi"[56] – oznaczając nimi m.in. transakcje dokonywane zagranicą. Mogą one uprzedzać przed ryzykiem oszustwa. „Terroryzmu nie da się ująć w modele prognostyczne, w sposób, w jaki umieszczamy w nich nawyki konsumpcyjne czy oszustwa finansowe. Nie jest bowiem tak powszechny", konstatują Jonas i Harper[57].

W 2008 roku Krajowa Akademia Nauk[58] skierowała dziesiątki ekspertów do zbadania potencjału wykopywania danych w celu walki z terroryzmem. Grupa ta doszła do podobnych wniosków. „Wysoce zautomatyzowane narzędzia i techniki nie mogą zostać w łatwy sposób zastosowane do rozwiązania złożonego problemu wykrywania i zapobiegania wystąpieniu ataków terrorystycznych. Być może osiągnięcie sukcesu w tej dziedzinie nie jest możliwe".

Niektórzy oficerowie wywiadu ironizowali na temat swej zdolności weryfikowania olbrzymich zbiorów danych celem przewidywania ataków. Przejawiali w tym względzie pesymizm. W 2012 roku, Matthew Olsen, dyrektor Krajowego Centrum ds. Antyterroryzmu powiedział, iż „jest szansa, że gdy dojdzie do kolejnego ataku, to po jakimś czasie dostrzeżemy w olbrzymiej ilości danych, do których mamy dostęp, jakąś wskazówkę lub trop, który do niego prowadził"[59].

Po zamachach podczas maratonu w Bostonie, komisarz tamtejszej policji, Ed Davis, poszedł nawet dalej, mówiąc w Kongresie[60], że więcej technologicznego nadzoru nic by nie dało. „Nie istnieje komputer, który wypluje z siebie imię i nazwisko terrorysty". Najlepsze tropy pochodzą natomiast od ludzi, którzy „ostrzegają organy ścigania, kiedy zauważą coś niepokojącego. To wtedy powinno się reagować. To powinien być

pierwszy krok”.

* * *

Jak więc możemy podsumować życie pod nadzorem?

Badania pokazują, że nadzór sprawowany przez człowieka lub choćby wrażenie bycia obserwowanym, budowane na podstawie zdjęcia ludzkich oczu czy widoku obsługiwanej przez człowieka kamery, może zmieniać zachowania, przyczyniając się do wyrabiania pozytywnych nawyków, takich jak sprzątanie po sobie naczyń w stołówce. Bywa, że pomaga zapobiegać przestępstwom przeciwko mieniu. Z drugiej strony, istnieją dowody na to, że latarnie uliczne mogą być równie skuteczne co kamery. Podobnie zdaje się, że świadomość wzajemności nadzoru przeciwdziałała destrukcyjnym siłom w czasie zimnej wojny.

Inwigilacja nie wydaje się być jednak dobrym narzędziem przewidywania zdarzeń takich jak ataki terrorystyczne. Wielu terrorystom udało się umknąć dragnetom. Nawet Stasi nie było w stanie przewidzieć upadku wschodnioniemieckiego reżimu w 1989 roku[61]. Zaś zalew danych płynących z masowego monitoringu może okazać się przytłaczający i zwieść tych, którym powierzono zadanie przemiatania ich w poszukiwaniu terrorystów.

Wszędobylska, niewidoczna inwigilacja wydaje się być jednak doskonałym narzędziem represji. Odkryto, że ludzie, którzy byli masowo, potajemnie monitorowani – czy to we Wschodnich Niemczech czy dla celów fińskiego badania – cenzurowali własne zachowania oraz to, co i jak mówili.

Pojawia się zatem pytanie: „Czy korzyści płynące z wszechobecnej, totalnej inwigilacji są warte życia w kulturze strachu?”.

4

WOLNOŚĆ STOWARZYSZANIA SIĘ

Yasir Afifi nie wierzy już w zbiegi okoliczności[1]. Gdy w czasie jazdy widzi dwukrotnie ten sam samochód, tężeje w napięciu i zastanawia się nad zmianą trasy. „Zbiegi okoliczności badam jak naukowiec", mówi.

Paranoja nie pasuje[2] do natury Yasira. Temperament ma pogodny, chód sprężysty. Zaledwie dwudziestotrzylatek, tryska wiecznym optymizmem urodzonego handlowca. Jednak odkąd odkrył, że jest inwigilowany przez Federalne Biur Śledcze (FBI), zachowuje się wyjątkowo ostrożnie.

Yasir wyprowadził się ze swojego kawalerskiego mieszanka – które dzielił z trzema przyjaciółmi – i ożenił z kobietą mającą dwie córki z poprzedniego małżeństwa. Spędza wieczory w domu, pomagając dziewczynkom odrabiać prace domowe. Zaprzestał używania Facebooka, poza graniem w kilka gier. „Jestem jednym z tych gości, którzy wierzą, że wszystko, co napiszesz *online* albo powiesz do telefonu, wędruje do jakiejś bazy danych", mówi Yasir[3].

Unika rozmów o polityce i religii. W pracy zaczął używać innego imienia, Aladdin, ponieważ nie chce, żeby jego szef wygooglał go sobie i zobaczył informacje o dochodzeniu prowadzonym przez FBI. Nie ma poczucia humoru, gdy chodzi o figle ocierające się o łamanie prawa. Mówi, że gdyby koledzy zrobili mu primaaprilisowy żart, powiedziałby im: „To, co mówicie nie jest prawdą i jest to nielegalne". „Nawet gdyby powiedzieli, że to tylko dowcip, odpowiedziałbym im: «Skasujcie mój numer»". Ocenia, że odciął się od około 90 proc. swoich byłych znajomych, którzy, jak mówi, „lubili sobie popić albo coś zażyć, a potem robić głupstwa". Rzadko rozmawia ze swoimi najlepszymi przyjaciółmi z dzieciństwa, którzy teraz piszą posty o paleniu marihuany i spędzają

wolny czas na graniu w gry wideo.

Podczas leniwego lunchu w hinduskiej restauracji z Yasirem i jego żoną, Angeliną Asfour, zapytałam ją, jak zmienił się od czasu, gdy zaczęto go inwigilować.

– W zasadzie jest taki sam. Tylko nie ma już tych samych znajomych – odpowiedziała[4].

A Yasir dodał:

– Stałem się naprawdę ostrożniejszy w kwestii tego, z kim się zadaję.

* * *

Kategoryzowanie ludzi poprzez ich przynależność do społecznej sieci jest ulubioną taktyką reżimów represyjnych. Stasi miało obsesję na punkcie wynajdywania u każdego związków z Niemcami Zachodnimi. Naziści – z żydowską krwią. Irańczycy mają ją na punkcie powiązań ze Stanami Zjednoczonymi[5], a Chińczycy z jakąkolwiek potencjalną opozycją wobec rządu[6].

Oto dlaczego wolność stowarzyszania się jest jednym z praw gwarantowanych przez Deklarację Praw Człowieka Organizacji Narodów Zjednoczonych[7], przyjętą po bestialstwach II wojny światowej.

Najogólniej rzecz biorąc, wolność stowarzyszania się oznacza, że ludziom nie można zabronić dołączania do grup ani, z drugiej strony, zmuszać ich do tego. W Stanach Zjednoczonych Pierwsza Poprawka do Konstytucji, chroniąca wolność wypowiedzi i swobodę zgromadzeń, gwarantuje również swobodę stowarzyszania się.

W roku 1958 Sąd Najwyższy orzekł[8], że próba uzyskania przez stan Alabamy listy członków Krajowego Stowarzyszenia Postępu Ludzi Kolorowych jest niezgodna z Konstytucją, ponieważ mogłaby ostudzić chęć członków do korzystania z wynikającego z Pierwszej Poprawki prawa do swobody stowarzyszania się, oraz że swoboda stowarzyszania się jest istotą wolności gwarantowanej przez Czternastą Poprawkę. „Ujawnienie danych szeregowych i funkcyjnych członków Stowarzyszenia naraziłoby ich na sankcje o charakterze ekonomicznym, utratę pracy, groźbę przymusu fizycznego i inne objawy publicznej wrogości", napisał w opinii większości sędzia John Marshall Harlan. „W tych okolicznościach uważamy za oczywiste, że przymusowe ujawnienie listy członków powoda pochodzących z Alabamy może niekorzystnie wpłynąć na zdolność

powoda i jego członków do realizacji ich wspólnych wysiłków zmierzających do promowania poglądów, które, co trzeba im przyznać, mają prawo wyznawać".

Jednak w dzisiejszym świecie idea ochrony tylko członków grup stanowi przestarzały sposób postrzegania swobody stowarzyszania się. Yasir wcale nie musiał przystępować do takiej grupy, jak Młodzi Muzułmańscy Mężczyźni z Santa Clara, żeby jego związki z nią zostały odnotowane przez władze. Na trop tych kontaktów naprowadził FBI jego cyfrowy ślad. Dalej FBI mogło już bez problemu się im przyglądać.

W istocie można dowodzić, że jedynym celem działania wielu technologii naszych czasów jest odkrywanie ukrytych związków. Spójrzmy na ludzi, którzy śledzą własne ruchy przy użyciu krokomierza Fitbit i innych przyrządów technicznych[9] – badają oni własne ruchy, aby lepiej zrozumieć ukryte powiązania. Może czują się lepiej, kiedy więcej chodzą?

Albo weźmy przykład mojego męża, który zainstalował w ścianach czujniki, aby monitorować nasze zużycie prądu, gazu i wody. On także próbuje wykryć pewne powiązania. I to działa: dziś już wiemy, że nasz toster zużywa niesamowicie dużo energii oraz że gwałtownie wzrasta u nas zużycie wody (składam to na karb długich kąpieli mojej córki, niemniej nie zgromadziliśmy jeszcze dotąd wszystkich danych, koniecznych, by to udowodnić).

Jestem zwolenniczką uczenia się na podstawie danych o sobie. Ale tę samą technologię, której używamy do monitorowania siebie, inni stosują do śledzenia nas i tworzenia naszych profili – zawierających o informacje o naszych upodobaniach i antypatiach oraz naszych powiązaniach.

W dzisiejszym świecie każdy wybór, jakiego dokonujemy, ma jakiś związek z osobą, miejscem albo ideą. Wejdźcie na stronę danej partii politycznej, a zostaniecie posądzeni o posiadanie konkretnych poglądów. Usiądźcie w restauracji obok kogoś, kto jest obserwowany, a wasz telefon komórkowy stanie się elementem „grupy interesów"[10], która może być obserwowana przez władze. Informacje o takich powiązaniach są skwapliwie gromadzone i trafiają do baz danych. Tam przygotowywane są prognozy waszych przyszłych zachowań.

Nawet orędownicy tak zwanego ruchu wielkich zbiorów danych [ang. *Big Data movement*] przyznają, że są to kwestie kłopotliwe. W swojej książce z 2013 roku, zatytułowanej *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Viktor Mayer-Schönberger

i Kenneth Cukier przekonują[11], że gdy wielkie zbiory danych coraz częściej wykorzystuje się do modelowania przyszłych ludzkich zachowań, trzeba ustanowić pewne środki bezpieczeństwa, co może wiązać się z koniecznością powstania nowej profesji „algorytmistów", przeprowadzających audyty wykorzystania Big Data. „Bez takich środków bezpieczeństwa może zostać podważona sama idea sprawiedliwości", piszą.

Nawet taki orędownik wielkich zbiorów danych jak Eric Schmidt, prezes firmy Google[12], przestrzega w napisanej wraz z Jaredem Cohenem książce *The New Digital Age*, że przybierające na sile zjawisko „praktycznie trwałego przechowywania danych" wprowadzi nas w erę, w której „ludzie będą obarczani odpowiedzialnością za swoje prawdopodobne, obecne i przeszłe, powiązania". Choć Schmidt i Cohen co do zasady są optymistami[13] i przekonują, że technologia wzbogaci życie obywateli, to jednak w rozdziale książki zatytułowanym „Państwo policyjne 2.0" ostrzegają: „Wszystko, czego władza mogłaby potrzebować do stworzenia niezwykle opresyjnego cyfrowego państwa policyjnego, jest już dostępne na rynku". W uścisku państwa policyjnego, jak piszą, „na tym poziomie monitoringu, termin *obwiniony przez skojarzenie* zyskuje zupełnie nowe znaczenie"[14].

* * *

Wydaje się, że inwigilacja Yasira Afifi zaczęła się od niewinnego pytania, dlaczego dezodorant nie mógłby przejść przez kontrolę bezpieczeństwa bagażu[15].

24 czerwca 2010 roku użytkownik internetowego serwisu społecznościowego Reddit.com, o nicku „JayClay", zamieścił pytanie: „A więc, skoro mój dezodorant mógłby być bombą, to dlaczego wyrzucacie go tak po prostu do kosza?"[16].

Jego post wygenerował setki komentarzy. Niektórzy użytkownicy Reddita nazywali zakaz przewożenia dezodorantów „teatrzykiem bezpieczeństwa". Inni chwalili się, że udało im się przemycić do samolotów obcinacze do paznokci, bambusowe igły, brzytwy czy noże. Jeden użytkownik zasugerował, że „łatwiejszym celem" byłoby wysadzanie galerii handlowej.

25 czerwca użytkownik o nicku „Khaledthegypsy" wtrącił: „wysadzenie

galerii handlowej wydaje się tak proste do zrobienia”[17]. I dodał: „bo wszystko, czego do tego trzeba, to bomba, zwykły ubiór, żeby nie wyglądać jak wariat w płaszczu, próbujący wysadzić sklep, i torba na zakupy. Bo, gdyby terroryzm był obecnie uzasadnionym zagrożeniem, to pomyślcie, ile pieprzonych galerii handlowych już by wyleciało w powietrze”.

Khaledthegypsy zakończył rodzajem żartu: „no tak... i teraz już pewnie jestem podsłuchiwany:/”.

Khaledthegypsy to w rzeczywistości Chalid Ibrahim, dziewiętnastoletni uczeń college’u w Santa Clara w Kalifornii, a także najlepszy przyjaciel Yasira Afifiego. Chalid nie sądził nawet, że trafił w punkt. Cztery miesiące później[18] przyjaciele pojechali razem zmienić olej w aucie Yasira, niebieskim sedanie Lincoln LS 2000. Gdy samochód był na podnośniku, Yasir zauważył zwisający z podwozia kabel. Był połączony z czymś, co wyglądało na doczepione pod spodem samochodu gigantyczne *walkie-talkie*.

– To nie jest część samochodu – powiedział Yasir do mechanika[19].

Kiedy mechanik szarpnął za urządzenie[20], szybko puściło, gdyż było przyczepione do podwozia za pomocą magnesu. Yasir pomyślał sobie: „Albo to jest bardzo przestarzały sprzęt do śledzenia, albo coś jakby rurobomba”[21].

Urodzony i wychowany w Santa Clara Yasir wyjechał do Egiptu ze swoim pochodzącym z Egiptu ojcem, kiedy miał dwanaście lat, po rozwodzie rodziców. Gdy skończył osiemnaście lat, powrócił do Stanów Zjednoczonych, aby pójść do college’u, znaleźć pracę i rozpocząć samodzielnie życie. Yasir i Chalid, którego rodzina to również Egipcjanie, jeszcze w podstawówce byli najlepszymi kolegami i odnowili znajomość, gdy ten pierwszy wrócił do USA.

Yasir opowiada, że krótko po tym, jak ponownie znalazł się w Stanach, pojawił się w jego drzwiach agent FBI i zostawił kartkę z prośbą o telefon[22]. Gdy chłopak zadzwonił pod wskazany numer, agent powiedział mu, że FBI chce z nim porozmawiać, bo „ma pochodzącą z anonimowego źródła informację, że Yasir może być zagrożeniem dla bezpieczeństwa kraju”. Ten odparł, że z przyjemnością odpowie na pytania, ale najpierw chce się skonsultować z prawnikiem.

Zadzwonił do firmy, świadczącej usługi prawne w ramach abonamentu. Poradzono mu, żeby nie spotykał się z agentem. Postanowił więc

zlekceważyć zaproszenie od FBI i zapomniał o sprawie. Rzucił się w wir pracy, polegającej na sprzedawaniu sprzętu komputerowego przedsiębiorstwom z Bliskiego Wschodu, oraz studiów w dziedzinie zarządzania biznesem.

Po tym jednak, jak odkrył urządzenie pod swoim samochodem, jego myśli znów wróciły do FBI. Wrzucił sprzęt na tylne siedzenie i pojechał do domu, opowiedzieć o tym współlokatorom.

Jeden z nich bał się, że to coś wygląda jak bomba. Yasir z kolei zastanawiał się, ile mógłby zarobić na sprzedaży urządzenia. Chalid, z natury bardziej podejrzliwy, zasugerował wywieszenie go w pierwszej kolejności na Reddit.com, żeby dowiedzieć się, co to w ogóle jest. I tak o godzinie 22.15 Chalid wgrał zdjęcie sprzętu z krótkim pytaniem: „Czy to znaczy, że śledzi nas FBI?”[23].

Jeszcze przed północą komentatorzy na Reddit zidentyfikowali urządzenie jako Guardian ST820 GPS, urządzenie do śledzenia produkowane przez Cobham, przedsiębiorstwo, które sprzedaje swoje produkty organom ścigania, koncentrując się wyłącznie na tym rynku. Krótko mówiąc: „Tak, śledzi was FBI albo policja”, jak napisał użytkownik „jeanmarcp.”.

Na początku Yasir był podekscytowany. Post znalazł się na stronie głównej Reddita. Ponad trzy tysiące ludzi skomentowało tekst. Porady płynęły z każdej strony. „Jest super”, myślał Yasir[24].

Następnego dnia jego ekscytacja zaczęła jednak słabnąć. Współlokatorzy Yasira powiedzieli mu, że na parkingu należącym do kompleksu apartamentowców stoją przy jego samochodzie kobieta i mężczyzna. Z pewną brawurą Yasir zszedł na dół na spotkanie z nimi. Wciąż stali obok jego samochodu, który był zaparkowany za elektronicznymi bramkami, kontrolującymi wstęp do jego kompleksu apartamentowców.

– Witam. Czy mogę w czymś pomóc? – zapytał Yasir. – Stoicie właśnie obok mojego samochodu

– Wie pan, że pana tablice straciły ważność – śmiejąc się, odpowiedział mężczyzna.

– A co to pana obchodzi? – spytał Yasir. – Odejdźcie proszę od mojego samochodu, gdy będę cofał.

Przez moment wydawało się, że Yasir zostawi obcych za sobą. Wyjechał z kompleksu apartamentowców i skręcił w lewo w ulicę. Tymczasem nagle usłyszał pisk hamulców i dostrzegł, jak doganiają go dwa ciemne SUV-y.

Jechały za nim przez pół przecznicy, po czym błysnęły światłami. W lusterku wstecznym zobaczył, że dołączył do nich także trzeci samochód – czarny Chevrolet Caprice.

Przejechawszy ledwie kilkadziesiąt metrów, Yasir zjechał na pobocze. Był przed szkołą podstawową znajdującą się po drugiej stronie ulicy, naprzeciw kompleksu apartamentowców. Do jego samochodu podeszło sześć osób – kobieta i mężczyzna, którzy stali już obok jego pojazdu, oraz czterech agentów w kamizelkach kuloodpornych i z pistoletami w dłoniach.

Żołądek Yasira dygotał, a ręce zrobiły się zimne. Starał się jednak być twardy. Agent przedstawił się jako „policja" i zapytał o jego nieważne tablice.

– I dlatego ta armia kazała mi się zatrzymać? – odpowiedział Yasir. Policjant zapytał, czy może przeszukać pojazd, na co Yasir odpowiedział, że tak. Jednak zamiast przeszukania, policjant poprosił Yasira o wyjście z samochodu i porozmawianie ze stojącymi za nim agentami FBI.

Yasir wysiadł, policjant przeszukał go na okoliczność posiadania broni, a potem pozwolił mu zbliżyć się do agentów FBI – tych samych, mężczyzny i kobiety, którzy stali wcześniej przy jego samochodzie. Mężczyzna przedstawił się jak Vincent, a kobieta jako Jennifer.

Vincent poprosił o zwrot urządzenia do śledzenia.

– Nie mam go – powiedział Yasir. – Skąd pan wie, że go nie sprzedałem?

Vincent grał twardego oświadczając, że sprzęt jest własnością federalną i grożąc postawieniem Yasirowi zarzutów[25].

– Proszę oddać nam sprzęt, inaczej może być pan aresztowany za utrudnianie działań wymiaru sprawiedliwości – ostrzegał Vincent. Yasir powiedział, że chce się skontaktować z prawnikiem, ale nie otrzymał odpowiedzi.

Jennifer grała tę sympatyczniejszą.

– My tylko chcemy dostać z powrotem nasz sprzęt[26], niech go nam pan odda i zostawimy pana w spokoju – powiedziała.

Yasir zasugerował, że może skontaktować z nimi swojego adwokata[27], aby ustalić szczegóły zwrotu sprzętu. To jednak tylko rozwścieczyło Vincenta, który krzyknął, że Yasir ma natychmiast oddać urządzenie.

– Dlaczego mi to robicie? – zapytał Yasir[28].

Vincent wyciągnął kartkę papieru z postem Chalida na Reddit.com o wysadzeniu galerii handlowej.

– Oto, dlaczego pana śledziliśmy – powiedział Vincent.

– To dlaczego nie podłożyliście tego pod jego samochód? – spytał Yasir.

– Och, przecież jesteście codziennie razem – odpowiedział Vincent.

– No, a co myślisz o tym, co on napisał? – zapytała Jennifer.

– To takie głupie – powiedział Yasir. – Chalid to bardzo bystry chłopak, ale to, co napisał, było bardzo głupie... Ale dlaczego nie pójdziecie porozmawiać z nim?

W końcu jednak twardość Yasira zaczęła kruszeć w obliczu uzbrojonych mężczyzn. Zgodził się na zwrot urządzenia, które aktualnie leżało na stoliku w jego mieszkaniu.

Na oczach przyjaciół i sąsiadów Yasira, Jennifer i Vincent przeszli przez ulicę z powrotem do kompleksu apartamentowców. Za nimi szło czterech agentów z pistoletami[29]. Yasir wpuścił ich przez elektroniczną bramkę i weszli razem schodami do mieszkania na drugim piętrze.

Gdy Yasir otworzył drzwi, Vincent chciał wejść do mieszkania wraz z nim.

– Proszę odsunąć się od drzwi – powiedział Yasir.

Jego współlokatorzy oglądali akurat telewizję w salonie.

– Hej chłopaki, za drzwiami jest FBI – powiedział do nich Yasir i zanim w ogóle mieli szansę odpowiedzieć, chwycił urządzenie i wyniósł je na zewnątrz, aby oddać Vincentowi.

– Aresztujecie mnie? – spytał Yasir.

– Nie – odpowiedział Vincent. – Ale chcielibyśmy zadać panu jeszcze kilka pytań.

Teraz, kiedy nie miał już w rękach sprzętu do śledzenia, Yasir był ciekaw usłyszeć, jak intensywnie był monitorowany przez FBI, zgodził się więc na krótką rozmowę.

Wyszedł z nimi z powrotem do ich samochodów. Czterech agentów z bronią odjechało, zostawiając Yasira samego z Vincentem i Jennifer. Ona dała mu wizytówkę[30], przedstawiającą ją jako agentkę FBI Jennifer Kanaan.

Zaczęli teraz zasypywać go pytaniami, które zdawały się dotyczyć dżihadu.

Czy podróżował do Syrii, Iranu albo Afganistanu? Nie.

Czy kiedykolwiek przechodził zagranicą szkolenie wojskowe? Nie.

Czy jest religijny?

– Co piątek chodzę do meczetu – odpowiedział Yasir.

Jennifer zapisała w swoim notatniku: „Yasir Afifi nie jest zagrożeniem dla bezpieczeństwa narodowego” i pokazała mu kartkę. Teraz nadeszła jego kolej na zadawanie pytań.

– Skąd mam wiedzieć, że mnie wszędzie nie śledzicie? – zapytał.

Jennifer odpowiedziała mu po arabsku.

– Podoba mi się pana gust kulinarny – powiedziała.

Yasir zdębiał.

– Pani mówi po arabsku. To jakiś żart? – odrzekł.

Kontynuowała po arabsku.

– Wiemy, dokąd chodzisz, wiemy, co robisz, wiemy, że zabierasz swoją dziewczynę do Santana Row, czyli galerii handlowej w San Jose.

– Rety, co jeszcze wiecie? – zapytał Yasir.

– Wiemy, że masz nową pracę. Nasze gratulacje – powiedziała. – Wiemy, że za dwa tygodnie lecisz do Dubaju.

Yasir zamarł. O pracy rozmawiał tylko przez telefon, a o podróży do Dubaju tylko przez e-maile[31]. „A może wiesz też, jaki kolor mają moje bokserki?”, pomyślał.

– Jestem pewien, że podsłuchujecie moje rozmowy telefoniczne – powiedział.

– Tego nie mogę panu powiedzieć – odpowiedziała.

– Czy jeszcze kiedyś was zobaczę? Zamierzacie znowu mnie zatrzymać z tą swoją armią? – spytał Yasir.

– Niech się pan już o to nie martwi, jest pan nudny – powiedziała. – Prawdopodobnie nigdy już pan o nas nie usłyszy. I nie ma potrzeby kontaktowania się z prawnikiem.

Yasir postanowił nie skorzystać z rady FBI. Po odejściu agentów[32] przyjaciel skontaktował go z Radą ds. Stosunków Amerykańsko-Islamskich (CAIR), muzułmańskiego zespołu doradztwa prawnego.

2 marca 2011 roku prawnicy CAIR złożyli skargę w sądzie federalnym[33] dotyczącą między innymi tego, że zamontowane bez nakazu urządzenie do śledzenia naruszało prawa Yasira wynikające z Czwartej Poprawki, że zbieranie informacji o praktykach religijnych, którym się oddawał, naruszało prawa wynikające z Pierwszej Poprawki oraz że inwigilacja spowodowała „obiektywne ostudzenie tych jego działań, którym przysługuje ochrona przewidziana w Pierwszej Poprawce do Konstytucji USA”.

W skardze twierdził, że odczuwa teraz lęk[34], „gdy wyraża swoje

poglądy polityczne i podtrzymuje pewne, zupełnie uprawnione, wnioski", oraz że wskutek stosowanego wobec niego nadzoru „inni odwrócili się od niego, a szczególnie odnosi się to do firm oferujących perspektywiczną pracę".

Yasir nie tylko domagał się sądowego zakazu śledzenia go w przyszłości, ale także żądał usunięcia z archiwów państwowych danych o swojej lokalizacji.

FBI uzyskało prawo do utajnienia odpowiedzi na skargę Yasira[35]. W poufnej korespondencji Biuro twierdziło[36], że inwigilacja Yasira jest już zakończona oraz że śledzenie bez nakazu było w rzeczonym okresie prawnie dopuszczalne. (Od tamtej pory Sąd Najwyższy zdążył już stwierdzić[37], że nieakceptowalne jest naruszanie prawa przez agentów przy instalowaniu urządzeń do lokalizacji). Rząd argumentował[38] także, że Yasir nie potrafił podać żadnego konkretnego dowodu na to, że jego prawa wynikające z Pierwszej Poprawki miałyby być w przyszłości ograniczone: „Nie pokazał konkretnego, bezpośredniego przyszłego związanego z tym zagrożenia".

* * *

Pierwsza Poprawka do Konstytucji Stanów Zjednoczonych jest prawem negatywnym. Stanowi ona, czego robić nie można: „Kongres nie uchwali ustawy obejmującej ustanowienie religii lub zabraniającej swobodnego jej praktykowania ani też ograniczającej wolność słowa, prasy albo prawo ludzi do pokojowego gromadzenia się i wnoszenia do rządu petycji o naprawę krzywd"[39]. W rezultacie nie zawsze jest łatwo powiedzieć, czego Pierwsza Poprawka właściwie dotyczy. Szukając sposobu na przebrnięcie przez ten prawny gąszcz, usiadłam ze znanym wykładowcą, specjalizującym się w tematyce Pierwszej Poprawki, Lee Bollingerem, który jest również rektorem Uniwersytetu Columbia. „Teorię Pierwszej Poprawki można określić jako paranoję", twierdzi Bollinger[40]. Ojcowie-założyciele wierzyli, że funkcjonująca demokracja wymaga swobody w krytykowaniu rządu. W konsekwencji, ważnym testem jakiegokolwiek przypadku prawnego dotyczącego Pierwszej Poprawki jest to, czy dana działalność ogranicza udział w demokratycznej debacie?

Sąd Najwyższy jest niezwykle ostrożny w ograniczaniu jakiejkolwiek działalności, jeśli ewentualne restrykcje miałyby studzić chęć partycypacji

w demokracji. Na przykład w 1964 roku orzekł[41], że New York Times Company nie odpowiada za naruszenie wynikające z publikacji ogłoszeń, zawierających nieprawdę o urzędniku publicznym, ponieważ „zasada, według której krytyka działania urzędnika dozwolona byłaby tylko pod warunkiem prawdziwości wszystkich zawartych w niej stwierdzeń, prowadziłaby do czegoś przypominającego autocenzurę". A w 2000 roku Sąd Najwyższy orzekł[42], że organizacja Boy Scouts of America nie musiała przyjmować jako swego członka geja, ponieważ zmuszanie grupy do przyjmowania członków naruszałoby swobodę wyrażania chęci stowarzyszania się. „Pierwsza Poprawka chroni swobodne zrzeszanie się, zarówno wokół popularnych jak i mniej popularnych idei", napisał sędzia William H. Rehnquist.

Niemniej sąd nie otworzył się na argument, że inwigilacja szkodzi wolnemu społeczeństwu. W 1972 roku orzekł[43] w stosunku 5 do 4, że obywatele USA, którzy byli w ramach programu inwigilacji szpiegowani przez armię, nie są w stanie udowodnić szczególnych szkód, które ponieśli, a zatem brakuje „udziału osobistego jako rezultatu sporu", koniecznego, by można było zasądzić zadośćuczynienie. W 2013 roku Sąd Najwyższy ponownie orzekł w stosunku 5 do 4, że obywatele USA, którzy byli szpiegowani przez NSA w ramach programu nielegalnych podsłuchów, nie potrafili udowodnić, żadnej „konkretnej, szczególnej, już doznanej albo dopiero nadciągającej" szkody, którą należałoby wziąć pod uwagę[44].

A jednak byłam zaszokowana elokwencją odrębnego zdania sędziów Williama O. Douglasa i Thurgooda Marshalla w sprawie z 1972 roku. Nazwali oni wojskowy program inwigilacji „rakiem na politycznym ciele", który pozostaje „w stanie wojny z zasadami Pierwszej Poprawki do Konstytucji". Napisali: „jeśli oficer wywiadu spogląda w bibliotece przez ramię każdemu nonkonformiście albo idzie niewidzialny u jego boku w grupie pikietujących, albo infiltruje jego klub, to Ameryka, nazwana kiedyś wszem i wobec głosem wolności, ma coraz mniej wspólnego z wizją, jaką jej dali Jefferson i Madison, a coraz więcej z wizją rosyjską".

* * *

Po swojej utarczce z FBI Yasir i Chalid wpadali w panikę na widok każdego samochodu, który obok nich przejeżdżał. Strach jednak powoli

mijał, za to pojawiało się nowe uczucie: zgoda na bycie obserwowanym. „Co możesz zrobić?", powiedział mi Chalid, kiedy rok po tym wydarzeniu spotkaliśmy się w Starbucksie w Santa Clara[45]. „Tak czy owak, właśnie tracimy całą naszą prywatność. Technika nam ją zabrała".

Chalid wyjaśnił mi, co się stało po tym, jak FBI stanęło u drzwi Yasira. Kilka dni później agentka FBI Jennifer zadzwoniła na komórkę Chalida i zostawiła wiadomość. Nie oddzwonił do niej. Od tej pory, mówi, często dostaje telefony z zastrzeżonych numerów – gdy odbiera słyszy tylko świszczący głos. „Dzwonią do mnie dwa razy dziennie przez dwa dni, a potem przerwa na trzy tygodnie", powiedział mi.

Na początku przyglądał się podwoziu samochodu za każdym razem, gdy do niego wsiadał. Szybko jednak z tym skończył. Pomyślał, że gdyby FBI chciało chodzić za nim, to i tak znalazłoby jakiś sposób.

Jego posty coraz rzadziej pojawiały się na Reddit.com. Tam, gdzie zwykł był umieszczać sążniste traktaty przeciwko niesprawiedliwości, publikował teraz krótkie, niekontrowersyjne komentarze.

Chalid przestał też się kolegować z Yasirem. Kiedy użytkownicy Reddita zaczęli męczyć go o wieści w sprawie śledzenia z pomocą GPS-u, Chalid napisał: „Okazał się głupim porąbańcem, więc się rozstaliśmy"[46].

Gdy spotkał się ze mną, właśnie wrócił z pobytu w Egipcie i mówił mi, że myśli o wyjeździe na stałe[47]. Powiedział, że ludzie w Stanach Zjednoczonych są zbyt ugodowi, gdy widzą, jak ich prawa odpływają w siną dal. „Tu jest tylko iluzja wolności", mówił. „Tam jest prawdziwa wolność. Możesz robić, co chcesz".

* * *

Ciężko było mi się spierać z Chalidem i namawiać go do optymizmu w kwestii wolności. Niestety od czasu ataku Al-Kaidy na Stany Zjednoczone 11 września 2001 roku, muzułmanie w Ameryce są często traktowani przez policję jako podejrzani.

Po 11 września FBI ustanowiło system „zarządzania terytorium" [ang. „*domain management*"], by za pomocą danych handlowych ustalić, gdzie żyją muzułmanie i skierować do ich społeczności informatorów[48]. Nie było niespodzianką, że natychmiast wzrosła liczba postępowań przeciwko muzułmanom w sprawach o terroryzm. Dziennikarz śledczy Trevor Aaronson przebadał 508 takich postępowań wszczętych przez FBI

po atakach z 11 września i stwierdził, że niemal w połowie przypadków korzystano z informatorów, a w dwóch trzecich stosowano także prowokacje[49]. Aaronson twierdził, że informatorzy często kierują się do podatnych, zdesperowanych ludzi i nakłaniają ich do dołączenia do fałszywego spisku terrorystycznego. „Nie było jeszcze prowokacji wobec ludzi, którzy mieli broń", mówi Aaronson. „Jest niemal powszechne, że to FBI dostarcza wszystkie środki".

Jedna z bardziej agresywnych akcji śledzenia muzułmanów prowadzona była w Nowym Jorku[50]. Nowojorska policja podjęła tajną współpracę z Centralną Agencją Wywiadowczą (CIA), by prowadzić infiltrację kół politycznych, dzielnic, imprez i grup studenckich na terenie miasta oraz w New Jersey. Muzułmańskim studentom z City College of New York towarzyszył w 2008 roku w spływie górskim agent pod przykryciem[51]. W roku 2009 tajni agenci z policji nowojorskiej utworzyli „dziuplę" niedaleko Rutgers University w New Jersey, ale ta ich przykrywka padła, gdy dozorca budynku zaczął podejrzewać, że to komórka terrorystyczna, i zadzwonił po policję.

Przyjrzyjmy się historii Asada Dandii, dwudziestoletniego studenta z Nowego Jorku, który był śledzony przez informatora policji nowojorskiej[52]. W roku 2011 Dandia był współzałożycielem organizacji charytatywnej o nazwie Fesabeelillah Services of NYC, która zbierała pieniądze na dożywianie bezdomnych i potrzebujących. W marcu 2012 roku skontaktował się z nim na Facebooku człowiek o nazwisku Shamiur Rahman, który powiedział, że chce się włączyć w działalność dobroczynną. „Mieliśmy wielu wspólnych przyjaciół i byłem szczęśliwy, że mogę mu pomóc w jego walce o religijne samodoskonalenie, więc przedstawiłem go moim przyjaciołom w FSNYC", napisał Dandia na swoim blogu opisującym inwigilację.

Rahman i Dandia, którzy byli mniej więcej w tym samym wieku, stali się bliskimi przyjaciółmi. Rahman wiele razy odwiedzał dom rodziców Dandii, a kiedyś spędził tam nawet noc. Był też dość wścibski. „Rahman prosił wszystkich, których spotkał, o numer telefonu, nierzadko już chwilę po spotkaniu", pisał Dandia. „Często także próbował robić sobie zdjęcia z ludźmi, których spotkał dzięki mnie, albo wręcz zdjęcia samych tych ludzi".

2 października 2012 roku Rahman umieścił na Facebooku wiadomość, że jest informatorem policji nowojorskiej[53]. Później powiedział prasie,

że został nim po tym, jak został kilkakrotnie zatrzymany za posiadanie małych ilości marihuany. Za swoje usługi pobierał tysiąc dolarów miesięcznie. Ale Rahman w końcu zmęczył się szpiegowaniem przyjaciół i porzucił to.

„Nienawidziłem tego, że wykorzystywałem ludzi do zarabiania pieniędzy", powiedział agencji Associated Press. „Popełniłem błąd".

Ujawnienie się Rahmana zszokowało jego przyjaciół. „Kiedy się o tym dowiedziałem, zmroziło mnie", napisał Dandia na swoim blogu[54]. „To było przerażające uczucie. Nie mogłem uwierzyć, że w moim domu był informator policji nowojorskiej. Incydent rzucił także podejrzenie na jego organizację charytatywną, która została teraz przemianowana na Muslims Giving Back. Lokalny meczet poprosił Dandię o wstrzymanie organizacji spotkań dobroczynnych w meczecie oraz działań polegających na zbieraniu datków od wiernych. „Instytucja cierpiała finansowo i emocjonalnie", mówi Dandia. On i inni członkowie zaczęli zamazywać swoje twarze na fotografiach, które umieszczali na facebookowej stronie instytucji. Dandia dołączył do pozwu przeciwko policji nowojorskiej[55].

„Kiedyś w odniesieniu do mojej działalności charytatywnej próbowałem być tak otwarty, jak to tylko możliwe – teraz kontaktuję się głównie z ludźmi, których znam osobiście", napisał Dandia.

* * *

Yasir Afifi także wycofał się za mur ochronny[56]. Już nie zadaje się ze swoim przyjacielem z dzieciństwa Chalidem. Jest zajęty pracą sprzedawcy oprogramowania i uczęszczaniem na kursy wieczorowe. Kończy college. Zaoszczędził na kupno domu, a jego żona jest w ciąży. „Gdy ty już dorosłeś, a twój najlepszy przyjaciel nie, ciężko jest się kolegować", wyjaśnił mi. „W tym momencie mojego życia, zadawanie się z nim byłoby kompletną stratą czasu".

Yasir nie może sobie pozwolić na ryzyko. Wierzy, że wciąż jest na jakiejś liście obserwacyjnej. Gdy on i jego żona wrócili w roku 2012 z podróży do Puerto Vallarta w Meksyku, był po przyjeździe przesłuchiwany przez blisko godzinę, a agenci federalni przeszukiwali jego bagaże i zadawali pytania. Mówił, że agenci zabrali telefon jego żony, ale on odmówił im oddania swojego.

„Zadawali pytania, których nie mieli prawa zadawać. Zapytali moją

żonę, dlaczego odeszła od swojego poprzedniego męża", opowiedział mi. „Byłem taki wściekły".

Niemniej stara się utrzymywać swój gniew pod kontrolą.

„Czy chciałbym, aby podjęto jakieś działania, które zatrzymałyby nękanie amerykańskich muzułmanów? Tak!", mówił mi, gdy staliśmy w tym samym miejscu, w którym został zatrzymany przez FBI[57]. „Czy chciałbym, żeby przysłali mi przeprosiny za włożenie tego [urządzenia GPS do śledzenia] do mojego samochodu? Tak, ale to są sprawy ode mnie niezależne. Żyję dalej. Chcę być bogaty. Chcę mieć porządną rodzinę. Chcę amerykańskiego snu. Chcę, żeby inni też to mieli".

Rok po tej rozmowie Yasir zrealizował swój sen. Wraz z żoną kupili dom w południowym San Jose w Kalifornii. Pewnego upalnego dnia odwiedziłam go, wjeżdżając swoim wypożyczonym samochodem w jego jednokierunkową uliczkę[58]. Zaparkowałam obok małego basenu dla wszystkich domów w sąsiedztwie.

W salonie Yasir pokazał mi zupełnie nowy skórzany komplet kanapowy, kolorowe prześcieradła i zasłony w sypialni dziewczynek. Na malutkim trawniku stał rozstawiony grill.

Gdy chodziłam po domu, wciąż myślałam o swoich krewnych, którzy wyemigrowali z Rosji do Stanów Zjednoczonych na przełomie XIX i XX wieku. Uciekali od świata, gdzie Żydzi byli prześladowani za wiarę.

Wycierpieli wiele, żeby się tu dostać – moja prababka wykonywała morderczą pracę w fabryce, mój pradziadek był ulicznym domokrążcą.

Rodzina Yasira przybyła do Stanów Zjednoczonych z Egiptu, z przyczyn ekonomicznych. Yasir ciężko pracował i osiągnął tutaj finansowy sukces. Ale nie posmakował tak wielkiej swobody, jaką mu obiecywano. Zamiast tego zaczął cenzurować sam siebie i powstrzymywać się od zrzeszania się.

Yasir cieszy się za to swobodą grillowania i możliwością kupna skórzanych kanap oraz domu na kredyt, ale już nie wolnością utrzymywania kontaktów z ludźmi, którzy opowiadają dowcipy o rządowych zakazach wnoszenia dezodorantu do samolotu.

5

MODELE ZAGROŻEŃ

W świecie, w którym niemal wszystko jest monitorowane, łatwo jest poczuć się bezradnym, gdy chodzi o prywatność. Gdy mówię napotkanym osobom, że piszę o prywatności, często ich natychmiastową reakcją jest: „Ja już się poddałem. Prywatność umarła”.

Ja także w pewnym sensie się poddałam. Przez trzy lata pisałam o inwazji na prywatność, jaką umożliwił rozwój techniki, a jednocześnie nie zrobiłam wiele, by chronić siebie samą. Wmawiałam sobie, że to dlatego, że byłam zbyt zajęta, w rzeczywistości jednak byłam przytłoczona pewnym imposybilizmem. Po odbyciu wielu takich rozmów, spadło na mnie poczucie winy. Czy sposób, w jaki opisuję inwazję na prywatność, nie buduje takiego właśnie poczucia beznadziei?

Jestem z natury optymistką: chciałam wierzyć, że istnieje dla nas nadzieja. Jestem także od urodzenia przekorna: chciałam więc przekonać wątpiących. Wreszcie jestem uparta: założyłam, że uda mi się wykrzesać jakąś nadzieję.

Postanowiłam więc, wbrew wszelkim przeciwnościom, spróbować wymknąć się spod kontroli dragnetów. Pomyślałam, że będę unikać monitoringu podczas wykonywania codziennych zajęć, takich jak zakupy czy czytanie. Że zaciemnię nieco moje miejsce zamieszkania – w domu i na zewnątrz. Że opatrzę moje e-maile i teksty cyfrowym odpowiednikiem laku. Że znajdę sposoby na swobodne utrzymywanie kontaktu z ludźmi i hołdowanie pewnym ideom. Że, w końcu, spróbuję wynaleźć sposoby chronienia moich dzieci przed zostawianiem cyfrowego śladu w sieci. Takiego, który mógłby objawić się znienacka w ich późniejszym życiu.

Zadanie było onieśmielające.

„Nie dam rady tego zrobić”, powiedziałam bliskiemu przyjacielowi. „Jak

będę żyć bez karty kredytowej? Bez telefonu komórkowego? To byłoby nieodpowiedzialne względem moich dzieci".

Uświadomiłam sobie jednak, że moje pytania były właśnie tym, co miałam zbadać: „Czy da się żyć w nowoczesnym świecie i jednocześnie wymknąć się kontroli dragnetow?", „Czy w jakimś sensie nie pogodziłam się już z wszechobecną inwigilacją, wymieniając moje dane na darmowe usługi albo większe bezpieczeństwo – o co tak zabiegają związani z branżą nadzoru?", „Co by się stało, gdybym spróbowała wycofać zgodę na zbieranie danych o mnie?".

* * *

Pierwszym krokiem była identyfikacja zagrożeń mojej prywatności.

W branży bezpieczeństwa cyfrowego identyfikowanie swoich przeciwników nazywane jest tworzeniem własnego „modelu zagrożeń" [ang. *threat model*][1]. Idea jest taka, że obronić się można tylko przed znanymi zagrożeniami. Ekspert w tej dziedzinie, Bruce Schneier, nazywa to pierwszą lekcją bezpieczeństwa: bezpieczeństwo jest handlem[2]. „Nie istnieje coś takiego jak absolutne bezpieczeństwo", napisał we wstępie do swojej książki *Schneier on Security*. „Życie niesie z sobą ryzyko, a bezpieczeństwo wymaga kompromisów. Dostajecie więcej bezpieczeństwa, bo rezygnujecie z czegoś: z pieniędzy, czasu, wygody, możliwości, wolności itd.". To, z czego rezygnujecie, zależy od tego, co i przed kim chcecie chronić.

Skupienie się na niewłaściwym adwersarzu może zakończyć się katastrofą. Spójrzmy na przypadek generała Davida Petraeusa, byłego dyrektora Centralnej Agencji Wywiadowczej (CIA).

W roku 2012 Federalne Biuro Śledcze (FBI) nakryło generała na stosowaniu mało wysublimowanych metod ukrywania romansu pozamałżeńskiego z jego biografką, Paulą Broadwell[3]. Krytycy ostro potępili go za używanie wspólnego konta Gmail, w którym on i pani Broadwell zostawiali sobie e-maile w folderze z dokumentami roboczymi – magazyn „Foreign Policy" nazwał to „starą szkołą szpiegowską". Jednak prawdziwym problemem było to, że generał niewłaściwie określił swojego przeciwnika.

On i jego kochanka próbowali ukryć romans przed swoimi małżonkami. W takim przypadku wspólne konto Gmail, do którego logowali się

z komputerów znajdujących się poza domem, zdawało się być wystarczającą ochroną. Nie przewidzieli jednak, że FBI zacznie śledzić Broadwell w związku z e-mailami z pogróżkami, które zaczęła otrzymywać pewna, mieszkająca w Tampie na Florydzie, organizatorka firmowych wyjazdów integracyjnych nazwiskiem Jill Kelley. FBI uzyskała adresy IP, z których wysyłano owe e-maile, najprawdopodobniej na skutek wezwania przesłanego do administratora poczty internetowej należącej do Broadwell. Agenci FBI śledzili pojawianie się tych adresów w rozmaitych punktach z publiczną siecią Wi-Fi, w tym w wielu hotelach[4]. Następnie analizowali listy gości hotelowych, według dat, w których wysyłano e-maile. Śledczy szybko się zorientowali, że częstym gościem hoteli w tych właśnie terminach była Paula Broadwell. Stąd już tylko krok dzielił ich od przejrzenia jej e-maili – z wykorzystaniem nakazu przeszukania lub sądowego wezwania – i odkrycia jej romansu z Petraeusem.

Gdyby generał i jego kochanka chcieli przechytrzyć FBI, musieliby co najmniej podjąć kroki zmierzające do zamaskowania adresów IP, z których logowali się na swoje konta, do szyfrowania wiadomości i upewnienia się, że konta założone są na fikcyjne nazwiska. Nawet wtedy jednak nie byłoby gwarancji, że nie zostaliby złapani[5].

Prywatność doskonała nie jest przecież możliwa, nawet jeśli prawidłowo zidentyfikujecie swojego przeciwnika.

Spójrzmy na inny przykład: Theodore J. Kaczynski, czyli Unabomber[6]. Przez dekadę żył on jak pustelnik w jednoizbowej chatce – bez elektryczności, kanalizacji czy telefonu – znajdującej się na odludziu w stanie Montana. Zarazem, za pomocą poczty, dokonywał wielu zamachów bombowych, w których zabił trzy i ranił dwadzieścia dwie osoby. Ale nawet ten pustelnik nie był w stanie wiecznie uchodzić FBI, które w końcu wyśledziło go w jego chacie, w dużej mierze za sprawą jego brata[7]. Podał on bowiem służbom pomocną dłoń, dostarczając im tekst Kaczynskiego, napisany przez niego w młodości. Dzięki temu można było dokonać analizy porównawczej jego stylu.

I to jest akurat pozytyw: społeczeństwo skorzystało na tym, że FBI złapało Kaczynskiego i zakończyło jego bombowe szaleństwo.

* * *

Jaki jest mój model zagrożenia?

Jestem aktywną dziennikarką, mam syna w wieku przedszkolnym i córkę będącą uczennicą szkoły podstawowej. Mój mąż jest profesorem, który dla celów badawczych często podróżuje na inne kontynenty.

Gdybym miała opisać moją rodzinę jednym krótkim słowem, byłoby to: „zajęta". Ciągle biegamy w różnych kierunkach. A prywatność i bezpieczeństwo są akurat tymi rzeczami, które umykają uwadze, gdy żyje się w ciągłym pośpiechu.

Mimo to chcę uchronić siebie i moje dzieci od przypadkowej inwigilacji. Chcę dla nas swobody zrzeszania się i wiązania z pewnymi miejscami i ideami, bez konieczności zamartwiania się o to, jak może to ograniczyć nasze perspektywy.

Chcę także uchronić siebie przed zagrożeniami czyhającymi na dziennikarzy. Przecież administracja Obamy była nadzwyczaj agresywna w prześladowaniu ludzi, którzy przekazywali poufne materiały dziennikarzom. Od roku 2009 oskarżyła ośmiu rządowych informatorów o naruszenie ustawy o szpiegostwie[8], tj. prawa, które w ciągu ostatnich 92 lat było użyte tylko trzy razy przeciwko urzędnikom państwowym, oskarżonym o dostarczanie tajnych informacji dziennikarzom[9].

Moje obawy dotyczą zresztą mojej sytuacji, jako że dziennikarze zwykle jednak nie kończą w więzieniu. Martwi mnie jednak, że ludzie, którzy dokonują przecieków do prasy, często trafiają za kraty. Chciałabym móc obiecać moim informatorom, że zachowam ich dane w tajemnicy i być pewnym, że dotrzymam danego słowa.

Zatem mierzę się z dwoma zagrożeniami: powszechnego śledzenia i ukierunkowanych ataków na dziennikarzy i ich źródła.

* * *

Kiedy tworzy się model zagrożenia, ważne jest także określenie swoich mocnych i słabych stron.

Moją siłą jest to, że piszę o prywatności i technologiach od wielu lat, a więc mam do dyspozycji armię ekspertów, do których mogę zadzwonić po pomoc i radę. Szczęśliwie nie muszę „wyczyścić" żadnych prywatnych spraw. Kilka lat temu, kiedy została opublikowana moja książka o sieci społecznościowej MySpace, poświęciłam trochę czasu, aby uczynić moją internetową reputację kuloodporną. Rozmawiałam z konsultantami

do spraw pozycjonowania, a oni pomogli mi stworzyć stronę internetową i oczyścić moje profile w sieciach społecznościowych, tak żeby wśród rezultatów wyszukiwania mojego nazwiska w Google, pojawiało się raczej to, co sama napisałam o sobie, niż to, co napisali o mnie inni.

Moje dzieci są jeszcze małe, a ich dane nie są publicznie dostępne. Nie mają telefonów komórkowych, dostępu do komputera, ani żadnych kont w mediach społecznościowych (poza tym, które szkoła mojej córki utworzyła dla niej w ramach zamkniętej strony internetowej). Mają za to ograniczony dostęp do iPada. W ich przypadku nie było więc czego „czyścić".

Mam jednak mnóstwo słabych stron. Prawdopodobnie najistotniejszą jest niecierpliwość[10]. Często chodzę na skróty, zamiast zastanowić się nad tym, dlaczego moje narzędzia technologiczne nie działają prawidłowo. Przez to bywam podatna na zagrożenia.

Kolejna ważna kwestia: mój adres zamieszkania jest powszechnie znany. Kiedy mój mąż i ja kupiliśmy i wyremontowaliśmy dom, uległam namowom kolegów z „Wall Street Journal" i na blogu w serwisie *online* poświęconemu nieruchomościom relacjonowałam postępy w renowacji. Choć nigdy nie opublikowałam dokładnego adresu domu, przynajmniej jeden bloger zidentyfikował go na podstawie fotografii[11]. W konsekwencji ten istotny składnik mojej prywatności zniknął.

Mój mąż także nie dba o prywatność. Jest profesorem i zwykle żartuje, że jeśli ktoś włamie się do jego plików, to liczba czytelników jego dokumentów wzrośnie dwukrotnie. Nie tylko nie troszczy się o swoją prywatność, ale wręcz zajmuje się zawodowo tym, co prywatność narusza. Jest inżynierem-mechanikiem, a jednym z jego projektów jest instalowanie czujników do monitorowania poboru energii. W istocie, bez pytania mnie o zdanie, zainstalował takie sensory nawet w naszym domu. Dowiedziałam się tym dopiero w dniu, w którym się wprowadzaliśmy. Zastałam w nim jednego ze studentów męża, który właśnie kończył podłączanie systemu.

Aparatura, do monitorowania zużycia energii, którą zainstalował, jest właściwie całkiem w porządku – możemy zobaczyć, jak dużo energii wykorzystujemy w danym okresie i zrozumieć nasze wzorce zużycia. Oczywiście, czuję się trochę dziwnie, że obserwują to także studenci męża.

– Co wy robicie w piątki? – zapytał go pewnego dnia jeden z nich. – Zużycie energii zawsze skacze wam w piątki.

Okazuje się, że chodzi o pomoc do sprzątania, która przychodzi do nas w tym dniu i uruchamia odkurzacz.

Moje dzieci także nie dbają o prywatność. Dla nich „prywatność" to słowo, które znaczy tyle, co „nie". To przez prywatność nie mogą umieszczać filmów wideo na YouTube. To przez prywatność nie pozwalam im zapisywać się do dziecięcych sieci społecznościowych. To przez prywatność skarżę się ich nauczycielom na wstawanie zdjęć z nimi na niechronione hasłami blogi.

Moja córka właściwie myśli, że prywatność to coś, co trzeba zwalczać. Uwielbia podejmować próby odgadywania moich haseł. Kiedyś dostała się tak do mojego iPhone'a, zmieniła moje hasło i zupełnie zapomniała tego nowego. Odcięła mnie od telefonu. Żeby ponownie uzyskać dostęp do urządzenia, musiałam wykonać reset.

Wiedziałam więc, że będę toczyć tę walkę sama, przynajmniej na odcinku domowym. Towarzyszyć mi w tym będzie rachityczna sieć techników, hakerów i zatroskanych obywateli całego świata.

* * *

Potrzebowałam planu bitwy, żeby wiedzieć, jak się bronić. I musiałam określić, jak głęboko chcę się skryć. Czy chcę żyć w bunkrze? Czy chcę zmienić nazwisko?

Przeczytałam kilka książek o ochronie prywatności i zawierały one dość radykalny program. W *How to Be Invisible: Protect Your Home, Your Children, Your Assets, and Your Life* J.J. Luna pisze, że „wasza podróż do niewidzialności musi zacząć się od tego pierwszego kroku: oddzielenia waszego nazwiska od adresu domowego"[12]. Jeśli zatem wasz adres jest już publicznie znany, Luna radzi się wam wyprowadzić.

Proponuje on założenie w Nowym Meksyku spółki z o.o., która będzie właścicielem waszych aktywów – samochodu, domu itd. Dalej sugeruje, że nie możecie posyłać dzieci do szkoły publicznej, ponieważ to może zdradzać wasze miejsce zamieszkania. „Istnieją tylko dwa sposoby, by temu zaradzić", pisze. „Edukacja domowa albo szkoła prywatna. O ile oczywiście, chcecie zapewnić dzieciom prywatność".

Nie stać mnie na umieszczenie moich dzieci w szkole prywatnej ani na rzucenie pracy i uczenie ich w domu. Nie chcę nawet słyszeć o takich pomysłach.

Model zagrożenia prywatności według Luny? Prywatni detektywi. Bo nawet jeśli zastosujecie się do wszystkich jego rad, prywatny detektyw, jeśli będzie dysponował nieograniczonym funduszem, wciąż będzie w stanie was wyśledzić.

W książce *One Nation, Under Surveillance* Kenneth W. Royce, ukrywający się pod pseudonimem Boston T. Party, pisze, że „prawo już nie działa, gdyż Ameryka oddzieliła się od trzonu swojego prawa”[13]. Radzi czytelnikom gromadzić karabiny, powiększać zapasy żywności, uczyć dzieci w domu i uruchamiać komputery z płyty CD z systemem operacyjnym Puppy Linux. W jego modelu zagrożenia najważniejszy jest rząd. Royce uważa, że jest gotowy w każdej chwili uderzyć w obywateli.

Nie jestem aż taką paranoiczką. Nie wierzę, że rząd to przegrana sprawa. Za to ciągle wierzę w system prawny i w to, że nasz układ kontroli i równowagi funkcjonuje całkiem nieźle. Nie jestem gotowa na gromadzenie broni i budowanie zapasów żywności (oprócz niewielkiej ilości pomidorów i bazylii w przydomowym ogródku każdego lata). I nie planuję edukacji domowej moich dzieci, ani całkowitego przejścia na rozliczenia gotówkowe.

Staram się obronić przed innym zagrożeniem: nasilającym się masowym śledzeniem, owymi dragnetami, ukierunkowanymi na przechwytywanie danych dotyczących każdego aspektu naszego życia i umieszczanie ich w jakiejś stałej bazie danych. Martwię się, że proceder masowego śledzenia będzie kolidował ze swobodą wiązania się z pewnymi ideami i ludźmi, że uprzykrzy mi to życie pod względem ekonomicznym i że stworzy kulturę strachu. Obawiam się, że w najgorszym przypadku może doprowadzić do powstania totalitarnego państwa nadzoru.

* * *

Aby stworzyć mój model zagrożenia, konsultowałam się z różnymi ekspertami – od urzędników państwowych wysokiego szczebla, posiadających dostęp do tajnych dokumentów po hakerów, którzy tworzą narzędzia przeciwdziałania inwigilacji. Każdy miał inne sugestie. Na przykład niektórzy doradzali mi używanie różnych komputerów, w zależności od celu przeznaczenia – jednego do bankowości, drugiego do spraw osobistych, a trzeciego do pracy. Inni zalecali korzystanie z oprogramowania, które podzieliłby mój komputer na trzy oddzielne

sekcje, imitując w ten sposób model z trzema komputerami. Jeszcze inni podpowiadali, że taki podział nie ma sensu, gdyż dane i tak się wymieszają. W efekcie, po wielu konsultacjach, uświadomiłam sobie, że cudownego środka nie ma.

Musiałam wymyślić swój własny plan bitwy. Sporządziłam tabelę z zagrożeniami i zaproponowałam taktyki przeciwstawiania się każdemu z nich. Niektóre wydawały się stosunkowo łatwe do zneutralizowania; na przykład by uniknąć śledzenia *online*, musiałabym zainstalować różne programy blokujące możliwość śledzenia i porównać, który z nich działa najlepiej. Inne były bardziej skomplikowane; nie znałam na przykład dobrej taktyki przeciwstawienia się automatycznym czytnikom numerów rejestracyjnych, które sfotografowałby tablice mojego auta, gdybym je minęła. Jeden z ekspertów sugerował, żeby pokryć blachy sprayem albo szkłem odbijającym podczerwone promieniowanie. Ale w Nowym Jorku, gdzie mieszkam, działania w wyniku których dochodzi do, „zniekształcenia nagranego albo sfotografowanego obrazu tablic rejestracyjnych" jest nielegalne[14].

Przyszło mi wtedy do głowy, że zanim zdecyduję się na jakąś taktykę, muszę wypracować ogólne wytyczne kierujące moim zachowaniem. Tak nakreśliłam osobiste zasady postępowania:

Nie łamać prawa. Nie zamierzam unikać opodatkowania ani łamać prawa. A więc będę się angażować tylko w działania, które są legalne. Oznacza to, że nie będę maskować tablic rejestracyjnych.

Czasami jednak nie jest do końca jasne, co jest zgodne z prawem, a co nie. Weźmy przykład fałszywych praw jazdy. Poprosiłam Marka Eckenwilera, byłego prawnika ds. inwigilacji w Departamencie Sprawiedliwości, o opinię, czy można posługiwać się fałszywym dowodem tożsamości[15]. Mark wskazał przepis, który za nielegalne uznaje wykorzystanie cudzych dokumentów do popełnienia przestępstwa[16]. Przywołał jednak także orzeczenie Sądu Najwyższego z 2009 roku interpretujące ten zapis w ten sposób, iż przestępca musi mieć świadomość naruszania danych istniejącej osoby. To implikuje, że dopuszczalne jest używanie fałszywego prawa jazdy, zawierającego dane nieistniejącej osoby[17]. Niemniej Mark zwrócił mi też uwagę na przepisy o oszustwach pocztowych i telekomunikacyjnych, według których, nielegalne jest

angażowanie się w „jakiekolwiek działania” mające na celu uzyskanie pieniędzy lub majątku poprzez składanie „fałszywych albo nieuczciwych obietnic”[18].

Nie jest niespodzianką, że Mark uchylił się od udzielenia mi wiążącej opinii na temat tego, czy powinnam wyrobić sobie fałszywy dowód tożsamości, czy nie. Jednak wspomniane przez niego przykłady zdawały się wskazywać, że prawdopodobnie byłabym bezpieczna, używając dokumentów wystawionych na fikcyjne nazwisko, o ile nie posłużyłabym się nimi do dokonania oszustwa.

Mimo wszystko postanowiłam nie załatwiać sobie podrabianego dowodu. Wolę stać po bezpiecznej stronie prawa.

Dalej żyć w nowoczesnym świecie. Nie jestem zainteresowana odłączeniem się od technologii. Wierzę, że to właśnie ona umożliwiła ludziom dokonanie w świecie wielkich zmian. Chcę tylko ograniczyć szkodliwe przejawy przesyconego technologią życia.

W związku z tym nie będę w stanie osiągnąć prywatności idealnej. Zdolny i zdeterminowany przeciwnik będzie w stanie poradzić sobie z niemal każdym środkiem ostrożności. John J. Strauchs, były agent CIA, który aktualnie jest konsultantem ds. bezpieczeństwa[19], opowiedział mi historię o tym, jak zatrudniono go do włamania się do głównej siedziby solidnie chronionego podmiotu z branży finansowej, posiadającego aż trzy zewnętrzne kręgi zabezpieczeń. Strauchs przemycił więc szpiega w bagażniku samochodu należącego do niewzbudzającego podejrzeń pracownika.

Większość działań, które podejmuję, także da się obejść. Na przykład jeśli będę używać kodów do szyfrowania treści e-maili, mój przeciwnik i tak może zainstalować na moim komputerze oprogramowanie, który wyłapie uderzenia w klawisze, zanim słowa zostaną zakodowane.

Moim celem nie jest jednak zwycięstwo za wszelką cenę. Chcę tylko zmusić ewentualnego przeciwnika do cięższej pracy. Mogę nie być w stanie ochronić się przed inwigilacją na publicznych ulicach, ale być może jestem w stanie skazać mojego wroga na analizowanie wielogodzinnych nagrań wideo, uniemożliwiając mu proste i skuteczne śledzenie wszystkich moich ruchów za pomocą danych z lokalizatora GPS.

Używać konwencjonalnych narzędzi. W swojej znakomitej książce na temat przetworzonej żywności, zatytułowanej *The Omnivore's Dillema*, Michael Pollan przygotowuje posiłek z tego, co upoluje i uzbiera[20]. Zabija świnię, zbiera grzyby w lesie i wiśnie z drzewa sąsiada. Nazywa to „idealnym posiłkiem".

Niektórzy z moich doradców hakerów mają podobne podejście do technologii. Nie ufają narzędziom, których nie potrafią sami stworzyć, zmodyfikować albo zaprojektować. Obchodzą oprogramowanie zainstalowane na ich telefonach, aby działać na tym, które sami sobie wybiorą. Odpalają komputery raczej z płyty CD niż z tradycyjnego systemu operacyjnego.

To może być „idealny" sposób na ochronę danych, niestety jest on poza moim zasięgiem. Jestem wystarczająco sprawna technicznie, żeby zarządzać moją stroną internetową, ale nie ufam sobie na tyle, żeby dać radę zmodyfikować oprogramowanie mojego telefonu. Nie sądzę też, aby to było właściwe podejście. Piękne w erze nowoczesności jest to, że te potężne technologie są jednak dość łatwe w użyciu z punktu widzenia zwykłych ludzi. To dzięki temu możemy czerpać z nich korzyści.

A więc, w związku z wyznawaną przeze mnie zasadą życia w nowoczesnym świecie, mam zamiar wystrzegać się najbardziej ekstremalnych praktyk hakerów, pochodzących ze środowiska, które „żywi się tylko tym, co upoluje". Zamiast tego będę wykorzystywać konwencjonalne narzędzia, znajdujące się w zasięgu większości ludzi o podobnym do mnie poziomie umiejętności technicznych. (Nie będę udawać, że wasza babcia może zrobić to wszystko, co ja zamierzam. Ale wasze nastoletnie dziecko z pewnością będzie do tego zdolne).

Dążyć do nieprzetrzymywania żadnych danych. Doskonały sposób na ochronę własnych danych to nie zdradzanie ich. A najlepszą metodą osiągnięcia tego jest korzystanie z serwisów, które nie przechowują danych.

Oczywiście, takie serwisy są rzadkością, niemniej rzeczywiście istnieją. Przyjrzyjmy się gabinetowi mojego lekarza, który mieści się w wieżowcu w centrum Manhattanu. Od ataków 11 września 2001 roku, jak w większości budynków w Nowym Jorku, portierzy pytają tam gości o dane osobowe. Gabinet mojego lekarza chroni jednak prywatność pacjentów w ten sposób, że przydziela każdemu z nich kod do przekazania

portierowi zamiast danych identyfikacyjnych. Pracownicy recepcji są usatysfakcjonowani, a przy tym nie przechowuje się tam żadnych danych pacjentów.

Podczas mojej akcji będę starać się więc współpracować z przedsiębiorstwami, które przechowują jak najmniejszą ilość danych, wystarczającą do realizacji ich zadań. W niektórych szczęśliwszych przypadkach będzie to oznaczało wręcz zero danych. W innych ich ilość będzie minimalna.

Przeprowadzać „test kałuży błotnej". Jednym ze sposobów na określenie, czy udało wam się zminimalizować wasz ślad cyfrowy, jest wykonanie czegoś, co niektórzy inżynierowie ds. bezpieczeństwa nazywają „testem kałuży błotnej". Oto na czym on polega: wyobraźcie sobie, że upuściliście swoje urządzenie do pełnej błota kałuży, poślizgnęliście się, rozbiliście głowę i zapomnieliście hasła dostępu. Czy możecie je teraz odzyskać z systemu, którego używacie? Jeśli odpowiedź brzmi „tak", znaczy to, że zostawiliście swój ślad cyfrowy. Jeśli odpowiedź brzmi „nie" – udało się wam uniknąć pozostawienia go. Oczywiście nie macie już też swoich danych.

Problem z „testem kałuży błota" jest taki, że tak czy inaczej przegrywacie. Ale przypomina on o tym, że jeśli korzystacie z usług, których dostawca pozwala wam na przywrócenie utraconego hasła, to znaczy, że serwis ten ma dostęp do waszych danych. Będę stosować „test kałuży błotnej" do oceny systemów, których używam.

Zanieczyszczać dane. Gdy nie jestem w stanie zminimalizować mojego cyfrowego śladu, mogę spróbować zanieczyścić dane, używając fałszywych nazwisk i mylących informacji.

Wstyd się przyznać, ale nie umiem kłamać. Gdy to robię, odczuwam fizyczny dyskomfort – nawet gdy wpisuję fałszywe nazwisko do internetowego formularza. Zaczynam odczuwać uderzenia gorąca, a mój puls wpada w galopadę.

Niemniej w istocie nie mam się właściwie czego wstydzić. Do niedawna to przecież anonimowe transakcje były normą przy wielu codziennych czynnościach. Płaciliśmy gotówką. Dzwoniliśmy z telefonów, które nie miały identyfikacji numeru dzwoniącego. Wysyłaliśmy listy, które

czasami nie miały adresu nadawcy.

A więc ślubuję przypominać sobie, że ludzie proszący mnie o wypełnienie formularza *online*, gdy pragnę zamówić podstawową usługę, nie zawsze zasługują na prawdziwe odpowiedzi. Trudno jednak przyzwyczaić się do tego dziewczynce, która w podstawówce była takim wzorem wszelkich cnót, że zostawała na przerwie i ścierała tablicę przed kolejną lekcją.

Mimo to spróbuję uczynić zanieczyszczanie danych kluczowym składnikiem mojego arsenału bezpieczeństwa prywatności.

Chronić swój ruch internetowy. Zamierzam ciężko pracować nad tym, by nie pozwolić nikomu analizować mojego „ruchu internetowego", a więc zbierać informacji o tym, z kim wymieniam e-maile, do kogo dzwonię i z kim nieustannie czatuję.

Ludzie martwią się o prywatność zawartości ich e-maili, tekstów i czatów. Tymczasem analiza samego ruchu może często ujawnić tyle samo, a nawet więcej, co sama treść komunikacji. Jeśli wymieniam sześć wiadomości dziennie z dilerem narkotyków, to czy naprawdę potrzeba wiedzieć, o czym mówimy? Sama liczba przesłanych wiadomości zaprowadzi mnie na listę podejrzanych kontaktów tego dilera.

Komputery są zresztą dużo bardziej wydajne w analizowaniu zestawień kierunków komunikacji, niż w odnajdowaniu wzorców pośród ogromnych ilości tekstu. To znaczy, że ci, którzy dokonują masowej inwigilacji niemal zawsze najpierw skupią się na ruchu internetowym. A więc priorytetem uczynię jego ochronę.

Komunikować się w czasie rzeczywistym. Ustawa o podsłuchach (Wiretap Act) nakłada na policję[21] obowiązek uzyskania „supernakazu" – który jest trudniejszy do zdobycia niż zwykły nakaz przeszukania – zanim zacznie przechwytywać krajową komunikację, np. rozmowy telefoniczne, czaty wideo i kontakty przez komunikatory internetowe, w czasie rzeczywistym.

Jednak gdy komunikacja jest zarchiwizowana, organy ścigania nie potrzebują już nakazu, by się do niej dostać. A więc dobrą metodą unikania śledzenia jest praktykowanie komunikacji w czasie rzeczywistym i nie przechowywanie jej. (O ile oczywiście nie jest się podejrzanym i policja nie ma supernakazu do przechwytywania twojej komunikacji

w czasie rzeczywistym – w takim przypadku życzę powodzenia).

Nie jest łatwo uniemożliwić archiwizację tekstów i czatów, w szczególności dlatego, że często nie da się skontrolować tego, czy nasz współrozmówca nie przechowuje tych informacji. Na szczęście jednak większość dyskusji wideo i audio nie jest automatycznie archiwizowanych.

W ten sposób zwykła, staromodna domowa rozmowa telefoniczna jest ciągle jednym z bardziej prywatnych sposobów komunikacji.

Rozpraszać dane. Jedyną rzeczą gorszą od zgubienia karty kredytowej jest zgubienie całego portfela. Na tej samej zasadzie, utrata niektórych danych nie jest aż tak zła, jak utrata wszystkich. Będę więc starała się rozpraszać swoje dane – aby zminimalizować szkody z powstałe w wyniku nieuniknionych wycieków, włamań, rządowej inwigilacji itp.

Na przykład będę musiała wybrać, które spośród wielu serwisów Google zachowam – e-mail, wyszukiwarkę, mapy i telefon z Androidem. Biorąc pod uwagę, że w samej tylko drugiej połowie 2012 roku rząd przesłał do Google'a 21 389 zapytań o dane, dość rozsądnym byłoby nie przechowywać tam wszystkich ważnych informacji o sobie[22].

Oczywiście nie da się uniknąć przetrzymywania niektórych informacji w niepewnych bazach danych – o ile nie zdecyduję się na trzymanie wszystkich w domu. Ale mam nadzieję, że dzięki ich rozproszeniu, będę mogła zmniejszyć ryzyko narażenia się na niebezpieczeństwo.

Płacić za usługi. Wielu hakerów tworzących systemy ochrony prywatności jest zwolennikami darmowego oprogramowania. Uważają, że użytkownicy powinni być w stanie tworzyć i modyfikować programy, których używają, aby nie tkwić w pułapce systemów, których nie kontrolują. Teoretycznie, wolne (swobodnie modyfikowalne) oprogramowanie nie musi być darmowe. W rzeczywistości jednak to firmy nastawione na zyski wolą chronić swoje kody źródłowe przed możliwością majstrowania w nich z zewnątrz. Stąd, większość swobodnie modyfikowalnych rodzajów oprogramowania jest nieodpłatna.

Przykrą konsekwencją tego jest fakt, że z braku przychodów, wiele z tych przedsięwzięć więdnie. Programiści, którzy je tworzą, z czasem oddają się innym zajęciom. A więc w mojej pogoni za ochroną prywatności będę wspierać finansowo (poprzez datki lub zakup

programów) te przedsięwzięcia, w ramach których programiści dostają godziwe wynagrodzenia.

Podążać za przejrzystością. Śledzący mnie, którzy pozwalają mi na wgląd w informacje na mój temat, które posiadają, są mniej agresywni niż ci niedający mi obejrzeć swoich danych.

Przejrzystość jest kluczowa. Czuję się pewnie, jeśli chodzi o moją zdolność kredytową, ponieważ mam szansę przeglądania dotyczących jej danych. Mogę też zakwestionować każdy błąd, jaki zauważę. Ale większość dostawców usług, którzy śledzą moje ruchy, nie pokaże mi przechowywanych o mnie danych. Wydaje się to niesprawiedliwe. Zatem zamierzam z większą życzliwością podchodzić do tych śledzących mnie podmiotów, które oferują transparentność. Jeszcze milsza będę dla tych, którzy pozwolą mi usunąć moje dane, skorygować je albo pobrać na własny użytek.

Myśleć o prywatności jako formie protestu. Zawsze proszę o przeszukanie zamiast przejścia przez lotniskowe bramki skanujące ciało. Przeszukiwanie jest bardzo inwazyjne: pewnego razu podczas sprawdzania mojego paska, przeszukujący wcisnął swoją rękę nieco zbyt głęboko w moje spodnie; innym razem pociągnął za pasek na moich plecach z taką siłą, że omal nie upadłam. Jest to na wiele sposobów bardziej inwazyjne niż działanie zautomatyzowanych skanerów.

Celem, jaki stawiam sobie, unikając prześwietlania moich ubrań, jest zamanifestowanie sprzeciwu wobec tej procedury. Skanery tego rodzaju to rzadki – jawny – przykład działań z zakresu masowego śledzenia. Korzystam więc okazji, by zaprotestować. To trochę jak domowy recycling. Skrupulatne segregowanie puszek i butek prawdopodobnie nie zmieni losów planety. Kilometry, które przemierzam w samochodzie, są dużo bardziej szkodliwe dla środowiska niż te śmieci. Jednak recycling przypomina „pierwszą działkę narkotyku”; sprawia, że większe zmiany wydają się być w zasięgu ręki.

Żywię nadzieję, że ten mój mały protest wobec naruszania prywatności pozwoli mi myśleć, że większe zmiany są w zasięgu ręki.

Nie ulegać lękowi. Jest prawdopodobne, że podejmowanie kroków zmierzających w stronę ochrony mojej prywatności, zaprowadzi mnie na czarną listę podejrzanych.

Federalni prokuratorzy argumentowali w sprawie dotyczącej stanu Arizona, że zgodnie z logiką pozwany nie mógł dochodzić ochrony prywatności, ponieważ użył do podpisania się pod kartą prepaidową fałszywego nazwiska[23]. Ujawnione przez Edwarda Snowdena dokumenty NSA pokazują, że agencja archiwizuje zaszyfrowaną korespondencję obywateli USA, choć jej wytyczne mówią, że „krajowa komunikacja będzie natychmiast niszczona"[24]. Jednak wiadomości zawierające „ukryte znaczenia" mogą być przechowywane, co oznacza, że moje zaszyfrowane e-maile prawdopodobnie sprawią, że trafię na jakiegoś rodzaju czarną listę Agencji.

Nie chcę jednak ulegać lękowi, że moje działania podejmowane w obronie prywatności mogą sprawić, że znajdę się w kręgu podejrzanych. Wolę potraktować moją obecność na tej ewentualnej czarnej liście jako część politycznego protestu przeciwko dragnetom.

* * *

W pewnym sensie ten nowy świat, w który wchodzę, jest podobny do rzeczywistości dysydentów w represyjnych reżimach: w którym prowadzone ściszonym głosem kawiarniane rozmowy są znacznie bezpieczniejsze niż rozmowy telefoniczne, przesyłanie e-maili i inna elektroniczna komunikacja.

Aby zrozumieć życie, w jakie wkraczam, dotarłam do człowieka, który dogłębnie przebadał wyzwania stojące przed dysydentami – Mike'a Perry'ego, pracownika Project Tor, tworzącego oprogramowanie, które w zamyśle ma pomagać ludziom obejść cenzurę i inwigilację. Perry był zbulwersowany przypadkami naruszeń prywatności po atakach 11 września 2001 roku przez administrację Busha[25]. Rozpoczął więc pracę dla Project Tor jako wolontariusz-programista komputerowy. I zaczął poważnie traktować swoją prywatność.

Gdy ze swoim szefem i dyrektorem technicznym przeglądał materiały na Amazonie, denerwowało go, że wciąż widzi spersonalizowane rekomendacje różnych książek, dotyczących polityki i jego prywatnych zainteresowań.

Uznał, że sugestie Amazona miały charakter zbyt „osobisty”, zaczął więc czyścić dane umożliwiające śledzenie go w sieci.

Perry i ja spotkaliśmy się w parku w San Francisco. (Według Johna Strauchsa miejsca publiczne są idealne na prywatne konwersacje, dopóki nie używa się zapalnych słów, jak „bomba”, które powodują, że ludzie zaczynają uważniej słuchać)[26]. Perry wyglądał jak prawdziwy haker: szczupły, z bladawą cerą, ubrany na czarno. Opowiedział mi o niektórych stosowanych przez niego metodach zabezpieczeń (choć nie o wszystkich, gdyż naraziłoby to na szwank jego bezpieczeństwo).

Perry opisał siebie jako „inwigilacyjnego weganina” – mając na myśli to, że jest tak skrupulatny w unikaniu inwigilacji, jak weganin w unikaniu produktów pochodzenia zwierzęcego. (Czyni dwa wyjątki: wciąż rezerwuje *online* bilety samolotowe i czasem przebywa w hotelu pod własnym nazwiskiem).

Nawet jego najbliżsi przyjaciele nie wiedzą, gdzie mieszka, choć niektórzy z nich śledzili go aż do jego bloku. (Jego rodzina kiedyś go odwiedziła, ale wciąż nie ma dokładnego adresu). Jeden z nich wrzucił mu nawet do torby telefon na kartę z włączonym GPS-em, bezowocnie próbując go w ten sposób zlokalizować.

Odbiera pocztę w wielu miejscach, między innymi w pralni samoobsługowej i w paczkomacie, co pozwala mu odbierać paczki pod różnymi nazwiskami. Często używa telefonów z wieloma jednorazowymi identyfikacjami. Za gotówkę opłaca karty pre-paid, przeznaczone do różnego rodzaju kontaktów: jedne do prowadzenia interesów, inne do prywatnych spraw, jeszcze inne do komunikacji z Torem. „Usiłuję różne sprawy załatwiać przez różne telefony”, powiedział mi. Stara się wyjmować baterie z aparatów, gdy ich nie używa.

Perry wierzy w stosowanie różnych jednorazowych tożsamości dla różnego rodzaju relacji. Oznacza to, że wielokrotnie zakłada adresy e-mailowe i profile w komunikatorach internetowych. Po naszej rozmowie założył dedykowany mi adres komunikatora, abym mogła do niego dotrzeć. Powiedział, że skasuje go, gdy nasze rozmowy się zakończą.

Tryb życia Perry’ego stanowił prawdziwe wyzwanie. Zapytałam, jak to na niego wpłynęło. „Szczerze mówiąc, miało to znaczenie dla mojej zdolności do utrzymywania bliższych relacji”, odrzekł. Powiedział, że jego metoda unikania inwigilacji przyczyniła się do rozstania z dwiema dziewczynami oraz utrudniła mu kontakty z wieloma kolegami. Nie mieli

ochoty na utrzymywanie otwartych, dedykowanych, szyfrujących programów do czatowania, by móc z nim porozmawiać.

Zaczynało to przypominać rozrywkę młodego człowieka. Cóż, w końcu Perry jest singlem, który pracuje w domu. Ja jednak jestem mamą z dwojgiem dzieci, która codziennie chodzi do biura. Trudno byłoby mi kierować życiem z pralni samoobsługowej i zarządzać wieloma numerami telefonów przypisanymi do konkretnych osób, z którymi się kontaktuję.

Perry w pewien delikatny sposób upewnił mnie w przekonaniu, że działa jednak nie tak, jak powinien, a ja nie muszę być „inwigilacyjnym weganinem". „Niektórzy ludzie są po prostu inwigilacyjnymi *fleskitarianinami* i to też jest dobre", powiedział. A potem odwiózł mnie miejskim pociągiem do mojej stacji docelowej, skąd odprowadził mnie aż do parkingu.

I wrócił metrem do domu – gdziekolwiek się znajdował.

6

AUDYT

„Powinnaś znać swoje dane”, powiedział mi Michael Sussmann w trakcie śniadania w kawiarni niedaleko Kapitolu[1].

Sussmann, były prokurator federalny w Departamencie Sprawiedliwości w Sekcji Przestępstw Komputerowych i Własności Intelektualnej, był poprzedniego wieczora do późna poza domem. Wierny fan Bruce’a Springsteena jechał z żoną dwie i pół godziny, żeby zobaczyć „Bossa” grającego w Charlottesville w Wirginii. Sussmann miał zapuchnięte oczy, ale uprzejmie zgodził się pomóc mi stworzyć mój model zagrożenia.

„To nudne”, przyznał. Jednak to właśnie audyty są zwykle pierwszą rzeczą, którą robi dla swoich klientów. Sussmann jest aktualnie partnerem w kancelarii prawniczej Perkins Coie, gdzie doradza przedsiębiorstwom takim, jak Google w kwestiach dotyczących prywatności w internecie.

„Startujemy od schematu organizacyjnego, a potem odnajdujemy każdy kawałek danych, który gromadzi to przedsiębiorstwo z każdego źródła”, powiedział.

Podniósł ważną kwestię: jeśli nie wiem, gdzie są moje dane, to jak mogę je chronić? Dla mnie jednak wyzwaniem nie było wewnętrzne ich zlokalizowanie, ale zewnętrzne. Postanowiłam więc zacząć swoją pogoń za prywatnością od próby znalezienia moich danych.

* * *

Zaczęłam od najoczywistszych źródeł – Google, Facebook i Twitter, tj. od spółek, które nazywam „freestylowcami”. Co one o mnie wiedzą?

Aby znaleźć informacje o mnie znajdujące się w Google[2], weszłam

na stronę Data Liberation Front, nietypowego projektu Google, który pozwala użytkownikom ściągnąć dane tam przechowywane. Używszy w menu Data Liberation Front opcji „wyjmowania", pobrałam kontakty do 2192 osób, do których mailowałam od czasu, kiedy zaczęłam używać Gmaila w roku 2006. Ściągnęłam także kilka fotografii, które archiwizowałam w Picasa (serwis fotograficzny Google, o którym zapomniałam, że w ogóle z niego korzystałam) oraz dwanaście dokumentów, którymi podzieliłam się z innymi przy użyciu Google Drive (ale już nie te 204, którymi inni podzielili się ze mną).

To by było na tyle. Kiedy chciałam, by system wygenerował dla mnie historię stron, które odwiedzałam, Data Liberation Front oświadczył: „Nie ma aktualnie możliwości eksportowania historii stron internetowych Google".

Nieco więcej informacji znalazłam na mojej Google Dashboard – stronie, która zawiera informacje o mojej aktywności na różnych serwisach Google, zaszytych w moich ustawieniach konta. Dashboard odnotował, że spośród 2192 ludzi, z którymi połączyłam się przez Gmaila, najczęściej kontaktowałam się – co nie dziwi – z moim mężem. Odnotowano także, że miałam na Gmailu 23 397 e-maili i czatów.

Dziwne, tam również nie było mojej historii wyszukiwania stron internetowych. Była za to ukryta w zakładce mojego konta o nazwie „Inne narzędzia". Tam zobaczyłam, że Google zapisywał moje wyszukiwania sieci od czasu, kiedy otworzyłam konto, czyli od 2006. Wyglądało na to, że wykorzystywałam Google do wyszukiwania haseł 26 tysięcy razy miesięcznie!

Google w pomocny sposób posortował moje wyszukiwania według daty i rodzaju (mapy, podróże, książki itd.). Zyskałam wgląd do czegoś przerażającego, co buddyści mogliby nazywać „małpim umysłem" – zapisu niezmordowanych skoków z miejsca na miejsce.

Spójrzmy na 30 listopada 2010 roku: zaczęłam dzień od czytania jakichś wiadomości technicznych. Potem nagle szukałam brokatowych różowych espadryli dla mojej córki. Następnie weszłam do słownika, żeby poszukać słowa do artykułu, który pisałam, później do OpenTable, aby zarezerwować restaurację, a potem na stronę Kongresu, żeby ściągnąć tekst o prawie dotyczącym prywatności. Uff.

Te moje przeszukiwania nie tylko rzucały światło na moje myśli, ale także ujawniały miejsca pobytu. Garść wyszukiwań pod hasłem „mapa Berlina" była prowadzona w trakcie mojej podróży do tego miasta; „Hyatt

Regency Pune" – gdy jak co roku odwiedzałam teściów w Indiach; „lotnisko DFW, Irving, TX $\frac{23}{11}$ 3150 Binkley Ave., Dallas, TXN 75205" – podczas podróży biznesowej do Dallas.

To było bardziej prywatne niż osobisty dziennik. Było to okno wychodzące na moje codzienne myśli. Z pewną nostalgią przejrzałam wyszukiwania poduszek do karmienia po tym, jak urodził się mój syn a także dobrej meksykańskiej restauracji w trakcie rodzinnych wakacji w Arizonie.

I naprawdę chciałam ściągnąć te dane, ale nie było łatwego sposobu ich wydostania. Rzecznik Google Rob Shilkin[3] powiedział mi: „Jest wiele produktów, których nie da się *wyciągnąć*. Zaczęliśmy udostępniać dane w roku 2011, startując z pięcioma produktami. Systematycznie to uzupełniamy". Dodał, że mogę usunąć swoją historię. Kiedy jednak już ją zobaczyłam, nie chciałam jej kasować. Chciałam ją mieć.

Facebook był znacznie mniej otwarty w kwestii informacji o mnie. Kliknęłam na „ściągnij kopie moich danych" i wysłał mi archiwum, które było godne uwagi, ale ze względu na to, czego nie zawierało. Nie było tam listy znajomych, postów, lajków ani komentarzy przy postach innych. Zamiast tego moje archiwum fejsbukowe zawierało nieco fotografii, o których myślałam, że je skasowałam, znajomych, których usunęłam, oraz kompletną listę moich logowań (kiedy i skąd się wchodziłam na moje konto – przeważnie z domu, biura i podróży biznesowych). Okazuje się, że archiwum postów i lajków jest w innej sekcji Facebooka o nazwie „aktywne logowania", ale było także dziwnie niekompletne i zawierało tylko kilka fotografii, żadnych lajków i komentarzy. I nie można było go pobrać.

Moje dane z Facebooka były tylko bladym cieniem tego, co otrzymał Max Schrems, gdy pobrał informacje o sobie w 2011 roku[4]. Schrems, student prawa w Wiedniu, zażądał udostępnienia mu jego danych, przechowywanych przez Facebook na podstawie europejskiego prawa o prywatności i otrzymał raport liczący1 222 strony[5]. Zawierał nie tylko listę wszystkich znajomych, postów itd., ale także dane, o których myślał, że są wykasowane – prośby znajomych, które odrzucił, zaproszenia, które usunął, oraz aktualizacje tablic i statusów, które wykasował.

W sierpniu 2011 roku złożył skargę w irlandzkim Urzędzie Ochrony Danych (europejski oddział Facebooka mieści się w Irlandii), twierdząc, że większość danych przechowywanych przez Facebooka narusza przepisy

o ochronie danych obowiązujące w Unii Europejskiej. Unia wymaga bowiem od podmiotów przechowujących dane osobowe transparentności w kwestii praktyki ich zbierania[6]. Pozwala przetrzymywać je tylko dopóki jest to konieczne do realizacji celów, dla których były gromadzone.

W rezultacie irlandzki urząd przyjrzał się działaniu Facebooka i zalecił wprowadzenie pewnych „dobrych praktyk", w tym lepsze objaśnienie działań odnośnie usuwanych treści[7]. Rok później Facebook zmienił swoją politykę korzystania z danych i jasno oświadczył, że „informacje związane z twoim kontem będą przechowywane do czasu, gdy twoje konto zostanie zamknięte"[8]. W roku 2012 irlandzki urząd postanowił sprawdzić, czy Facebook przestrzega wytycznych i stwierdził, że spółka zaimplementowała „większość" jego sugestii[9]. Ale instytucja zauważyła także, że portal wciąż nie udostępnia opcji w pełni weryfikowalnego zamykania konta „ponad wszelką wątpliwość".

Krótko mówiąc, wydawało się, że Facebook zamierzał przetrzymywać moje dane – bez względu na to, czy je usunęłam, czy nie. Za to nie można było otrzymać w krótkim czasie kompletnego zestawu danych o mnie z Facebooka.

Wydostanie tego z Twittera było za to łatwe. Po prostu kliknęłam na ikonkę „prośba o archiwum". Twitter natychmiast odesłał mi e-maila z poręcznym arkuszem Excela, zawierającym moje 2,993 tweety napisane od czasu, kiedy założyłam swoje konto w 2008 roku.

Nie zawsze jednak było to takie proste. Twitter aż do roku 2012 nie dawał swoim użytkownikom możliwości ściągnięcia archiwum tweetów[10], choć od 2010 roku oferował podobne dane przedsiębiorstwom[11], które celem śledzenia trendów zapłaciły za subskrypcję całego strumienia wiadomości.

Moje tweety miały charakter mniej osobisty niż rezultaty wyszukiwań w Google. Wiele stanowiło tylko powielenie mojej pracy – podawania dalej artykułów kolegów i moich własnych, uczestniczenie w wydarzeniach twitterowych „na żywo". Ale było trochę tweetów, o których zapomniałam. 9 marca 2009 roku: „Moja pierwsza przespana noc w roku – dziecko w końcu przespało całą noc. Alleluja".

Ogólnie rzecz biorąc, freestylowcy zgromadzili w ciągu minionych kilku lat portret mojego życia, który całkiem sporo ujawniał. Był dużo kompletniejszy niż jakiekolwiek akta przeglądane przeze mnie w archiwum Stasi. A mimo to wiele z tego, i to jest przerażające, wprawiło

mnie w nostalgiczny nastrój. Przecież był to cyfrowy zapis mojego życia. Przypomniał mi się wtedy moment, gdy spotkałam przyjaciółkę i jej męża na placu zabaw w naszej dzielnicy na Manhattanie. Gdy patrzyliśmy na nasze córki – są w tym samym wieku – jak bawią się w małpim gaju, mężczyzna zapytał mnie o artykuł, który pisałam na temat prywatności.

„Kiedyś bardziej dbałem o prywatność", stwierdził. Szykowałam się już na zwykły argument typu: „Ja nie mam nic do ukrycia", ale on zaskoczył mnie zupełnie innym podejściem. Powiedział, że uświadomił sobie, że nie martwi się tak bardzo utratą części prywatności. Raczej bowiem „podoba mu się pomysł pozostawiania artefaktów" dotyczących jego życia. Krótko mówiąc, rzekł, wszystkie te informacje o nas, które pozostawiamy w sieci, dają nam pewnego rodzaju „nieśmiertelność".

Patrząc na moje stare tweety i wyszukiwania w Google, nie mogłam przestać myśleć o tej rozmowie z mężem przyjaciółki. Ze wszystkich argumentów na rzecz powszechnego zbierana danych, pragnienie nieśmiertelności wydawało mi się najbardziej sensownym.

* * *

Zyskałam jednak inne spojrzenie na tę nieśmiertelność, kiedy zerknęłam na informacje, jakie mają na mój temat spółki gromadzące dane. A zaczęło się to, gdy siedziałam na tarasie domu Mike'a Griffina na przedmieściach Baltimore, spoglądając na Zatokę Chesapeake[12].

Mike jest windykatorem[13], który wpadł w biznes związany z monitoringiem samochodów. Jest wysoki, chudy, pełen nerwowej energii. Wydaje się utrzymywać przy życiu tylko dzięki kawie i papierosom.

Zbierałam informacje do artykułu o nasilaniu się zjawiska korzystania z automatycznych czytników tablic rejestracyjnych i postanowiłam złożyć wizytę Mike'owi. Kieruje on jedną z największych w USA prywatnych akcji fotografowania tablic rejestracyjnych. Jego flota dziesięciu wyposażonych w aparaty fotograficzne samochodów przejeżdża dziennie od 450 do 650 km, skanując tablice w metropoliach Baltimore i Waszyngtonu. Co miesiąc pracujący dla niego na dwie zmiany kierowcy gromadzą dane o lokalizacji milionów tablic.

Mike w pierwszej kolejności wykorzystuje te dane do wyłapywania aut, które mają być przejęte za długi. Technologia poprawiła jego wyniki:

zamiast sześciu samochodów, jak do tej pory, dzięki aparatom przejmuje ok. piętnastu takich samochodów na dobę. Ostatecznym celem Mike'a jest jednak sprzedanie dostępu do gromadzonych przez niego danych poręczycielom, doręczycielom pism procesowych, prywatnym detektywom i ubezpieczycielom. „Mam nadzieję, że za kolejne pięć lat moim głównym biznesem będzie zbieranie danych", powiedział mi.

Dumał nad jednym możliwym kupcem danych: spółce o nazwie TLO[14]. Już od lat słyszałam o TLO. Jej założyciel, Hank Asher, był legendą. Niegdyś przemytnik narkotyków, który zmienił się w maniaka egzekwowania prawa, Asher był najbardziej ekstrawaganckim facetem w biznesie polegającym na gromadzeniu danych. Zarobił miliony jako właściciel przedsiębiorstwa, które pomalowało wieżowce na Florydzie i w wieku trzydziestu lat przeszedł na emeryturę[15]. Przeprowadził się do Great Harbour Cay na Wyspach Bahama, pływał motorówką, latał dwusilnikowym Aerostarem i coraz bardziej uzależniał się od kokainy. Pewnego razu po uzgodnieniu przetransportowania samolotem na Florydę kilku ładunków narkotyków, uświadomił sobie, że sprawy zaszły jednak za daleko. Zerwał więc z tym wszystkim z dnia na dzień i postanowił, że zakończy z procederem przemytu na wyspie.

Zaczął pracować dla Amerykańskiej Agencji Antynarkotykowej (Drug Enforcement Administration, DEA) i zauważył, że potrzebuje ona lepszej bazy danych. I w roku 1992 stworzył produkt o nazwie AutoTrack, który miał zmienić branżę zbierania danych.

AutoTrack stanowił udoskonaloną metodę przeglądania publicznych danych: Asher kupił informacje od wydziału komunikacji stanu Floryda i sprawił, że można je było łatwo przeszukać. Nagle policja mogła obejrzeć zapisy dotyczące danego pojazdu i jego zachowania na drodze, wyszukując kierowcę po adresie, po fragmencie numeru ubezpieczenia czy fragmencie nazwiska. Wcześniej, żeby uzyskać numer tablicy rejestracyjnej, trzeba było wprowadzić imię i nazwisko osoby, płeć i datę urodzenia. AutoTrack zmienił tryb prowadzenia dochodzeń policyjnych. Zmienił także sposób prowadzenia śledztw dziennikarskich. Wiele razy korzystałam z AutoTracka, aby odnaleźć nazwiska i adresy ludzi, którym się przyglądałam.

W końcu jednak dopadły Ashera jego ekstrawagancja oraz narkotykowe historie. Jego własna spółka wykupiła jego udziały za 147 mln dolarów. Niezrażony założył kolejne przedsiębiorstwo, oferując bardzo podobny

produkt o nazwie Accurint. Natomiast po 11 września 2001 roku opracował program o nazwie MATRIX, który miał przygotowywać listy „czynników zagrożenia terrorystycznego", ale utknął w kwestiach dotyczących prywatności. I znów Asher zmuszony został odejść ze swojej firmy.

W roku 2009[16] po raz kolejny zajął się biznesem i powołał spółkę specjalizującą się w bazach danych, pod nazwą TLO, co oznaczało The Last One, gdyż była ostatnią firma, jaką planował prowadzić[17]. Jego plan się spełnił[18]. Asher zmarł bowiem w roku 2013 w wieku sześćdziesięciu jeden lat.

Mike twierdził, że dane TLO były dobre i tańsze od tych dostarczanych przez spółkę LexisNexis[19], która wiele lat wcześniej kupiła dwa poprzednie przedsiębiorstwa Ashera[20]. TLO pobierało tylko 25 centów za proste wyszukanie[21] i 5 dolarów za wyszukiwanie zaawansowane. Dla porównania, serwis People Wise, należący do LexisNexis, pobierał 1,95 dolarów za raport podstawowy i 24,95 dolarów za raport premium[22].

– Mogę zobaczyć swój raport? – spytałam.

– Jasne – odpowiedział.

W mniej niż minutę trzymałam w ręku czterostronicowe zestawienie, zawierające wszystkie moje poprzednie adresy – łącznie z numerem mojego pokoju w college'u: 536B. Nie było tam jakiejkolwiek nieścisłej informacji.

Zatkało mnie. Sama już zapomniałam numeru mojego pokoju, adresu domu w Waszyngtonie, który dzieliłam z pięcioma innymi świeżo upieczonymi absolwentami college'u i mojej kawalerki z czasów panieńskiego życia w Nowym Jorku, jeszcze zanim poznałam przyszłego męża. Z każdym z tych adresów wiązały się pewne wspomnienia.

Były to w pewnym sensie nawet bardziej pogłębione informacje niż te, które posiadali o mnie „freestylowcy". W końcu opisywały moje prawdziwe życie, tylko że dekady wstecz. Mówiliśmy coś o nieśmiertelności...

* * *

Gdy jednak wyszukiwałam informacje o sobie w innych bazach danych, mój romans z nieśmiertelnością nieco ostygł. Sporządziłam listę ponad dwóch tysięcy komercyjnych baz danych, a byłam zupełnie pewna,

że i tak nie znalazłam wszystkich. Miało to więcej wspólnego z prostytucją niż nieśmiertelnością.

Niektóre z nich nosiły dobrze znane nazwy, jak agencja informacji kredytowej Experian. Ale większość z nich stanowiły malutkie firemki, oferujące dostęp do danych i należące do biznesu „podglądaczy" – były to strony internetowe, które za niewielką opłatą, a czasem nawet za darmo, w zamian tylko za obejrzenie reklamy, umożliwiały ludziom wyszukiwanie informacji o innych ludziach.

* * *

W przypadku biznesu oferującego dostęp do danych, niewiele jest barier wejścia. Przyjrzyjmy się historii BeenVerified.com. W roku 2007 Josh Levy i Ross Cohen postanowili zaoferować po atrakcyjnej cenie możliwości poszukiwania *online* podstawowych danych[23]. Założyli sklep z danymi, inwestując w niego 200 tys. dolarów. Spółka twierdziła, że do roku 2011 przynosiła już przychody rzędu 11 mln dolarów[24], licząc zaledwie szesnastu pracowników. Niezła praca, jeśli tylko możecie ją dostać.

Biznes baz danych jest w USA w dużej mierze nieuregulowany. Zupełnie inaczej jest w większości krajów zachodnioeuropejskich. Państwa te wymagają[25] od firm gromadzących dane umożliwienia ludziom dostępu do ich danych, korygowania ich, a w niektórych przypadkach, usuwania.

Po przeczytaniu tego, co zostało napisane drobnym drukiem na 212 stronach internetowych stwierdziłam, że tylko 33 z nich daje mi szansę wglądu w informacje o mnie, które przechowują. Po bliższym przyjrzeniu się okazało się jednak, że nie wszystkie z nich były prawdziwymi ofertami. Niektóre wymagały ode mnie założenia konta, w celu przejrzenia danych.

Skontaktowałam się z 23 spółkami prowadzącymi bazy danych i otrzymałam swoje informacje od 13 z nich. Niektóre prosiły mnie o przesłanie wniosku pocztą wraz z kopią mojego prawa jazdy. Innym wystarczyły e-maile. Większość odpowiedzi, które dostałam, pochodziła od największych graczy w branży.

Epsilon, jedna z największych firm zajmujących się marketingiem bezpośrednim, której przychody ze sprzedaży przekraczają 3 mld dolarów rocznie, przesłała mi skąpy, dwustronicowy raport wskazujący moje nazwisko, adres, wiek i poglądy polityczne. Aktualne kategorie zakupowe

podawał w nad wyraz szerokim zakresie: odzież, media, biznes, dom/biuro i sport. Najkonkretniejszą informacją był opis moich prywatnych zainteresowań: rower, bieganie i sport. Dla kogoś, kto od pięciu lat nie wsiadł na rower, to bardziej kwestia aspiracji niż rzeczywistości.

Byłam zaszokowana, że Acxiom, gigant w branży gromadzenia danych, którego roczne przychody sięgały 1,1 mld dolarów, przed udostępnieniem informacji, zażądał ode mnie czeku na 5 dolarów w charakterze opłaty manipulacyjnej[26]. Zacisnęłam zęby i przesłałam pieniądze. Miesiąc później przysłano mi dziewięciostronicowy raport z moim numerem ubezpieczenia, datą urodzenia, informacją o obwodzie do głosowania, w którym jestem zarejestrowana i adresami, pod którymi mieszkałam od czasów dzieciństwa. Nie otrzymałam żadnej informacji, która by dotyczyła moich zainteresowań – a takie właśnie Acxiom sprzedaje na rynku. Niechęć firmy do dzielenia się danymi była szczególnie irytująca, jako że chełpi się ona w swoim rocznym sprawozdaniu posiadaniem ponad „3,000 charakterystyk opisujących niemal każdego amerykańskiego konsumenta".

Jednym z jej podstawowych produktów jest baza danych PersonicX[27], która upakowuje ludzi w siedemdziesięciu „klastrach" w ramach dwudziestu jeden „etapów życia".

Dzięki dziennikarzowi Danowi Tynanowi[28], który robi świetną robotę na polu ochrony prywatności, znalazłam zakładkę na stronie internetowej Acxiom, pozwalającą po wprowadzeniu wieku, stanu cywilnego, dochodu i wieku dzieci, na określenie klastra, do jakiego jest się przypisanym w PersonicX. Gdy wpisałam moje prawdziwe dane (co było nieco denerwujące), Acxiom odpowiedział, że jestem w klastrze zwanym „Szczęście i rodzina" – „którego członkowie są jednymi z najlepiej wykształconych i najzamożniejszych spośród wszystkich grup". Ludzie w tej grupie z dużym prawdopodobieństwem uczęszczali na studia doktoranckie (tak) i są Azjatami (tak, to mój mąż). I prawdą jest też, że: „Ich intensywne życie czyni zakupy w internecie raczej koniecznością niż wyborem". Mimo to zdjęcie obrazujące klaster „Szczęście i rodzina" jest odrobinę absurdalne – widok kobiety i mężczyzny stojących na tle prywatnego odrzutowca. Nasz poziom zamożności nie ma nic wspólnego z prywatnym odrzutowcem. Nie jesteśmy nawet klasą biznes. Jesteśmy tylko klasą ekonomiczną.

Inne klastry Acxioma mają takie nazwy, jak „Stylowe półciężarówki",

„Wyrafinowani żonaci", „Miejski ścigacz", „Terenowy Rover" i „Wystawny styl życia". A jednak nie jest jasne, do którego klastra tak naprawdę przyporządkował mnie Acxiom, ponieważ jego strona demo nie pyta o nazwiska. Acxiom wprowadził z czasem serwis *online*, który pozwalał ludziom na dostęp do informacji o sobie po podaniu nazwiska[29], adresu, daty urodzenia, adresu e-mail i ostatnich czterech cyfr numeru ubezpieczenia. Byłam niechętna podawaniu tych bardzo wrażliwych danych, niemniej, jeszcze raz, zagryzłam wargi i je przesłałam. Rezultat w postaci danych demograficznych był nadzwyczaj marny: Acxiom twierdził, że jestem samotnym rodzicem pochodzenia azjatyckiego, z siedemnastoletnim dzieckiem, który jeździ Toyotą Corollą z 2009 roku – wszystko to było nieprawdą. Jednak informacje o moich zwyczajach zakupowych robiły wrażenie: trafnie wskazywały, że przedkładam zakupy *online* nad *offline*, oraz identyfikowały kategorie, na które wydaję pieniądze: pościel, AGD i odzież kobieca – bielizna i wyroby pończosznicze.

Datalogix, który utrzymuje, że ma dane na temat „niemal każdego amerykańskiego gospodarstwa domowego i transakcji konsumenckich wartych w sumie 1 mld dolarów", potrzebował aż trzech miesięcy, by odpowiedzieć na moje zapytanie[30]. Niemniej pewnego dnia nadeszła koperta FedEx'u z zawartością w postaci dwóch kartek od Datalogix wymieniających moje „zainteresowania" według segmentów. To był dopiero miszmasz. Owszem, jestem mamą i „smakoszem", i „kupującym *online*" „modę i odzież kobiecą", ale nazywanie mnie „fashionistką" oraz „młodą i modną" to chyba o jeden most za daleko.

Podobnie było z moją rodziną, która rzeczywiście kupuje energooszczędne żarówki i mleko ekologiczne. Byłam zaskoczona, że zakwalifikowano nas do „zielonych konsumentów" i amatorów „zdrowej żywności". Z kolei niektóre informacje były zwyczajnie nieprawdziwe: nie mamy żadnych zwierząt ani telewizora, zatem w ogóle nie kupujemy „zaopatrzenia dla zwierząt" ani nie oglądamy „hiszpańskojęzycznej telewizji". Informacje w innych kategoriach Datalogix były z rozmysłem zamaskowane. Pod względem zainteresowań należałam do kategorii: „poglądy polityczne" i „geografia polityczna". Raport jednak nie przypisywał mi żadnych konkretnych przekonań. Tak samo jako kategorie wymienione były: dochód mojego gospodarstwa domowego i wartość domu. Liczb jednak nie ujawniono.

Infogroup przysłał mi ledwie e-maila zawierającego moje nazwisko

i adres – tj. te same informacje, które dostarczyłam, aby uzyskać dostęp do mojego *dossier*. Wielkie dzięki. Lepszą odpowiedź otrzymałam od LexisNexis, innego giganta tej branży. Cztery dni po przesłaniu zapytania, firma odesłała mi darmowy dziesięciostronicowy Accurint Person Report, zawierający każdy adres pod jakim mieszkałam od 1989 roku.

Tak jak raport TLO, był irytująco dokładny. Wyłapał nawet ten jeden miesiąc, kiedy przebywałam w domu moich rodziców, gdy w roku 1996 szukałam mieszkania w San Francisco. Wychwycił dwa miesiące, które spędziłam pomieszkując na strychu u mojego szefa, gdy w roku 1992 byłam na stażu w „Washington Post". Pod „Możliwymi powiązaniami" wymieniono mojego męża i jego matkę oraz daty, kiedy odwiedzała go w jego mieszkaniu w Nowym Jorku.

Thomson Reuters's Westlaw okazał się najhojniejszy, uprzejmie przesyłając mi dwa darmowe raporty: trzydziestoczterostronicowe „podsumowanie", które w większości było zgodne z prawdą, poza faktem, że wskazywało mojego brata jako głowę mojej rodziny, oraz ośmiostronicowy raport „kompleksowy", w którym umieszczono numer rejestracyjny mojego samochodu, informacje o hipotece i nazwę pracodawcy. Raport kompleksowy Westlaw był jedynym, jaki widziałam, który wymieniał źródła informacji o moich dawnych adresach – wszystkie pochodziły z biura informacji kredytowej.

Dostęp do danych oferowany przez wiele innych spółek zdawał się niczym więcej niż tylko mydleniem oczu. Intelius, jedna z największych firm dostarczająca *online* informacji o ludziach, która w 2010 roku (ostatni rok, gdy tę informację podano do wiadomości publicznej) osiągnęła przychody ze sprzedaży na poziomie 150 mln dolarów[31], oddawał do dyspozycji użytkownika stronę internetową o nazwie TrueRep.com, na której można było przeglądać dane. Jednak serwis ten nie ogłaszał się na żadnej ze stron Inteliusa, jakie znalazłam. A kiedy odwiedziłam TrueRep, żeby poszukać swoich danych, ten nie zadziałał. Dopiero gdy skontaktowałam się z firmą, która naprawiła „błąd w programie", uzyskałam dostęp – najpierw musiałam jednak odpowiedzieć na zestaw osobistych pytań, na przykład o to, kiedy został zbudowany mój dom i jakim modelem samochodu jeżdżę. Dziwne, że kiedy już przeszłam przez te pytania, raport nie dostarczył żadnych szczegółów na temat mojego domu i auta. Z całą pewnością więc Intelius musi dysponować większą

pulą informacji, której nie ujawnia. Podał za to prawidłowe nazwiska moich rodziców, męża i brata. Miał też dwa błędne adresy – jeden na Bronksie i jeden w budynku Organizacji Narodów Zjednoczonych.

Mimo wszystko strony oferujące wyszukiwanie osób [ang. *lookup webstites*] zwykle dobrze mnie identyfikowały. Trafnie wskazywały większość moich adresów i określały moje relacje. I w dużej mierze zgodnie z prawdą opisały mnie jako zabieganą, pracującą mamę, skłonną przedkładać wygodę nad oszczędności.

* * *

Miałam nadzieję, że jeszcze więcej prawdziwych informacji odnajdę w królestwie baz danych, które podlega regulacjom – w instytucjach zajmujących się oceną zdolności kredytowej.

Uchwalona w 1970 roku ustawa o rzetelnej informacji kredytowej (Fair Credit Reporting Act) wymaga od każdego, kto wykorzystuje raport kredytowy oraz niektóre inne typy raportów, by informował o przypadkach, w których ludzie – ze względu na dane zawarte w raporcie – ucierpieli wskutek „niepożądanych działań", takich jak odrzucenie ich podań o pracę, ubezpieczenie czy pożyczkę[32]. Nota ta musi dostarczać informacji o podmiocie zbierającym dane, który je dostarczył. Jednak jeszcze do niedawna ludzie wcale łatwo nie uzyskiwali dostępu do swoich raportów, gdyż zawsze z jakiegoś powodu im tego odmawiano.

W 2003 roku Kongres uchwalił prawo nakładające na trzy wielkie agencje informacji kredytowej – TransUnion, Experian i Equifax – wymóg udzielania nieodpłatnego dostępu do rocznych raportów kredytowych na stronie AnnualCreditReport.com[33]. Jednak te darmowe raporty nie ujawniają oceny punktowej, na podstawie której konsumentom przyznaje się lub odmawia pożyczek.

Kiedy zażądałam darmowej kopii mojego raportu od TransUnion, pierwszym sygnałem dla mnie, że coś jest nie tak, było to, że nie mogłam poprawnie odpowiedzieć na pytanie zabezpieczające, zaprojektowane celem weryfikacji mojej tożsamości: „Na poniższej liście wskaż dwa podmioty, dla których pracowałaś". Pracowałam tylko dla jednej spółki z listy, ale nie mogłam przejść dalej, dopóki nie kliknęłam drugiego przedsiębiorstwa. A więc wybrałam jedno na chybił trafił, a i tak dostałam się do swojego raportu. Hmm, to tyle na temat bezpieczeństwa. (Okazuje

się, że nie byłam jedyną osobą, która zauważyła, że pytania zabezpieczające były łatwe do obejścia. W marcu 2013 roku ujawniono[34], że odpowiedzieli na nie hakerzy, w efekcie otrzymując, umieszczone potem w sieci, raporty kredytowe osób publicznych, od Pierwszej Damy Michelle Obamy i dyrektora FBI Roberta Muellera po gwiazdy – Beyoncé i Paris Hilton).

Gdy dobrnęłam już do swojego raportu kredytowego, zauważyłam, że wymieniono mnie jako pracującą od 30 stycznia 2011 roku dla spółki o nazwie Borjomi 1 Inc. Po pobieżnym przeglądzie informacji zawartych w sieci, dowiedziałam się, że Borjomi 1 Inc. jest dystrybutorem butelkowanej wody mineralnej z Gruzji z siedzibą na Brooklynie. Przekręcono także mój poprzedni adres: „304 06920304 T75 Apt 79".

Te moje doświadczenia nie były niczym niezwykłym. Ostatni przegląd wiarygodności raportów kredytowych dokonany przez Federalną Komisję Handlu wykazał, że 26 proc. osób znalazło przynajmniej jeden istotny błąd w co najmniej jednym z trzech dotyczących ich raportów[35].

* * *

Wkrótce jeszcze gorsze informacje na swój temat znalazłam w nieuregulowanym zakątku branży baz danych – biznesie zajmującym się tworzeniem ocen punktowych na podstawie zgromadzonych danych [ang. *data scoring*].

Wpadłam na to, kiedy otrzymałam informacje ze spółki o nazwie eBureau. Był to jednostronicowy raport, który wskazywał, że nie mam dzieci, nie ukończyłam liceum i mam dochody rzędu 35 tys. dolarów – z czego wszystko jest dalekie od prawdy.

Po krótkich poszukiwaniach odkryłam, że eBureau było gorącym, nowym startupem działającym na polu kategoryzowania osób na podstawie danych. Istnieją spółki, które analizują popularność waszych tweetów i postów na Facebooku, aby ocenić, czy jesteście „wpływowi". Są i takie, które skupiają się na nowym rodzaju danych – takich jak osobowość czy aktywność telefonu komórkowego – do budowania alternatywnych ocen punktowych wiarygodności kredytowej.

Mające siedzibę w Chicago, założone w 2004 roku eBureau chce stworzyć lepszy, niż te istniejące, system oceny wiarygodności kredytowej[36]. W tym celu pozyskało kapitał typu *venture* o wartości 38

mln dolarów. Spółka twierdzi, że analizuje informacje o ludziach, przewiduje ich „dostępność" i „całożyciową wartość konsumencką"[37], tak by działy marketingu jej klientów wiedziały, kim się interesować. eBureau promuje swój system ocen punktowych jako mogący mieć zastosowanie względem ludzi o ograniczonej historii bankowej i kredytowej[38], a także jako dobre narzędzie dla windykatorów do przewidywania prawdopodobieństwa spłacenia zobowiązania przez dłużnika[39]. W broszurze reklamowej pisze, że wyniki uzyskiwane w jej „estymatorze dochodów" mogą być wykorzystywane do oceny „nowo przyjętych pacjentów szpitali w kontekście kwalifikowania ich do programów pomocowych"[40].

Gdy skontaktowałam się z eBureau, chcąc sprostować nieścisłości moich danych, otrzymałam e-mailem notę z „Biura Skarg eBureau", powiadamiającą mnie, że niektóre z prezentowanych danych zostały oznaczone jako „oszacowania"[41]. Dodatkowo spółka zauważyła, że „pozyskuje informacje od osób trzecich i ani eBureau, ani ich dostarczyciele, sprzedawcy, licencjodawcy, agenci czy współpracownicy nie gwarantują, że dane te są wiarygodne czy wolne od błędów". Twierdziła też, że jeśli moje dane są nieprawdziwe, mogę je wycofać. Skorzystałam z tej propozycji.

Jeszcze bardziej upiorna była spółka o nazwie PYCO[42], która twierdziła, że jest w stanie określić mój typ osobowości na podstawie nazwiska i adresu. W swoich materiałach marketingowych PYCO przekonuje, że stworzyła „algorytm do inżynierii wstecznej tych danych na zachowania – powiązania, transakcje, działalność, zainteresowania, hobby, zachowania konsumenckie itd.". PYCO otrzymuje informacje od wielkich brokerów danych i poddaje analizie te, dotyczące pewnych życiowych decyzji, a następnie tworzy na ich podstawie opisy osobowości. Na przykład zawarcie małżeństwa może oznaczać gotowość do podejmowania zobowiązań[43]. Następnie firma wykorzystuje dane do określania cech takich jak ekstrawertyzm czy introwertyzm, bycie liderem czy naśladowcą.

PYCO utrzymuje, że stworzyło profile 181 mln dorosłych Amerykanów[44]. Ale twierdzi też, że nie ma wśród nich mojego.

* * *

Na końcu spróbowałam wydobyć swoje dane od amerykańskiego rządu. Agencja Bezpieczeństwa Krajowego (NSA) naturalnie nie udostępniłaby mi żadnych moich akt (inni już próbowali i nie udało im się)[45], mogły jednak to zrobić niektóre urzędy.

Uchwalona w roku 1974 ustawa o prywatności (Privacy Act) daje obywatelom prawo do wglądu w gromadzone przez państwo dane i do prostowania niezgodnych z prawdą informacji. Ale ustawa ta ma gigantyczną lukę: urzędy mogą się same uwolnić od jej przepisów.

W konsekwencji obywatelom nie jest wcale łatwo otrzymać swoje akta. Przyjrzyjmy się historii mieszkanki Ohio, nazwiskiem Julia Shearson[46]. Gdy w 2006 roku wracała do domu po weekendzie spędzonym w Kanadzie, trafiła na posterunek amerykańskiego Urzędu Celnego i Ochrony Granic (U.S. Customs and Border Protection), gdzie okazało się, że jest oznaczona jako „uzbrojona i niebezpieczna" oraz „podejrzewana o prowadzenie działalności terrorystycznej". Agenci federalni zatrzymali ją i jej czteroletnią córeczkę na kilka godzin, a później puścili wolno.

Shearson, która dawno temu przeszła na islam[47], chciała się dowiedzieć, dlaczego została umieszczona na liście obserwacyjnej (co oznacza, że należy albo może należeć do grupy terrorystycznej). Zażądała więc na podstawie ustaw o swobodzie informacji (Freedom of Information Act) i o prywatności (Privacy Act) swoich akt z Urzędu Celnego i Departamentu Bezpieczeństwa Krajowego. W informacjach, które otrzymała, nie znalazła jednak żadnych przyczyn tego stanu rzeczy. Pozwała więc urzędy za naruszenie jej praw wynikających powyższych ustaw, na co te odpowiedziały, że są zwolnione z dostarczania informacji o liście obserwacyjnej. W 2008 roku Shearson otrzymała więcej dokumentów, jednak nigdy nie udało jej się dowiedzieć, dlaczego została oznaczona jako potencjalne zagrożenie dla bezpieczeństwa kraju. W 2011 roku Sąd Apelacyjny dla Szóstego Okręgu orzekł[48], że jeśli państwo bezprawnie przechowuje dane o aktywności chronionej Pierwszą Poprawką do Konstytucji, może być pociągnięte do odpowiedzialności odszkodowawczej. Sprawa trafiła ponownie do sądu niższej instancji. W końcu w 2013 roku Shearson poszła na ugodę po ponad siedmiu latach prawnej batalii[49].

Mimo to wymyśliłam sobie, że sprawdzę, czego mogę dowiedzieć się na swój temat. Zażądałam od FBI dokumentów[50] i zostałam poinformowana, że nie ma na mnie żadnych zapisów (uff!), ale że ta

odpowiedź „nie potwierdza ani nie wyklucza obecności Pani nazwiska na jakiejś liście obserwacyjnej".

Zapytanie przesłane do Urzędu Celnego i Ochrony Granic przyniosło lepszy efekt. Około trzy miesiące od jego złożenia, otrzymałam opasłą kopertę – dość szybka odpowiedź, jak na rządowe standardy.

Do pomocy przy interpretacji tych dokumentów poprosiłam Edwarda Hasbroucka[51], mieszkającego w San Francisco niezależnego pisarza podróżnika, który przez piętnaście lat pracował w branży turystycznej. Zażądał on zapisów o sobie po tym, jak Urząd Celny Stanów Zjednoczonych ujawnił w listopadzie 2006 roku, że zaczął używać systemu zwanego Automated Targeting System (ATS), który kompilował zapisy o podróżach obywateli Stanów Zjednoczonych dla celów „oszacowania ryzyka". Wysłał zapytanie do ATS, które ponowił w 2009 roku. Rok później pozwał urząd twierdząc, że odmowa przekazania wszystkich dotyczących go dokumentów celnych, jest naruszeniem ustawy o prywatności[52]. Przegrał, gdy sąd federalny stwierdził, że Urząd Celny był uprawniony do wyjęcia z mocą wsteczną owych dokumentów spod rygorów przepisów ustawy o prywatności, i to już po tym, gdy ich zażądał.

Hasbrouck zgodził się spojrzeć w moje akta i pomóc mi je rozszyfrować.

Pierwsze osiem stron było z bazy danych TECS[53] – uaktualnionej i zmodyfikowanej wersji dawnego Treasury Enforcement Communications System – która jest rodzajem superbazy danych, zawierającej informacje z różnych działów Departamentu Skarbu i Departamentu Bezpieczeństwa Wewnętrznego. Moje akta w TECS zawierały informacje o międzynarodowych przylotach i wylotach od 1990 roku. Dla każdego przekroczenia granicy odnotowywały lotnisko, datę i godzinę oraz niejasną kategorię o nazwie „wynik", która, jak powiedział Hasbrouck, była prawdopodobnie wskazówką czy byłam wysłana na dodatkową kontrolę lotniskową.

Był to tylko ogólny obraz mojej historii podróży. Informacje o lotach zawierały czas przybycia do strefy celnej, ale już nie to, dokąd leciałam ani skąd przylatywałam. Była tylko jedna wzmianka o „VEH", tj. przekroczeniu granicy pojazdem – kiedy przejechałam do Kanady w Niagara Falls w roku 2003.

Dużo konkretniejszy wgląd w moje podróże zawarty był w drugim zestawie dokumentów – trzydziestojednostronicowej szczegółowej

informacji o międzynarodowych rezerwacjach, pochodzącej z bazy danych zwanej PNR, czyli Imiennego Rejestru Pasażera [Passenger Name Record].

Dawniej PNR-y nie trafiały do rządowych rąk, gdyż są to zapisy handlowe, przechowywane przez linie lotnicze. Jednak po ataku terrorystycznym z 11 września 2001 roku[54], Kongres uchwalił naprędce ustawę o bezpieczeństwie lotniczym i transportowym (Aviation and Transportation Security Act), która wymaga od linii lotniczych dostarczania informacji handlowych o rezerwacjach do Urzędu Celnego „na żądanie". Owo, rozumiane tradycyjnie, „na żądanie", szybko zostało sklasyfikowane jako wymóg przekazania urzędowi przez linie lotnicze elektronicznego dostępu do pełnych baz danych o rezerwacjach lotniczych[55].

Obecnie linie lotnicze rutynowo włączają rezerwacje międzynarodowych podróży swoich klientów do ATS, do którego dostęp dzierży Urząd Celny i Ochrony Granic[56]. Oszacowuje on „zagrożenie", jakie poszczególni podróżujący stanowią dla bezpieczeństwa Stanów Zjednoczonych. Urząd twierdzi, że wykorzystuje dane dotyczące rezerwacji od pięciu lat, ale przechowuje je do celów związanych z walką z terroryzmem od piętnastu lat.

Po 11 września 2001 roku rządy europejskie sprzeciwiły się wprowadzonym przez USA zmianom, argumentując, że naruszają one europejskie przepisy o ochronie prywatności. Po długotrwałej batalii dyplomatycznej i prawnej[57], podczas której Europejski Trybunał Sprawiedliwości na krótko unieważnił porozumienie, Europejczycy w końcu poddali się i podpisali umowę o współpracy. Nie chciano przecież, by obywatele utracili prawo do bezwizowych podróży do Stanów Zjednoczonych[58]. Ale też wymuszono na USA pewne ustępstwa – istnieją ograniczenia co do tego, jak długo Stany Zjednoczone mogą przechowywać i korzystać z danych PNR, zaś prawo dostępu do wrażliwych danych może być realizowane tylko w indywidualnych przypadkach.

Zrozumiałam, o co toczyła się batalia, kiedy zajrzałam do swoich akt. Każdy PNR był niezwykle szczegółowy i opisywał każdą moją interakcję, od momentu zrobienia rezerwacji do wejścia na pokład samolotu.

Był tam wymieniony szereg razy mój pełny numer karty kredytowej, tak samo adres e-mailowy, data urodzenia, numer paszportu i wszystkie numery telefonów – do pracy, domu i komórkowy. Informacje o osobach, z którymi podróżowałam, także się tam znalazły – adres e-mail mojego

męża, daty urodzenia moich dzieci i wszystkie nasze numery paszportów. Imiona moich dzieci (były oznaczone jako CHD1 i CHD2) oraz zamawiane przez nas posiłki wydawały się jedynymi informacjami, które zostały usunięte.

Hasbrouck odkodował zaszyfrowane instrukcje, których linie lotnicze używają do komunikowania się między swoimi terminalami komputerowymi. „OSI YY TCP-4PAX-RECLOC 5CLMWQ/5BUOEM" był we wszystkich systemach sygnałem alarmującym obsługę linii lotniczych, że członkowie mojej rodziny chcą siedzieć razem, i trzeba skompletować grupę (TCP) czteroosobową (4PAX), pomimo że istnieją dwie oddzielne rezerwacje w dwóch różnych zapisach (RECLOC).

Okazuje się, że także moje firmowe biuro podróży dostarczało informacji rządowi federalnemu. W przypadku wylotu do Londynu przesłało Urzędowi Celnemu moją rezerwację hotelową (Bloomsbury Hotel, łoże królewskie), numer mojej firmowej karty kredytowej i datę jej ważności, mój numer identyfikacyjny pracownika, numer do rozliczeń podatkowych oraz wewnętrzny kod oznaczający, że nie jestem VIP-em.

Co jeszcze smutniejsze, biuro przesłało rządowi informację z pola „cel podróży", które reporterzy wypełniają rezerwując wyjazd. Opis ten jest przekazywany do zatwierdzenia szefowi. Szczęśliwie jestem superparanoiczką, więc wpisuję w tych polach tylko „konferencja" albo „podróż dziennikarska". Ale jestem pewna, że niektórzy z moich kolegów mogą w bardziej szczegółowy sposób opisywać swoje plany. Nie byłoby przesadą sądzić, że niektórzy dziennikarze mogli pisać w tej rubryce coś w stylu: „podróż dziennikarska celem spotkania się w Maryland z informatorem, urzędnikiem Johnem Smithem".

Zadzwoniłam do naszych prawników z „Wall Street Journal", którzy byli zaskoczeni, że plany podróży dziennikarzy są przesyłane rządowi. Po weryfikacji tej informacji, rzeczniczka wydawnictwa poinformowała mnie, że było to działanie niezamierzone i dotyczyło międzynarodowych lotów realizowanych przez konkretnego przewoźnika. „Journal" zaprzestanie więc podróży z wykorzystaniem tego przewoźnika, dopóki nie zostanie naprawiona techniczna usterka: 020-56903_ch01_2P.indd 94 11/27/13 8:42 PM. „Ściśle współpracujemy z naszym biurem podróży, aby rozwiązać tę kwestię tak szybko, jak to tylko możliwe", powiedziała mi[59].

A w tym czasie szczegółowe informacje o moich podróżach dziennikarskich tkwiły w rządowych aktach i były analizowane pod

względem ryzyka terrorystycznego, jakie mogę stwarzać dla kraju. Nie mogłam zrobić nic, żeby je usunąć.

* * *

Wyniki mojego audytu były zatrważające. Otrzymałam niewielką ilość dostępnych informacji o mnie. Były one jednak niepokojąco wyczerpujące. Zawierały:

- Każdy adres, pod jakim zamieszkiwałam od czasów college'u.
- Każdy numer telefonu, jakiego kiedykolwiek używałam.
- Nazwiska niemal wszystkich moich krewnych (także tych ze strony męża).
- Listę niemal trzech tysięcy ludzi, z którymi wymieniałam e-maile w ciągu ostatnich siedmiu lat.
- Zapis około dwudziestu sześciu tysięcy wyszukiwań stron internetowych, które prowadziłam każdego miesiąca od siedmiu lat, starannie posortowanych według kategorii, takich jak „mapy" czy „zakupy".
- Ogólny opis moich zwyczajów zakupowych.
- Wewnętrzną korespondencję z moim pracodawcą, czyli „Wall Street Journal", o planach dziennikarskich.

Większość danych o mnie była przechowywana w handlowych bazach danych, ale wszystkie mogły łatwo wpaść w rządowe dragnety.

Nie mogłam się powstrzymać przed porównaniem moich danych do przeglądanych przeze mnie akt Stasi – przedstawiających efekty szczątkowej inwigilacji, dających ograniczony wgląd w życie ludzi. Nawet w swych najśmielszych snach Stasi nie mogła marzyć o tak wielkiej ilości informacji o obywatelach, jakie są dostępne dziś, przy tak niewielkim wysiłku.

7

PIERWSZA LINIA OBRONY

Zanim w ogóle ruszyłam ze swoim projektem dotyczącym prywatności, zostałam zhakowana. Miało to miejsce w trakcie długiego weekendu majowego w 2012 roku. Mój brat z narzeczoną wzięli dzieciaki pod namiot, więc w końcu mogliśmy z mężem pobyć sami w domu.

Nieśpiesznie wstaliśmy w sobotni poranek. Ponieważ nie musieliśmy spieszyć się tak, jak to zwykle bywa – by nakarmić dzieci i zawieźć je na lekcje pływania – usiadłam przy komputerze, aby sprawdzić swoją skrzynkę e-mailową i profil na Twitterze. Od razu moją uwagę przykuło wiele komentarzy od osób, które twierdziły, że otrzymały wiadomości typu SPAM z mojego konta na Twitterze. Sprawdziłam skrzynkę nadawczą i zobaczyłam, że przesłałam dziesiątki wiadomości do znajomych, prosząc ich, aby kliknęli w podane linki. To co się wydarzyło, było dla mnie oczywiste: moje konto zostało zhakowane. „Przepraszam wszystkich, którzy otrzymali ode mnie SPAM. Zostałam zhakowana. Obecnie staram się uporządkować zaistniały bałagan", napisałam o godzinie 9.27 rano.

Usuwanie ponad setki wiadomości zajęło mi godzinę. Na szczęście, nie było poważniejszych konsekwencji. Przecież mogło być znacznie gorzej. Od momentu, kiedy po raz pierwszy zaczęłam korzystać z internetu, utworzyłam dla wielu kont podstawowe hasło, na podstawie powszechnie stosowanego wyrazu, składające się z sześciu znaków. Sprytny haker mógł więc za jego pomocą dostać się do innych moich kont.

Doskonale zdawałam sobie z tego sprawę. Jako dziennikarka specjalizująca się w nowych technologiach, wiedziałam, że powinnam używać długich, skomplikowanych haseł, a do tego dla każdego konta powinnam stworzyć osobne. Od ponad roku prowadziłam dyskusje o najlepszych sposobach zabezpieczania haseł. To było zawstydzające.

Rozważałam wymyślenie słowa-klucza[1], które byłoby wykorzystywane w różnych wariacjach dla każdego z portali, na których się logowałam. Jednak wadą tej metody było to, że nawet jednorazowy atak hakera powodowałby konieczność zmiany wszystkich haseł. Sprawdzałam różne rodzaje oprogramowania do zarządzania hasłami [ang. *password-management software*], ale nie mogłam się zdecydować, czy bardziej ufam płatnemu czy bezpłatnemu programowi. Ponadto, obawiałam się, czy program będzie dobrze działał, uruchamiany jednocześnie w pracy i w domu, gdzie korzystam z różnych komputerów. Rozważałam także sposób zaproponowany przez znajomego hakera, Michaela J.J. Tiffany'ego, znany jako „metoda *loci*". Polega ona na uczeniu się bardzo długich haseł przy użyciu technik, z których korzystali Starożytni Grecy, ucząc się na pamięć długich poematów. Jednak, gdy tylko Michael zaczynał wyjaśniać mi, jak prosta jest to metoda, mnie natychmiast wydawała się skomplikowana.

Podsumowując: przez rok trwałam w wewnętrznych rozważaniach nad właściwym sposobem zabezpieczeń, a jednocześnie używając łatwych do zhakowania haseł, i planowałam je zmienić, gdy tylko obmyślę optymalną strategię.

* * *

Włamanie na moje konto e-mailowe było dla mnie sygnałem ostrzegawczym: zrozumiałam, że zanim będę mogła zająć się kwestią prywatności, powinnam zmienić swój stosunek do bezpieczeństwa.

Bywa, że te dwa zagadnienia uważa się za wzajemnie sprzeczne. W końcu stale prosi się nas, byśmy rezygnowali z prywatności w imię bezpieczeństwa. Zastanówmy się nad kilkoma przypadkami: skanerami do prześwietlania ludzi na lotniskach, programami skanującymi sieć internetową w poszukiwaniu słów związanych z działalnością terrorystyczną, czy kamerami przemysłowymi na rogach ulic.

„Mamy takie powiedzenie w naszej branży: prywatność i bezpieczeństwo są grą o sumie zerowej", mówił w rozmowie z tygodnikiem „New Yorker" Ed Giorgio, konsultant ds. bezpieczeństwa pracujący dawniej dla Agencji Bezpieczeństwa Krajowego (National Security Agency, NSA)[2].

W rzeczywistości jednak prywatność nie może istnieć bez

bezpieczeństwa.

„Musimy odłożyć na bok nasze przekonanie, że wolność i bezpieczeństwo są wartościami przeciwstawnymi, znajdującymi się na szalach wagi – że jeśli jedna jest wyżej, to druga koniecznie musi być niżej”[3], mówiła w 2012 roku Janet Napolitano, sekretarz bezpieczeństwa krajowego USA. „Oczywistym jest, że nie można być wolnym, jeśli żyje się w strachu. Bezpieczeństwo jest podstawowym wymogiem, jeśli chcemy korzystać z umiłowanych przez nas praw”.

Miała rację. Zanim zacznę bronić swoich wolności, powinnam najpierw zabezpieczyć swoją cyfrową przestrzeń. Po co bowiem podejmować działania mające chronić mnie przed powszechnym śledzeniem, skoro jestem podatna na ataki hakerów i innego rodzaju włamania do mojej przestrzeni?

Nie byłam gotowa na to, że ten projekt okaże się tak trudny.

* * *

Problem z cyberbezpieczeństwem [ang. *computer security*][*10] polega na tym, że większość rad, które otrzymujemy, jest absurdalnych.

Weźcie pod uwagę problem pedofilii. W 2008 roku, kiedy pisałam moją książkę o MySpace[*11], największy postrach siali internetowi pedofile. Wielu ekspertów radziło wówczas, by trzymać rodzinny komputer w salonie i sprawować kontrolę rodzicielską, gdy dziecko korzysta z urządzenia. Wskazówka ta była absurdalna i praktycznie niewykonalna[4]. Przecież większość rodziców w ciągu dnia pracuje – w biurze lub w domu. Natomiast dzieci zazwyczaj wykonują na komputerze wiele zadań jednocześnie: odrabiają pracę domową, czatują ze znajomymi i przeglądają strony internetowe. Założenie, że rodzice będą nadzorować wszystkie te czynności, a jednocześnie w tym samym czasie zarabiać na utrzymanie oraz przygotowywać i podawać posiłki, jest po prostu śmieszne.

Zaczęłam myśleć o tych zaleceniach jak o wystających metkach na materacach do spania, na których napisane jest, że ich usuwanie jest nielegalne, albo jak o etykietach na kablach suszarek do włosów – przestrzegających przed ich obcinaniem. Wszystkie te informacje przeznaczone są dla jednego typu odbiorcy – prawników. Reszta z nas podchodzi do nich z niefrasobliwym lekceważeniem lub poczuciem winy,

wynikający z faktu ich lekceważenia.

Niemożliwych do zastosowania jest też większość rad odnoszących się do bezpieczeństwa cyfrowego. Pomyślcie o poradzie, którą znalazłam, korzystając z prostego wyszukiwania: uruchomcie oprogramowanie antywirusowe; zainstalujcie zaporę sieciową [ang. *firewall*]; stwórzcie kopie zapasowe swoich dokumentów; wyłączcie sieć Wi-Fi kiedy z niej nie korzystacie, nie używajcie publicznego Wi-Fi bez zastosowania systemów szyfrujących, zabezpieczcie kablem komputer, gdy jesteście w hotelu (sic!); unikajcie stron wykorzystujących język JavaScript; odinstalujcie stare programy; unikajcie Microsoft Outlook oraz Adobe Reader; zapamiętajcie swój numer IMEI (International Mobile Station Equipment) na wypadek utraty bądź kradzieży telefonu. Część z tych wskazówek jest wartościowa, tj. tworzenie kopii zapasowych czy zachowywanie ostrożności przy korzystaniu z publicznej sieci Wi-Fi. Jednak większość osób, które nie zajmują się technologiami informacyjnymi zawodowo, może mieć problem z rozróżnieniem tego, co jest naprawdę ważne, od tego, co nieistotne.

Jednym z powodów tego zamieszania jest fakt, że musimy się naprawdę wystraszyć, byśmy zechcieli zapłacić za produkty oferowane przez sektor bezpieczeństwa teleinformatycznego. Wyolbrzymianie zagrożeń leży zatem w dobrze pojętym interesie jego graczy. Pamiętacie zapowiadaną katastrofę komputerową, nazywaną problemem roku Y2K, która jednak nie nastąpiła?

Ciekawe spostrzeżenie: większość znanych mi osób, które specjalizują się w bezpieczeństwie cyfrowym, nie polega wcale na programach antywirusowych. Ludzie ci starają się raczej na bieżąco aktualizować system i bardzo skrupulatnie dobierają oprogramowanie, które zainstalują na swoich komputerach. Najważniejsze jednak, że gdy nie mają pełnej wiedzy o źródle danego dokumentu czy odnośnika hipertekstowego, po prostu ich nie otwierają. Ci ze specjalistów ds. bezpieczeństwa, którzy mają największą obsesję na jego punkcie, pilnują, by w sieciach społecznościowych dostępnych było jak najmniej informacji o nich.

Hasła są najlepszym dowodem na absurdalność większości porad dotyczących bezpieczeństwa cyfrowego. Według obiegowej opinii powinniśmy zmieniać hasło co trzy miesiące, a ono samo powinno być silne dzięki zastosowaniu kompilacji znaków i liczb. Nie powinno się też go nigdzie zapisywać.

Te zasady w moim biurze traktowane są jak 10 przykazań. Co trzy

miesiące otrzymuję e-mail z przypomnieniem o zmianie hasła. Zanim wprowadzono tę regułę, miałam dosyć długie hasło składające się z 11 znaków, jeśli dobrze pamiętam. Jednak stała presja na wymyślanie nowych haseł sprawiła, że stopniowo moja kreatywność zaczęła maleć. Poddałam się w 2012 roku i zaczęłam tworzyć hasła, których podstawą był wyraz określający miesiąc, w którym otrzymywałam e-mail z przypomnieniem. Kiedy więc otrzymałam taką wiadomość w marcu, zmieniłam hasło na Marzec2012! (z wymaganym wykrzyknikiem, aby zadowolić kontrolę). W czerwcu, zmieniłam na 2012Czerwiec? itd. Zatem mój poziom ochrony spadł do dziewięciu łatwych do odgadnięcia znaków.

Dowodów na to, że nie jestem jedyną osobą, która idzie na skróty, jest masa. W 2010 roku, badacze z dziedziny bezpieczeństwa cyfrowego[5] przeanalizowali bazę ponad 32 milionów haseł, które zostały zhakowane i na krótko umieszczone w sieci. Odkryli, że najpopularniejszym stosowanym zabezpieczeniem jest sekwencja cyfr: „123456". Inne powszechnie stosowane kompilacje to: „12345", „123456789" czy po prostu „hasło". Analitycy firmy Imperva[6], działającej w obszarze bezpieczeństwa teleinformatycznego, ustalili, że co trzecie hasło składało się z mniej niż siedmiu znaków, a co drugie wykorzystywało imię bądź wyraz powszechnego użytku (słownikowy). Rezultat był następujący: „Przy zaledwie stu dziesięciu próbach, haker będzie w stanie uzyskać dostęp do nowego konta co sekundę albo będzie potrzebował tylko siedemnastu minut, by włamać się do tysiąca kont".

Z nowszego badania z 2013 roku wynika, że niewiele się w tej kwestii zmieniło. Ofcom (Office of Communications), brytyjski regulator telekomunikacyjny odkrył[7], że połowa dorosłych internautów w Wielkiej Brytanii posługuje się tym samym hasłem, korzystając z różnych, wymagających logowania, stron internetowych. Ponadto, 26 proc. respondentów przyznało, że używa łatwych do odgadnięcia haseł, takich jak data urodzin czy imię.

Na szczęście, informatycy doszli także do wniosku, że to wcale nie my jesteśmy winni tworzenia tak fatalnych haseł. Ross Anderson z Laboratorium Cyfrowego Uniwersytetu Cambridge pisze w swej bardzo chwalonej książce *Security Engineering*, że: „Kwestię haseł zgrabnie sprowadza się do dwóch czynności: wybierz hasło, którego nie pamiętasz i nie zapisuj go"[8].

W 2004 roku Instytut Inżynierów Elektryków i Elektroników (Institute

of Electrical and Electronic Engineers) opublikował badanie „Password Memorability and Security”[9], którego współautorem był Anderson. Wnioski były następujące: niedoskonałość haseł wynika po części z instrukcji, które otrzymują, jeśli w ogóle, ludzie tworzący hasła.

Autorzy przeprowadzili eksperyment dotyczący tworzenia haseł na około trzystu studentach. Jedna grupa została poproszona o wymyślenie własnych kompilacji, składających się co najmniej z siedmiu znaków w tym jednego, który nie będzie literą. Członkowie drugiej grupy dostali kartkę z literami i cyframi, z zaleceniem, by spośród z zamkniętymi oczami wybrali spośród nich osiem przypadkowych znaków. Natomiast trzeci zespół został poproszony o stworzenie szyfru metodą mnemoniczną – czyli na przykład zapisanie zdania: „Jest 12:00 w południe, jestem głodny”, w następujący sposób: „J12wp, jg”. Następnie badacze starali się złamać hasła, posługując się różnymi technikami hakerskimi. Udało im się rozpracować co trzecie hasło stworzone przez pierwszą grupę (użytkownicy nie otrzymali szczegółowych instrukcji) i mniej niż co dziesiąte w dwóch kolejnych zespołach. „Zalecamy zmianę instrukcji, które otrzymują użytkownicy haseł”, brzmiał jeden z wniosków badaczy. W niektórych przypadkach, powinno się podpowiadać, jak tworzyć hasła metodą mnemoniczną, a w innych po prostu przydzielać je użytkownikom. Pozostawieni sami sobie, „użytkownicy rzadko wybierają hasła, które są jednocześnie trudne do zgadnięcia i łatwe do zapamiętania”.

W 2010 roku także informatycy z University College London uznali, że winą za słabe hasła obarczyć należy stosowaną przez instytucje politykę haseł. Autorzy przeanalizowali „hasła w środowisku naturalnym” dwóch dużych organizacji i zauważyli, że zbyt restrykcyjna polityka haseł[10] – na przykład zmuszająca użytkowników do częstej ich zmiany – przynosiła efekt odwrotny od zamierzonego: zestresowani użytkownicy zapisywali swoje hasła, tym samym osłabiając zabezpieczenia. „Kiedy wymagania związane z polityką [bezpieczeństwa] przekraczają możliwości pracowników, są oni zmuszeni znaleźć bardziej wyrafinowaną, bądź wręcz przeciwnie – mniej bezpieczną – metodę radzenia sobie z problemem”, skonkludowali autorzy raportu.

Wielu ekspertów ds. bezpieczeństwa teleinformatycznego twierdzi zresztą, że nie ma nic złego w zapisywaniu swych haseł, pod warunkiem, że trzyma się je w bezpiecznym miejscu[11].

W 2005 roku na konferencji poświęconej cyberbezpieczeństwu, Jesper Johansson, wówczas starszy menedżer programu polityki bezpieczeństwa w Microsoft, skrytykował branżę za udzielanie złych porad dotyczących haseł[12].

– Jak wielu z was ma w swojej firmie politykę, która zabrania zapisywania haseł pod rygorem śmierci? – zapytał uczestników. Większość z nich podniosła ręce.

– Uważam, że jest zupełnie niewłaściwe. Sądzę, że polityka haseł powinna umożliwiać notowanie. Sam korzystam z sześćdziesięciu ośmiu różnych haseł. Gdybym nie mógł zapisać żadnego z nich, zgadnijcie, co bym zrobił? Używałbym wszędzie takiego samego. Jako że nie wszystkie systemy umożliwiają korzystanie z dobrego hasła, wybrałbym naprawdę beznadziejne, używał go i nigdy nie zmieniał. Jeśli więc zapiszę hasła na kartce i ją zabezpieczę, albo jeśli zapiszę je na czymkolwiek innym, to nie ma w tym nic złego. To pozwala na zapamiętanie większej liczby lepszych haseł".

Lektura raportów z badań pomogła mi poczuć się lepiej po moim doświadczeniu ze słabymi hasłami. Jednak nie rozwiązywało to mojego problemu, jakim było stworzenie dziesiątek silnych zabezpieczeń.

Przecież haseł mnemonicznych jest tylko tyle, ile jestem w stanie zapamiętać. A korzystanie z wielu stron internetowych, wcale nie jest warte wysiłku intelektualnego.

* * *

W dniu, w którym zostałam zhakowana, zmieniłam hasło do ważniejszych kont: skrzynki e-mail, konta bankowego i portali społecznościowych. Zamiast wymyślić różne wariacje sześcioznakowego słowa, stworzyłam dłuższe kombinacje liter, cyfr i symboli, zapisując je na kartce papieru.

Było to tymczasowe rozwiązanie. Wiedziałam, że moje hasła nadal nie były wystarczająco dobre. Stanowiły wciąż tylko pewną odmianę tekstu szyfrującego. Jednak gdy tylko starałam się wymyślić nowe frazy, czułam w głowie pustkę. Przypomniało mi się badanie, z którego wynikało, że aż 38 proc. dorosłych wolałoby wykonywać obowiązki domowe (takie jak czyszczenie toalety czy mycie naczyń) niż tworzyć nowy login i hasło[13].

Po kilku tygodniach intelektualnego odrętwienia, poddałam się.

Postanowiłam zainstalować oprogramowanie do zarządzania hasłami. Jako że przyświeca mi filozofia „płacenia za jakość" wybrałam program 1Password. Jest on odpłatny i ma bardzo dobre recenzje. Miałam w związku z tym nadzieję, iż jest to autentyczne przedsięwzięcie, które nie będzie stanowiło przykrywki dla innych działań. Ponadto, liczyłam na dobry poziom obsługi klienta.

Program 1Password jest przede wszystkim sejfem dla haseł: umożliwia ich przechowywanie. Sejf otwiera się jednym nadrzędnym hasłem. Firma, aby zapewnić bezpieczeństwo haseł, nie przechowuje ich na swoich serwerach w Kanadzie, lecz na komputerach użytkowników, w zaszyfrowanych plikach. Jeśli zapomnicie głównego hasła, tracicie dostęp do wszystkich swoich haseł. Innymi słowy, 1Password zdał wspomniany wcześniej test kałuży błotnej [ang. *mud puddle test*].

Umieszczenie wszystkich haseł na komputerze wydawało mi się przerażające. Zdecydowałam się jednak na to, po skonfrontowaniu się z pustką w mojej głowie przy wymyślaniu fraz. Pobrałam program i zaczęłam wprowadzać do niego hasła stopniowo, odwiedzając kolejne strony.

Był to naprawdę powolny proces. Zapomniałam na ilu stronach hoteli, programów lojalnościowych linii lotniczych czy serwisów sprzedażowych miałam założone konta. Postanowiłam, że na niektórych z nich skorzystam z generatora haseł 1Password, aby stworzyć takie o odpowiedniej długości i kombinacji znaków. Na mniej istotnych portalach używałam słabego hasła, obiecując sobie, że kiedyś je zmienię.

W ciągu trzech miesięcy wprowadziłam pięćdziesiąt jeden haseł do programu 1Password. Mimo to, nadal z nieufnością podchodziłam do pomysłu umieszczenia tam zabezpieczeń do konta bankowego czy e-mailowego, albo haseł dostępu do innych ważnych plików roboczych. Takie hasła postanowiłam zapisać na kartce papieru. I od razu zaczęłam mieć problem – nie potrafiłam bowiem odróżnić jednych haseł od drugich. Te, które stworzyłam za pośrednictwem 1Password stanowiły niezrozumiałe ciągi znaków w stylu qwER43@! Natomiast te, które wymyśliłam sama, były kombinacją słów i cyfr, np. Tr0ub4dour&3. Żadne z nich nie były łatwe do zapamiętania.

Zdziwiłam się jak często potrzebuję tych haseł, gdy jestem z dala od komputera. Raz zadzwonił do mnie mąż, pytając o dostęp do konta Amazon, by skorzystać z bezpłatnej dostawy. Odpowiedziałam mu, że jestem na lunchu i nie mogę sprawdzić hasła. Innym razem mąż napisał

do mnie e-maila, bym podała mu hasło do jednego z kont programu lojalnościowego linii lotniczych. Także nie miałam do niego dostępu. Kiedy dostałam nowy telefon, chciałam skonfigurować konto na Twitterze, będąc z dala od komputera. Wtedy przypomniałam sobie, że przecież nie znam hasła do swojego konta. (1Password ma także wersję mobilną, ale uznałam, że przechowywanie wszystkich haseł w telefonie byłoby zbyt ryzykowne)

Byłam poirytowana. W końcu jednak zrozumiałam, że te niby awaryjne sytuacje wcale takimi nie były: zarówno „ćwierkanie" w sieci jak i zamówienie na Amazonie mogły poczekać.

* * *

W międzyczasie zaczęłam chronić swoje dane także na inne sposoby. Aby zabezpieczyć się przed możliwością podszycia się pode mnie (inaczej: kradzieżą tożsamości), kupiłam niszczarkę i zaczęłam pozbywać się dokumentów zawierających moje dane osobowe. Ponadto, nabyłam portfel blokujący nadawanie sygnału radiowego (RFID)[14], który to sygnał hakerzy potrafią przechwytywać celem pozyskania danych z kart kredytowych i dowodu.

Kupiłam także dysk zewnętrzny i zaczęłam tworzyć kopie zapasowe plików, aby zabezpieczyć dane na wypadek poważniejszego włamania. (Tak, wcześniej tego nie robiłam. I wiem, to straszne). Zaszyfrowałam swój twardy dysk, aby pokrzyżować plany potencjalnym hakerom, gdyby dostali się do mojego komputera. (Operacja ta wymaga na Macu jednego kliknięcia).

Zakleiłam naklejką kamerkę internetową mojego komputera, aby hakerzy nie mogli mnie zdalnie podglądać. Kupiłam filtr prywatyzujący, który chroni ekran mojego laptopa przed wzrokiem osób zerkających mi przez ramię bądź siedzących w fotelu obok w samolocie.

Chciałam zabezpieczyć się przed hakerami potrafiącymi wykradać hasła za pośrednictwem Wi-Fi dostępnego w kawiarniach[15]. Zainstalowałam więc oprogramowanie HTTPS Everywhere, szyfrujące połączenie z Internetem w każdym możliwym momencie.

Stałam się też w ogóle bardziej ostrożna w korzystaniu z Wi-Fi. Zamiast polegać na swoim domowym ruterze, podłączyłam do komputera sieciowy kabel ethernetowy. W czasie podróży zaczęłam korzystać

z przenośnego hot spotu Wi-Fi. Połączenie bywało nierówne, ale czułam się z tym dużo lepiej niż przyłączając się do tych wszystkich inwazyjnych systemów Wi-Fi dostępnych w hotelach, które wymagają, by przechodził przez nie cały ruch generowany przez was w sieci.

Kiedy było to możliwe, ustawiałam także podwójny system zabezpieczeń, znany jako dwuetapowe uwierzytelnienie [ang. *two-factor authentication*]. W przypadku Gmaila oznaczało to zainstalowanie aplikacji, która generowała dla mnie dodatkowy kod, potrzebny, poza hasłem, do zalogowania się na koncie[16]. W profilu bankowości elektronicznej musiałam gruntownie przejrzeć ustawienia dostępu *online*, aż znalazłam sposób na to, by system wymagał autoryzacji wszystkich płatności kodem PIN.

Wprowadziłam te ustawienia wyłącznie dla tych usług, które nie wymagały od mnie podawania mojego numeru telefonu. Twitter oferował dwuetapowe uwierzytelnienie wyłącznie tym użytkownikom, którzy zgodzili się otrzymywać od serwisu wiadomości SMS, więc zrezygnowałam z tego.

Spróbowałam także pracy z systemem zwanym Little Snitch, aby móc kontrolować wszystkie połączenia, które próbuje nawiązać mój komputer[17]. Szybko jednak porzuciłam to rozwiązanie. Okazało się, że naprawdę nie chcę wiedzieć, ile połączeń nawiązuje moje urządzenie w danym momencie. Odkryłam, że muszę zaakceptować aż siedemdziesiąt sześć połączeń, aby otworzyć przeglądarkę, uruchomić Gmaila czy puścić muzykę ze Spotify. Każde żądanie dostępu wyglądało następująco: „Pozwolenie na połączenia wychodzące do portu 80 (http) z d1hza3lysoht.cloudfront.net aż do wyjścia z programu Spotify". Miałam do wyboru dwie opcje: zezwalać na to „zawsze" albo „do zakończenia połączenia". Przez godzinę podjęłam 97 bezsensownych decyzji, więc zrozumiałam, że nie wiem co tak naprawdę robię i odinstalowałam oprogramowanie.

Kiedy rozważałam różne sposoby zabezpieczeń, doszłam do wniosku, że największym problemem jest to, iż nie wiem komu ufać. Miałam wystarczającą wiedzę, aby być świadomą różnych cynicznych zagrywek, żerujących na ludzkim strachu. Jednak nie znałam się na tym na tyle, by potrafić testować produkty i ocenić, na ile dobrze działają.

Dotąd korzystałam z powszechnie uznanych narzędzi albo pochodzących od znanych mi osób. Ufałam inżynierom z Electronic Frontier Foundation,

którzy stworzyli oprogramowanie HTTPS Everywhere. Program Little Snitch był dobrze znanym programem, podobnie jak i 1Password. Nie wiedziałam jednak, co myśleć o usłudze szyfrującej dane w chmurze, zwanej SpiderOak, z której miałam zamiar skorzystać. Chciałam przechowywać swoje dane w chmurze, aby mieć do nich dostęp z dowolnego miejsca, a także na wypadek, gdyby coś stało się z moimi fizycznymi kopiami zapasowymi. Niestety, SpiderOak nie był dobrze znany.

Nie byłam w stanie właściwie ocenić firmy na podstawie jej strony internetowej. Podobało mi się to, że nie przypominała większości stron firm działających w obszarze bezpieczeństwa cyfrowego[18], które zazwyczaj mają ciemne tło i nawiązują do „szyfrowania na poziomie wojskowym". Strona SpiderOak była utrzymana w pogodnej pomarańczowej tonacji i oferowała „środowisko oparte na dowodzie o wiedzy zerowej" [ang. *zero-knowledge privacy environment*], który w zamyśle przypomina wspomniany już eksperyment myślowy – test kałuży błotnej. SpiderOak został mi polecony przez Christophera Soghoiana, inżyniera z American Civil Liberties Union. Jednak sama strona i rekomendacja nie były przystawką wystarczającą dla kogoś, kto chce zjeść pełnowartościowy posiłek. Napisałam więc do prezesa firmy, Ethana Obermana i zarezerwowałam czas na spotkanie podczas mojego kolejnego pobytu w San Francisco.

Spotkaliśmy się w modnej kawiarni. Ze swoimi blond włosami i umięśnionymi ramionami, Ethan wyglądał raczej na bywalca siłowni niż maniaka komputerowego [ang. *geek*]. Zaczęłam przyglądać mu się sceptycznie.

Swoją historię opowiedział mi przy kawie[19]. W istocie, nie była to typowa opowieść informatyka. Wychował się na przedmieściach Chicago, poszedł do liceum z internatem, Hotchkiss, by następnie trafić na Uniwersytet Harvarda. Tak jak się domyślałam[20], był hokeistą i kapitanem drużyny lacrosse[*12]. Ukończył studia w 2000 roku i zaczął pracować w firmie ojca[21], która pomagała wydawcom zarządzać danymi dotyczącymi sprzedaży. Przedsiębiorstwo potrzebowało strategii cyfryzacji, toteż Ethan zaproponował e-mailowe działania marketingowe. Jednak po kilku latach miał dosyć pracy w rodzinnym przedsięwzięciu. Postanowił zrobić sobie przerwę i zaczął podróżować. Wtedy też kupił swój pierwszy komputer firmy Macintosh. Gdy dzwonił do mamy

z prośbą o przesłanie mu jakichś plików z jego komputera stacjonarnego, który przechowywał w garderobie rodziców, dostrzegł rynkową szansę.

Na rynku było wiele usług oferujących możliwość tworzenia kopii zapasowych, takich jak Xdrive czy Mozy, jednak każda z nich oferowała kopiowanie zawartości pojedynczego urządzenia. On natomiast chciał zsynchronizować swoje dane znajdujące się na różnych komputerach. „Tworzenie kopii zapasowych nie jest *sexy*. To obowiązek, taki jak mycie zębów. To, co jest naprawdę sexy to dostęp do twoich danych z dowolnego miejsca", wyjaśnił mi.

Słowo *sexy* nie było dokładnie tym, o co mi chodziło. Chciałam raczej dowiedzieć się czegoś więcej o wykorzystywaniu przez firmę procedury „dowodu o wiedzy zerowej". Ethan z radością odesłał mnie do jego partnera biznesowego, Alana Fairlessa (szczerze mówiąc, Ethan nie był pewnie przyzwyczajony do dziennikarzy, którzy wymagali od niego czegoś więcej oprócz cytatu do chwytliwego nagłówka artykułu prasowego). Sam sprawiał wrażenie człowieka, który w jednym palcu ma finanse firmy. Powiedział mi, że jego przedsiębiorstwo jest rentowne i zarabia głównie na sprzedaży subskrypcji, mniej na reklamach. Pozostawało to w zgodzie z moją zasadą „płacenia za jakość".

Dwa tygodnie później rozmawiałam przez telefon z Alanem, współpracownikiem Ethana i dyrektorem ds. technicznych (CTO) w SpiderOak[22]. Alan wytłumaczył mi, że to jemu zależało na szyfrowaniu danych. „Było dla mnie ważne, aby [dane] były zaszyfrowane zanim zostawię swój komputer", powiedział. Jednocześnie wyjaśnił jak firma zbiera hasła użytkowników i na czym polega unikalny sposób ich szyfrowania. Sam szyfr jest tak silny, jak hasło, które stworzy użytkownik. „Nie ma wymagań co do długości hasła. Uznaliśmy, że zachęcanie użytkowników do zmiany sposobów tworzenia haseł nie jest najlepszym pomysłem, skoro mówimy im, że jeśli zapomną hasła to utracą dane".

Po tym, czego dowiedziałam się o hasłach, spodobało mi się podejście firmy SpiderOak, która nie zmusza użytkowników do zajęcia przegranej pozycji. Alan zaskarbił sobie moje uznanie, mówiąc że w jego firmie „model oceny ryzyka opiera się na ochronie użytkownika przed nim samym, co zdaje się także być dobrą tarczą przed resztą świata".

Przyznał, że firma otrzymywała już żądania udostępnienia danych ze strony organów ścigania. Gdy jednak funkcjonariusze dowiadywali się, że przedsiębiorstwo nie ma jak odszyfrować danych, rezygnowali.

Odetchnęłam z ulgą. Bezpośrednia rozmowa o modelach oceny ryzyka i hasłach sprawiła, że uznałam mojego rozmówcę za wiarygodnego. Firma przeszła z powodzeniem test. Wykupiłam subskrypcję. Jednak sposób, w jaki doszło do zakupu przeze mnie tej usługi był raczej niedorzeczny. Czy naprawdę muszę odwiedzić wszystkich technologicznych usługodawców, aby sprawdzić ich wiarygodność?

Poza wszystkim, moje bezpieczeństwo na SpiderOak wciąż zależało od siły mojego hasła.

* * *

Kiedyś trzeba było posiadać pewne umiejętności, aby złamać hasło. Obecnie może to zrobić każdy.

Zwiększenie mocy obliczeniowej komputerów pozwoliło hakerom działać szybciej[23]. Coraz łatwiej dostępne długie listy haseł logowania do różnych portali, pochodzące z wycieków danych, umożliwiły programistom stworzenie programów do skutecznego łamania haseł. By pokazać, że nie nastręcza to trudności, dziennikarz Nate Anderson złamał 800 haseł jednego dnia, korzystając z darmowego programu online Hashcat[24]. „Wiedziałem, że łamanie haseł jest dziś proste, ale nie miałem pojęcia, że tak bardzo. W każdym razie, odkąd przezwyciężyłem chęć zmiażdżenia swojego komputera młotkiem i zrozumiałem w końcu, co robię, stało się to absurdalnie banalne".

Oto, na czym polega łamanie haseł (w dużym uproszczeniu):

- Haker otrzymuje listę haseł do złamania.
- Listy są zazwyczaj zaszyfrowane bądź „zahaszowane".
- Haker przystępuje do odkodowania skrótów (do odhaszowania).
- Zazwyczaj na początku haker próbuje przeprowadzić atak „słownikowy", polegający na porównaniu skrótów z wyrazami powszechnego użytku.
- Haker następnie porównuje wzorce haszowania do tych znanych z baz danych zawierających hasła.
- Później haker przypuszcza atak brutalnej siły [ang. *brute force attack*], który polega na sprawdzaniu prostych sekwencji takich jak „aaaaaa", „aaaaab" i „aaaaaac" itd.

Robert Graham, badacz specjalizujący się w bezpieczeństwie cyfrowym, twierdzi, że ataki brutalnej siły są „problemem natury wykładniczej”[25]. Według niego „ilość czasu, której wymaga przeprowadzenie go, szybko zaczyna przekraczać zdroworozsądkowe granice”. Z tego powodu, Anderson przeprowadzał takie ataki wyłącznie na hasłach nieprzekraczających sześciu znaków[26]. Oszacował, że gdyby próbował złamać hasła składające się z dziewięciu lub dziesięciu symboli, zajęłoby mu to kilka tygodni lub miesięcy. Był w stanie rozpracować jedynie osiemset z siedemnastu tysięcy haseł. „Wniosek był oczywisty: mogłem złamać każdy ostatni symbol w ciągu znaków. Aby jednak to zrobić, potrzebowałbym większej części roku, przy założeniu, że moje urządzenie nie padłoby w wyniku przeciążenia”.

Lekcja, która płynie ze świata łamaczy haseł, jest następująca[27]: ci, którzy przechowują hasła, powinni je lepiej szyfrować. Jedną z dobrych praktyk jest tak zwane „solenie” [ang. *to salt*] szyfru – polega to na tym, że gdy użytkownik tworzy sześcioznakowe hasło, kodujący dodaje do niego kilka dodatkowych symboli, sprawiając, że jeszcze przed zahaszowaniem, staje się dłuższe. Dzięki temu jest trudniejsze do złamania.

Niestety, „solenie” nie jest jeszcze powszechne[28]. Ostatnie włamania do LinkedIn, Yahoo! i eHarmony ujawniły zasoby „nieposolonych” szyfrów, które zostały szybko złamane.

Wszyscy ci, którzy tworzą hasła, powinni ze świata hakerów wysnuć jeden wniosek: dobrze jest tworzyć długie hasła, unikając słów słownikowych i często stosowanych wyrazów (takich jak „hasło1”).

* * *

Miarą siły hasła jest poziom czegoś, co informatycy nazywają „entropią informacyjną”. Im wyższy poziom entropii, tym trudniejsze do złamania jest hasło. Jeffrey Goldberg, ekspert z AgileBits, twórcy usługi 1Password, powiedział mi, że entropia wskazuje „na jak wiele sposobów możecie osiągnąć różne wyniki, wykorzystując te same metody”[29]. Krótkie, proste hasła, na przykład oparte na wyrazach powszechnego użytku, mają niską entropię, ponieważ łatwo je odgadnąć. Dłuższe hasła, zawierające różne rodzaje symboli, litery i cyfry, mają wyższą entropię, gdyż rozpracowanie ich wymaga większej liczby prób odgadnięcia.

Wiedział to Julian Assange[30], kiedy tworzył następujące hasło do bazy dokumentów WikiLeaks[*13]:

AcollectionOfDiplomaticHistory-Since_1966_ToThe_PresentDay#

Jest to łatwe do zapamiętania hasło, złożone z 58 znaków, z niewieloma symbolami. Oczywiście, znamy je, ponieważ dziennik „The Guardian" opublikował je w wydanej przez siebie książce o WikiLeaks. Pod wieloma innymi względami nie było to więc hasło bezpieczne.

Niezwykle trudno jest oszacować poziom entropii. Długie hasło może mieć niską entropię, jeśli skomponowane jest z prostych słów i oczywistych zasad. Zaczęłam mieć obsesję na punkcie poziomu entropii moich haseł. Jednego dnia, gdy czekałam na występy taneczne córki, trafiłam na wirtualny wskaźnik entropii stworzony przez Dana Wheelera, inżyniera z Dropboxa[31]. Jego narzędzie mierzyło poziom entropii każdego hasła, a także czas potrzebny do jego złamania. Natychmiast poczułam dreszczyk emocji związany z możliwością przetestowania dopiero co stworzonych, mnemonicznych haseł. Lekkomyślnie zaczęłam je wszystkie wprowadzać do systemu.

Zaczęłam od mojego hasła do konta bankowego (stworzonego przy użyciu technik mnemonicznych, składającego się z 12 znaków). Och, to bardzo ekscytujące. Jego entropia wynosiła 56., a złamanie zajęłoby „wieki"!

Następnie sprawdziłam moje hasło do konta Gmail, stworzone przez 1Password (osiemnaście znaków). Entropia wyniosła 80. Łamanie tego hasła także trwałoby całe wieki. Mimo tego, nie znoszę tego hasła: nie jestem w stanie go zapamiętać.

Natomiast moje hasło do skrzynki e-mail w „Wall Street Journal" (dziewięć znaków) było rozczarowująco słabe. Chociaż stworzyłam je przy użyciu metody mnemonicznej, jego poziom entropii wynosił zaledwie 28. Można by je rozpracować w ciągu siedmiu godzin!

O rety, jak to się stało? Podczas gdy hasło, którym zabezpieczam swoje konto na 1Password (kolejne stworzone przy użyciu techniki mnemonicznej, składające się z siedemnastu znaków) miało wynik 37. i mogło zostać złamane w ciągu 5 miesięcy. Ech.

Było to zajęcie wciągające, a zarazem przygnębiające. Wszystko układało się w pewną spójną całość: hasła stworzone przez 1Password były bardzo silne, ale siła tych wymyślonych domowymi sposobami była bardzo różna: od naprawdę dużej do niewielkiej.

Najgorzej było z moim hasłem do komputera: można było je złamać w ciągu czterech minut. Natomiast, zabezpieczenie do bloga można było ominąć w „chwilę".

Kiedy emocje związane ze sprawdzaniem haseł opadły, zdałam sobie sprawę, że zachowałam się nad wyraz głupio: używając Wi-Fi, wprowadziłam do nieznanego systemu łamiącego kody [ang. *cracking system*] wszystkie moje hasła. Mimo, że korzystałam ze swojego prywatnego, przenośnego punktu dostępu do sieci i zaszyfrowanego połączenia, a strona obiecywała nie przechowywać haseł, istniało ryzyko, że trafią one do bazy użytkowanej przez hakerów.

Miałam teraz dwa powody, by stworzyć nowe hasła: 1) fakt, iż obecne nie miały odpowiedniego poziomu entropii; 2) moja własna głupota.

W poszukiwaniu haseł o wysokim poziomie entropii, zastanawiałam się nad wieloma możliwościami, włączając w to hasła wykorzystujące mało znane języki i długie frazy, takie jak stosował Julian Assange.

Jednak ponownie zderzyłam się z problemem, jaki stanowił mój umysł. Mogłam wymyślić jedno lub dwa słowa w mało znanym języku, bądź jeden czy dwa ciągi wyrazów. Ostatecznie jednak pomysły by mi się skończyły i zaczęłabym tworzyć słabe hasła.

Z badań wynika, że nawet jeśli ludzie wymyślają dłuższe hasła, to szukają drogi na skróty. W 2012 roku, badacze z Uniwersytetu Cambridge przeanalizowali[32] wykorzystywane przez ludzi ciągi wyrazów i zaobserwowali, że wiele z nich opartych jest na tytułach znanych filmów, utworów muzycznych czy sentencjach, np. „stowarzyszenie umarłych poetów", „three dog night"[*14] lub „with or without you"[*15]. W konsekwencji, wiele ciągów było tak słabych jak zwykłe hasła. „Wyniki wskazują, że użytkownicy nie są w stanie tworzyć fraz z zupełnie przypadkowych słów. Wyraźnie inspirują się oni zdaniami występującymi w ich codziennym języku", podsumowywali Joseph Bonneau i Ekaterina Shutova.

Badania potwierdziły moje podejrzenia: potrzebowałam rozwiązania, które zwolniłoby mnie z konieczności myślenia.

Znalazłam je w systemie haseł zwanym Diceware[33]. Sprawa jest zwodniczo prosta: rzucacie pięciokrotnie sześcienną kostką i z zapisanych wyników wybieracie słowo na liście Diceware, zawierającej 7 776 krótkich słów w języku angielskim. Każde słowo jest ponumerowane.

Wygląda to następująco:

- 16655 paragraf
- 16656 pazur
- 16661 glina
- 16662 czysty
- 16663 przejrzysty
- 16664 łącznik
- 16665 złamanie, rozszczepienie
- 16666 ekspedient

Twórca Diceware, Arnold Reinhold, zaleca wykorzystanie ciągu składającego się z co najmniej pięciu słów. W takim przypadku hasło wygląda mniej więcej tak: „algier klm curry blond duszek". Można stworzyć mocniejsze hasło, dodając więcej słów, liter, symboli czy wielkich liter. Jednak, jak twierdzi Bruce Marshall, założyciel PasswordResearch.com, złamanie nawet prostego szeregu pięciu wyrazów, z których każdy składa się z pięciu małych liter, musiałoby zająć ponad 180 dni[34].

Wykorzystanie kostki gwarantuje, że wybierzecie przypadkowe cyfry. Oczywiście, są także strony internetowe, które wygenerują dla was przypadkowe znaki. Jednak Reinhold i inni specjaliści ds. bezpieczeństwa odradzają tę metodę. Nieznane strony mogą być bowiem stworzone przez przeciwników, chcących łamać nasze hasła. Jak pokazują dokumenty udostępnione przez Edwarda Snowdena, faktycznie tak się dzieje: NSA opracowała jeden z naukowych standardów generowania losowych liczb i potrafiła złamać jego algorytm[35].

Podekscytowana wizją, że już nigdy więcej nie będę musiała wymyślać hasła, wydrukowałam trzydziestosiedmiostronicową listę słów firmy Diceware, którą podziurkowałam i umieściłam w segregatorze. Jednak perspektywa rzucania kostką setki razy, aby stworzyć konieczne hasła, zniechęcała mnie. Segregator leżał na biurku tak długo, aż wpadłam na genialny pomysł. Postanowiłam zatrudnić swoją ośmioletnią córkę, która – jak to dziecko – nudziła się w domu podczas wakacji. Powiedziałam, że zapłacę jej za tworzenie haseł.

W ciągu godziny wręczyła mi kartkę papieru z pięcioma hasłami. I poprosiła o wypłatę. Wręczyłam jej 3,5 dolara.

Zachwycona wizją łatwego zarobku, napisała e-maila do dziadków, wujka i kilku znajomych rodziny, aby poinformować ich o swoim nowym przedsięwzięciu. Napisała co następuje:

Temat: Moje przedsięwzięcie (sic!)

Zaczynam prowadzić swój własny interes, w którym tworzę hasła.

5 haseł kosztuje 3 dolary i 50 centów. 5 haseł na stronę. Mam nadzieję, że je wypróbujecie.

Moja mama natychmiast napisała do mnie z zapytaniem, czy konto jej wnuczki przypadkiem nie zostało zhakowane. Zapewniłam ją, że to prawdziwe przedsięwzięcie, ona natomiast zamówiła nowe hasła dla siebie. Do końca lata moja córka stworzyła około pięćdziesięciu haseł dla rodziny i przyjaciół, podnosząc cenę do dolara za hasło.

Byłam podekscytowana. Miałam w 1Password masę haseł, których nie znałam i dziesiątki silnych, możliwych do zapamiętania haseł do najważniejszych kont. Poza tym, nieoczekiwanie zachęciłam córkę do dbania o poufność danych albo przynajmniej do umiejętnego czerpania z niej zysków.

8

POŻEGNANIE Z GOOGLE

8 czerwca 2004 w bibliotece publicznej w Deming[1], w stanie Waszyngton, pojawił się agent Federalnego Biura Śledczego (Federal Bureau of Investigation, FBI) domagający się nazwisk osób, które wypożyczyły książkę *Bin Laden: Człowiek, który wypowiedział wojnę Ameryce* autorstwa Yossefa Bodansky'ego.

Nic podobnego nie zdarzyło się dotąd[2] w tej niewielkiej mieścinie liczącej 353 mieszkańców, położonej nieopodal granicy z Kanadą. Deming nie jest znane jako wylęgarnia terrorystów. Jeśli w ogóle ktoś o nim słyszał, to jako o miejscu, gdzie można zatankować paliwo i napić się piwa u podnóża Północnych Gór Kaskadowych.

Mimo to, pracownicy biblioteki byli przygotowani[3]. Rok wcześniej Deborra Garrett, prawniczka systemu bibliotek hrabstwa Whatcom przeszkoliła ich, jak odpowiadać na zapytania organów ścigania[4]. Bibliotekarze stali się obrońcami danych w latach 80. ubiegłego wieku, kiedy to agenci FBI pojawiali się w bibliotekach uniwersyteckich, żądając informacji o tytułach wypożyczanych przez obcokrajowców. W następstwie tych wydarzeń, czterdzieści osiem stanów[5] przyjęło przepisy chroniące do pewnego stopnia poufność danych związanych z obiegiem książek.

Kiedy więc agent FBI pojawił się w Deming[6], bibliotekarka pełniąca dyżur[7] odmówiła przekazania ewidencji wypożyczeń. Obiecała w zamian, że przekaże jego prośbę prawnikom biblioteki i odprowadziła go do drzwi.

Kiedy zapytanie przekazano do Garrett, zadzwoniła do agenta FBI i spytała, czego oczekuje. Odpowiedział, że pewien czytelnik zadzwonił do Biura, żeby poinformować o odręcznej notce, którą znalazł

na marginesie książki. Brzmiała ona: „Jeśli podejmowane przeze mnie działania uważane są za przestępstwo, to niech historia będzie mi świadkiem, że jestem przestępcą. Wrogość wobec Ameryki jest obowiązkiem religijnym, a my mamy nadzieję, że Bóg nam to wynagrodzi".

Po tej rozmowie Garrett odkryła, że cytat pochodził z wywiadu z Osamą bin Ladenem, przeprowadzanego w 1998 roku. Wysłała jego zapis do agenta FBI, sądząc, że – jak powiedziała – „to zakończy sprawę". Jednak parę tygodni później[8] do biblioteki dotarł sądowy nakaz wydania ewidencji wypożyczeń wraz z pouczeniem do pracowników, by go nie kwestionowali.

Biblioteka hrabstwa Whatcom znalazła się w trudnej sytuacji. Zrealizowanie nakazu oznaczałoby porzucenie wartości, w które wierzyli bibliotekarze. Z drugiej strony walka miała być trudna, bowiem prawo obliguje do działania zgodnego z prawomocnym wezwaniem wielkiej ławy przysięgłych. Biblioteka musiała walczyć o zawężenie przedmiotu wezwania. Garrett zasugerowała[9], żeby oprzeć się na precedensie z 1998 roku: sąd federalny w Waszyngtonie uznał wówczas, że księgarnia Kramerbooks & Afterwords nie musiała ujawnić ewidencji sprzedaży książki Moniki Lewinsky ze względu na ochronę, którą nad materiałem czytelniczym roztacza Pierwsza Poprawka do Konstytucji Stanów Zjednoczonych.

Członkowie rady biblioteki byli zaniepokojeni. Jeśli podejmą walkę i przegrają, będą musieli stanąć przed strasznym wyborem: przekazać żądane informacje i zdradzić własne ideały lub potencjalnie ryzykować odsiadką za odmowę działania zgodnego z wezwaniem sądowym. Po wewnętrznych dyskusjach zdecydowano się jednak na walkę. „Konieczność dokonania tego wyboru była okropna", wspomina Amory Peck[10], przewodnicząca zarządu systemu bibliotek publicznych hrabstwa Whatcom. „Nie mogliśmy jednak postąpić inaczej. Musieliśmy chronić podstawowe prawo naszych czytelników, które gwarantuje dostęp do całego wachlarza literatury i możliwość czytania w sposób szalony, z zaciekawieniem, czasem nawet ocierając się o niebezpieczeństwo... przy całkowitej pewności, że wybory czytelnicze pozostaną tajemnicą".

Kiedy Garrett złożyła wniosek o uchylenie wezwania w związku z Pierwszą Poprawką, FBI je wycofało. „Moim zdaniem ta sprawa pokazuje, co dzieje się, kiedy ludzie wiedzą, że podejmowane przez nich

działania zostaną zweryfikowane przez sąd", powiedziała Garrett, która obecnie sama jest sędzią[11]. „Skłania to do uczciwości".

* * *

Nie mogłam oczekiwać, że moi dostawcy internetu podejmą równie heroiczną walkę w obronie poufności moich wyborów czytelniczych.

Oczywiście do pewnego stopnia starają się oni bronić swoich klientów. Google dysponuje armią doskonałych prawników. W 2006 roku gigant zakwestionował wezwanie[12] Departamentu Sprawiedliwości do przedłożenia ewidencji wyszukiwań obejmującej dwa miesiące. Wygrał, zawężając je do raptem pięćdziesięciu tysięcy adresów URL wobec żądanych miliardów. W 2007 roku Amazon podjął skuteczną[13] walkę z rządowym wezwaniem do ujawnienia tożsamości osób, które za pośrednictwem serwisu dokonywały zakupów u sprzedawcy używanych książek. Władze chciały przesłuchać nabywców w związku ze śledztwem dotyczącym wyłudzeń podatkowych przez ten podmiot, jednak Amazon odmówił przekazania nazwisk. Sąd podzielił pogląd, że „wielce niepokojący i nieamerykański jest scenariusz, w którym agenci federalni przeczesują listy czytelników, będących uczciwymi obywatelami, w poszukiwaniu dowodów przeciwko komuś innemu".

Jeśli jednak chodzi o funkcjonowanie dragnetów rządowych, firmy internetowe często przegrywają walkę na tym polu, bowiem prawo nie stoi tu po ich stronie. Wobec internetu nie stosuje się stanowych przepisów o prywatności, chroniących ewidencje biblioteczne. Wnioski, które odwołują się do Pierwszej Poprawki, są często odrzucane ze względu na brak domniemanej szkody. Dodatkowo informatykom, w przeciwieństwie do bibliotekarzy, nie udało się zbudować reputacji obrońców wolności intelektualnej.

Przepisy, które regulują realizowany przez rząd monitoring komunikacji w internecie[14], znajdują się w ustawie o prywatności w łączności elektronicznej (Electronic Communications Privacy Act) z 1986 roku, którą zgłoszono celem rozszerzenia ochrony korespondencji telefonicznej i pocztowej na sferę cyfrową. W owym czasie nie przewidywano jednak, że ludzie będą gromadzić taką ilość informacji na swoich komputerach i zewnętrznych serwerach. W konsekwencji przechowywana komunikacja, taka jak poczta elektroniczna czy dane geolokalizacyjne telefonów

komórkowych, może zostać przejęta przez rząd bez nakazu przeszukania. Przepisy wymagają jedynie, by stosowne organa wykazały, że dane te stanowią „kluczowy materiał" w śledztwie.

Tym samym łatwiej jest organom ścigania legalnie czytać e-maile obywateli niż otwierać ich tradycyjną korespondencję. Co więcej, sądy często utajniają nakazy związane z monitoringiem elektronicznym[15], więc użytkownicy nigdy nie dowiadują się, że stali się obiektem inwigilacji. W efekcie strażnicy naszych danych mają ograniczone pole manewru, broniąc interesów klientów. W 2012 roku Microsoft dostarczył[16] dane o konsumentach w odpowiedzi na ok. 83 proc. wezwań organów ścigania. Google odpowiedział na dwie trzecie takich wezwań[17].

Wiodące firmy internetowe[18], między innymi Google, Apple i Facebook, zawiązały koalicję na rzecz nowelizacji dotychczasowych przepisów o prywatności w łączności elektronicznej, tak, by dostęp do poczty elektronicznej czy danych geolokalizacyjnych telefonów komórkowych także wymagał nakazu sądowego. Jak dotąd ich wysiłki nie zakończyły się sukcesem.

W kilku znanych nam przypadkach walki firm z rządowym monitoringiem, finał był marny. Przyjrzyjmy się dwóm sprawom – drobnego dostawcy internetu, Sonic.net, oraz internetowego olbrzyma Yahoo! W 2011 roku firma Sonic.net ujawniła[19], że stoczyła nieudaną walkę z tajnym sądowym nakazem ujawnienia adresów e-mail osób, które w ciągu dwóch lat korespondowały z wolontariuszem WikiLeaks, Jacobem Applebaumem. Podjęcie rękawicy było, zdaniem prezesa Sonic.net Dane'a Jaspera, „raczej drogie, jednak, w naszym odczuciu, musieliśmy tak zrobić". Rozmawiając ze mną[20], Jasper postąpił wbrew sądowemu zakazowi komentowania sprawy. (Później wyznał, że nie był świadomy, iż zakaz rozpowszechniania informacji na ten temat wciąż obowiązywał, gdy rozmawialiśmy)

Jeśli chodzi o Yahoo!, w 2008 roku Sąd Nadzoru Wywiadu Stanów Zjednoczonych (Foreign Intelligence Surveillance Court, FISC) odrzucił sprzeciw giganta[21] wobec żądania wydania danych użytkowników bez nakazu sądowego. Yahoo! argumentowało[22], że szeroki zakres żądania władz jest niekonstytucyjny, lecz sąd uznał, że firma nie przedstawiła dowodów na to, iż ktokolwiek został pokrzywdzony przez rządowy monitoring. „Pomimo szeregu zarzutów przedstawionych przez wnioskodawcę, nie potrafił on udokumentować faktycznej szkody czy

prawdopodobieństwa naruszenia prawa, ani umotywować obawy przed wystąpieniem rażącego błędu".

Podobnych przypadków było więcej. Występuje w nich ten sam powtarzający się wątek: firmy internetowe mają często związane ręce w działaniach wobec rządowego nadzoru.

* * *

Nie żywię niechęci do Google.

Prawdą jest, że Google naprawdę usiłowało zachować przejrzystość w kwestii monitoringu. Była to pierwsza duża firma internetowa[23], która zaczęła powszechnie publikować dane o wezwaniach otrzymanych od organów ścigania. Zawsze była także aktywnym członkiem koalicji na rzecz reformy ustawy o prywatności w łączności elektronicznej. Walczy z rządowym zakazem[24] rozpowszechniania informacji na temat liczby wezwań wystosowywanych przez sąd FISC.

Jednak Google wielokrotnie naruszyło zaufanie internautów. W 2010 roku gigant uruchomił[25] narzędzie w mediach społecznościowych o nazwie Buzz, które automatycznie oznaczało użytkowników jako „obserwujących" te osoby, z którymi często wymieniali e-maile lub czatowali na Gmail-u. Użytkownicy, którzy nacisnęli przycisk „Świetnie! Wypróbuj Buzz", nie byli w wystarczającym stopniu poinformowani, że tożsamość ich najbliższych znajomych na Gmail-u zostanie opublikowana. Firma Google zgodziła się później z zarzutami Federalnej Komisji Handlu (FTC), że usługa Buzz mogła wprowadzać w błąd i zapłaciła 8,5 mln dolarów[26] w ramach ugody w związku z pozwem zbiorowym. W 2012 roku wraz ze współpracownikami ujawniliśmy[27], że spółka obchodziła ustawienia prywatności przeglądarki Safari, z której korzystają posiadacze iPhone'ów i innych urządzeń Apple, za sprawą specjalnego kodu, który umożliwiał śledzenie. Jeszcze tym samym roku Google zgodziła się zapłacić 22,5 mln dolarów[28] w ramach ugody po tym, jak FTC zarzuciła firmie, że obejście zabezpieczeń Apple naruszało treść ugody sądowej dotyczącej Buzz. Była to zresztą w owym czasie najwyższa kara nałożona w cywilnym postępowaniu przez FTC. Z kolei w 2013 roku Google zgodziło się zapłacić 7 mln dolarów w ramach ugody[29] z prokuratorami generalnymi trzydziestu ośmiu stanów, którzy twierdzili,

że firma naruszyła prywatność osób, gdy samochody Street View losowo zbierały dane z sieci Wi-Fi.

Ja także gromadzę zbyt dużo informacji w Google. Mój prywatny audyt wykazał, że Google gromadziło wszystkie dane dotyczące moich wyszukiwań od 2006 roku oraz zidentyfikowało 2192 osoby, do których napisałam w tym okresie. Biorąc pod uwagę nieaktualną ustawę o prywatności, nie mogłam liczyć, że firma utrzyma wszystkie te informacje w sekrecie. Potrzebowałam przejść na dietę informacyjną.

Zaczęłam od porzucenia wyszukiwania w Google.

Byłam niezadowolona ze zmiany w polityce prywatności[30] Google ogłoszonej w 2012 roku, która pozwalała firmie łączyć informacje z różnych usług i na przykład tworzyć na ich podstawie spersonalizowane reklamy wyświetlające się w Gmail-u[31]. Google nie usuwa historii wyszukiwań[32] powiązanej z moim kontem, chyba, że sama o to zadbam. Gdy wyszukuję coś na komputerze, na którym nie jestem zalogowana do konta Google, część danych identyfikacyjnych zostaje usunięta dopiero po dziewięciu miesiącach. Teoretycznie rząd może zażądać od Google historii moich wyszukiwań od roku 2006. O żadnych tego typu działaniach nie informowano jak dotąd publicznie, niemniej fakt, że ta ewidencja istnieje stanowi wręcz otwarte zaproszenie do działania.

Historia moich wyszukiwań zawiera chyba najbardziej poufne informacje o mnie. Gdy szukam telefonu na kartę, wszystkie moje wyszukiwania dotyczą telefonów na kartę. Gdy szukam informacji do artykułu na temat technologii rozpoznawania twarzy, wszystkie moje wyszukiwania dotyczą technologii rozpoznawania twarzy. Zasadniczo, to, czego poszukuję stanowi precyzyjną prognozę moich przyszłych działań.

W zastępstwie Google znalazłam malutką wyszukiwarkę o nazwie DuckDuckGo, która prowadzi politykę zerowego gromadzenia danych. Nie zbiera ona żadnych informacji automatycznie przekazywanych przez mój komputer[33] – adresu IP czy innych śladów cyfrowych.

W konsekwencji DuckDuckGo nie ma możliwości powiązania moich wyszukiwań z moją osobą.

„Kiedy wchodzicie na DuckDuckGo (albo jakąkolwiek inną stronę) wyszukiwarka automatycznie wysyła informacje na temat waszego komputera", mówi polityka prywatności firmy. „Ponieważ dane te mogłyby zostać użyte do połączenia was z waszymi wyszukiwaniami, nie gromadzimy ich. Jest to bardzo nietypowa praktyka, niemniej czujemy,

że stanowi istotny krok w kierunku ochrony waszej prywatności".

Dopiero kiedy zmieniłam wyszukiwarkę, zrozumiałam, jak bardzo stałam się zależna od Google. Bez sugerowanych wyników wyszukiwania Google oraz jego perfekcyjnej pamięci dotyczącej tego, czego zwykle szukałam, każde wyszukiwanie wymagać ode mnie wysiłku. DuckDuckGo nie wie na przykład, że mieszkam w Nowym Jorku, więc kiedy błędnie wpisałam „Muzeum Historii Naturalnej", wyświetlił się wynik z taką placówką, tyle, że w Los Angeles. Dla porównania sprawdziłam to samo Google: oczywiście, poprawiło mnie i słusznie założyło, że jestem w Nowym Jorku, wyświetlając Amerykańskie Muzeum Historii Naturalnej na Manhattanie na górze wyników.

Brak zgromadzonej o mnie przez DuckDuckGo wiedzy zmusił mnie do uważniejszego wyszukiwania. Zauważyłam na przykład, że stałam się na tyle leniwa, że adres strony – taki jak CNN.com – wpisywałam w wyszukiwarce zamiast w panelu nawigacyjnym, mimo, że dokładnie wiedziałam, dokąd zmierzam. Zaczęłam więc wpisywać adresy we właściwym miejscu przeglądarki.

Kolejną rzeczą, na jaką zwróciłam uwagę, było to, że wyszukiwałam strony, które odwiedzam bardzo regularnie – choćby szkół moich dzieci czy tę z grafikiem studia jogi – zamiast umieścić je w zakładkach. Zaczęłam więc korzystać z zakładek.

Byłam tak przyzwyczajona do tego, że Google pracuje za mnie, że konieczność wpisywania całych słów, bez autouzupełniania, zaczęła mnie drażnić. Z drugiej strony fakt, że wyszukiwarka przestała sugerować mi hasła, sprawił, że stałam się mniej podatna na poszukiwanie rzeczy, których nie potrzebuję. Kiedy wpisywałam literkę „a", wyszukiwarka nie podpowiadała mi słowa: „amazon", wobec czego nie przypominałam sobie, że muszę nagle kupić coś w sklepie Amazonu.

Korzystając z DuckDuckGo z reguły znajdowałam to, czego chciałam, chociaż czasami dziwne wydawało się uzyskanie raptem trzech wyników. Byłam tak bardzo przyzwyczajona do „milionów" rezultatów pojawiających się w Google.

Niemniej DuckDuckGo miało pewne ograniczenia. Bardzo tęskniłam za Google Maps i nie byłam w stanie znaleźć dla usługi żadnego substytutu, który bym polubiła. Brakowało mi także sekcji Google News.

Przed wyjściem na obiad do przyjaciela chciałam sobie przypomnieć, na jakie dokładnie stanowisko otrzymał właśnie awans na Uniwersytecie Columbia. Ukazywały się na ten temat wiadomości, jednak wszystkie

moje wyszukiwania imienia i nazwiska Sree Sreenivasan oraz nazwy uczelni nie przynosiły rezultatu. Dopiero kiedy spróbowałam zestawienia „Sree", „Columbia" oraz „wiadomości" dotarłam do właściwego artykułu. Informacja tam była. Musiałam po prostu spróbować innego podejścia, żeby skutecznie wyszukiwać wiadomości w strukturze DuckDuckGo.

Zrozumiałam, że w rzeczywistości byłam zaprogramowana pod Google. Zawsze sądziłam, że jest ono niczym czysta kartka papieru – być może, że względu na jego ładny, biały interfejs – ale w istocie naginałam własne zapytania do tego, jak Google lubi na nie odpowiadać.

Tym razem musiałam dostosować się do nowego serwisu, DuckDuckGo, który w inny sposób odpowiadał na pytania. To było jak nowy związek; poznawałam dziwactwa i słabostki swojego partnera. Doświadczenie okazało się wzbogacające, bowiem partner ten nie miał ukrytej chęci śledzenia mnie.

Uwolniłam się od Google, a świat funkcjonował tak jak zawsze. Zgłębiałam tajniki innego serwisu i mogłam znaleźć informacje, których potrzebowałam. Sytuacja ta przypomniała mi słowa Marca Andreessena, twórcy Netscape, pierwszej przeglądarki stron internetowych, którą wprowadzono w 1994 roku. „Rozprzestrzenianie się komputerów[34] i internetu doprowadziło do podziału pracy na dwie kategorie – ludzi, którzy mówią komputerom, co mają robić oraz tych, którym to komputery będą mówić, co robić", mówił Adreessen w wywiadzie w 2012 roku.

Przejście do DuckDuckGo i jego opanowanie sprawiło, że miałam wrażenie, iż rosną moje szanse znalezienia się wśród ludzi, którzy mają kontrolę nad komputerami.

* * *

Po paru miesiącach użytkowania DuckDuckGo zaczęłam się czuć nieswojo. Kim są ludzie, którym zaufałam? Dlaczego ich logo stanowiła kaczka przystrojona w muchę? To wydawało się dziwne.

Mimo całej mojej niechęci do praktyk śledzenia stosowanych przez Google, wykształciłam emocjonalne wyobrażenie Google jako podmiotu o pewnej arogancji, rodem z któregoś z uniwersytetów należących do Ligii Bluszczowej. Miał ono swoje wartości[35], ale także niewiele skrupułów. Niewątpliwie wielkiej odwagi wymagało postawienie się cenzurze chińskich władz, co jednocześnie nie przeszkadzało w zarabianiu każdego

dnia na moich prywatnych danych.

Miałam problem z wytworzeniem w swojej głowie wizerunku podmiotu, który symbolizowała kaczka w muszce.

Wsiadłam więc do pociągu do Filadelfii, żeby poznać ludzi za nią stojących. Musiałam spędzić jeszcze dodatkowych dwadzieścia minut w podróży z miasta przez zielone przedmieścia, aż za Bryn Mawr College, by dotrzeć do celu. Łatwo było dostrzec założyciela DuckDuckGo, Gabriela Weinberga, na parkingu – jego auto było upstrzone kaczymi naklejkami. Miał bujną kasztanową czuprynę, ale wyglądał jak typowy maniak komputerowy [ang. *geek*] w okulary o grubych oprawkach i w bluzie z kapturem. Wskoczyłam do jego samochodu i w ciągu dwóch minut byliśmy w jego biurze.

Ku memu zaskoczeniu, wjechaliśmy na parking znajdujący się za kamiennym zamkiem z kolorowymi, okrągłymi wieżyczkami. „Pracujesz w zamku?" – zapytałam.

Tak, pracował. Biura DuckDuckGo znajdowały się na drugim piętrze, zaś ściany ozdobione były motywem kaczki. Weinberg miał w swoim gabinecie sofę w kropki oraz strefę zabaw dla swoich dzieci koło biurka. Powiedział mi[36], że pierwotnie prywatność nie była dla niego priorytetem. Chciał po prostu stworzyć lepszą wyszukiwarkę. Po tym jak w 2006 roku sprzedał portal społecznościowy[37] o nazwie Names Database za 10 mln dolarów, przeniósł się z żoną do Valley Forge w Pensylwanii, tak by jego małżonka miała bliżej do pracy w gigancie farmaceutycznym GlaxoSmithKline.

Jako świeżo upieczony milioner, Weinberg eksperymentował z szeregiem projektów. Założył własne studio telewizyjne, pracował nad siecią społecznościową dla golfistów a także usługą wykorzystującą społeczność jako źródło informacji [ang. *crowdsourcing*] celem osiągania jak lepszych rezultatów wyszukiwania. Kiedy zajmował się ostatnim projektem, rosła jego irytacja wynikami wyszukiwania w Google, które były pełne SPAM-u.

Postanowił więc stworzyć lepszą wyszukiwarkę. „Chciałem wrócić do starych czasów Google'a, kiedy nacisk kładziono na jakość odnośników". Kwestia prywatności pojawiła się dopiero po uruchomieniu pierwszej wersji strony dla społeczności pracowników IT, gdy część użytkowników zaczęła pytać się o politykę prywatności strony. „Szczerze mówiąc do tamtej chwili w ogóle się nad tym nie zastanawiałem. Dlatego

solidnie przyjrzałem się kwestii poufności wyszukiwań. Pomyślałem, że to przerażające, ile może wiedzieć o człowieku wyszukiwarka – to bez wątpienia najbardziej wrażliwe dane o kimś, które można zgromadzić za pomocą internetu. Stwierdziłem, że najlepiej będzie całkowicie umyć od tego ręce i najzwyczajniej nie gromadzić żadnych danych. Wtedy zrozumiałem że to stanowić będzie naczelną zasadę firmy".

Do 2011 roku całkowicie poświęcił się kwestii prywatności. Wykupił billboard w San Francisco, który głosił: „Google was śledzi. My nie." Do tego zgodził się na inwestycję ze strony funduszu *venture capital*, Union Square Ventures, który stawia na rozwijający się rynek narzędzi do ochrony prywatności.

Kilku z zatrudnianych przez niego inżynierów, spożywając w międzyczasie kanapki na wynos, przyłączyło się do nas by przedyskutować kwestię budowy wyszukiwarki internetowej od zera. Rozmawialiśmy o wyzwaniach tworzenia nowych map i mojej frustracji związanej z wyszukiwaniem przez ich serwis wiadomości. Utrzymanie przyjaznej polityki prywatności w DuckDuckGo było trudne. Inżynierowie musieli zbudować wiele narzędzi kompletnie od zera. Musieli na przykład stworzyć własne oprogramowanie do blogowania, ponieważ istniejące darmowe wersje zawierały technologię śledzenia.

– Zupełnie jakbyście byli pionierami – powiedziałam Weinbergowi – Musicie produkować własną żywność i gromadzić własną broń.

W trakcie rozmowy zaskoczyło mnie, jak żarliwie podchodzili do kwestii stworzenia lepszej wyszukiwarki. Kanapa w kropki, kaczki, zamek i kasztanowe włosy Weinberga – wszystko to sprawiało wrażenie, że to bardziej hobby niż prawdziwa firma. Oni byli jednak śmiertelnie poważni.

Przypomniało mi to czasy, kiedy pod koniec lat 90. XX wieku byłam dziennikarką w „San Francisco Chronicle". Zlekceważyłam wówczas świeżo wprowadzoną wyszukiwarkę Google. Pamiętam, jak myślałam: w jaki sposób poleganie na rankingu stron opartym na maszynach może być lepsze niż ręcznie wybierane wyniki z mojej ulubionej wyszukiwarki AltaVista?

Teraz siedziałam na kanapie w kropki na przedmieściach Filadelfii, zastanawiając się, jak kilku gości pracujących w zamku może stanowić zagrożenie dla wyszukiwarki, której obroty sięgają blisko 30 miliardów dolarów rocznie.

Jednak w branży technologicznej wiele z najlepszych pomysłów wydaje się początkowo szalona.

* * *

Naprawdę nie chciałam rezygnować z korzystania z Gmail. Większość z zaprzyjaźnionych ze mną hakerów go używała – nawet ci, którzy mieli obsesję na punkcie prywatności. Gmail pozwala na bardzo łatwe dzielenie się dokumentami, jak i czatowanie z innymi jego użytkownikami.

Z drugiej strony ciężko było uzasadnić korzystanie z usługi e-mail, której dostawca przyznawał się do czytania mojej korespondencji. Oczywiście Google mówi (a nie mamy żadnych powodów, żeby mu nie wierzyć), że to nie inni ludzie czytają moją pocztę[38]. To tylko komputery skanują moje wiadomości w poszukiwaniu słów kluczowych, następnie zaś wyświetlają reklamy oparte na ich podstawie.

To samo mówi jednak NSA o swoich dragnetach. Tak, to komputery agencji pod pretekstem działań kontrwywiadowczych przeszukują wszelkiej maści amerykańskie dane[39]. Twierdzi się, że przetwarzanie danych obywateli jest „ograniczone do minimum", przez co agenci ludzie nie mają z nimi do czynienia poza konkretnymi przypadkami, jak na przykład działania wywiadowcze, czy kiedy działania w związku z istnieniem dowodów przestępstwa.

Ostatecznie w przypadku wszystkich dragnetów liczy się jedno pytanie: czy dojdzie do nadużycia danych? Odpowiedź zdaje się być w sposób złowieszczy twierdząca. W 2010 roku firma Google zwolniła inżyniera[40] za przeglądanie czatów nastolatków na Gmail-u – poinformowano wówczas, że było to drugie wypowiedzenie za tego typu[41] postępowanie. W 2008 roku dwóch byłych techników z NSA ujawniło[42], że razem z kolegami podsłuchiwali rozmowy setek Amerykanów, włącznie z tymi najbardziej intymnymi.

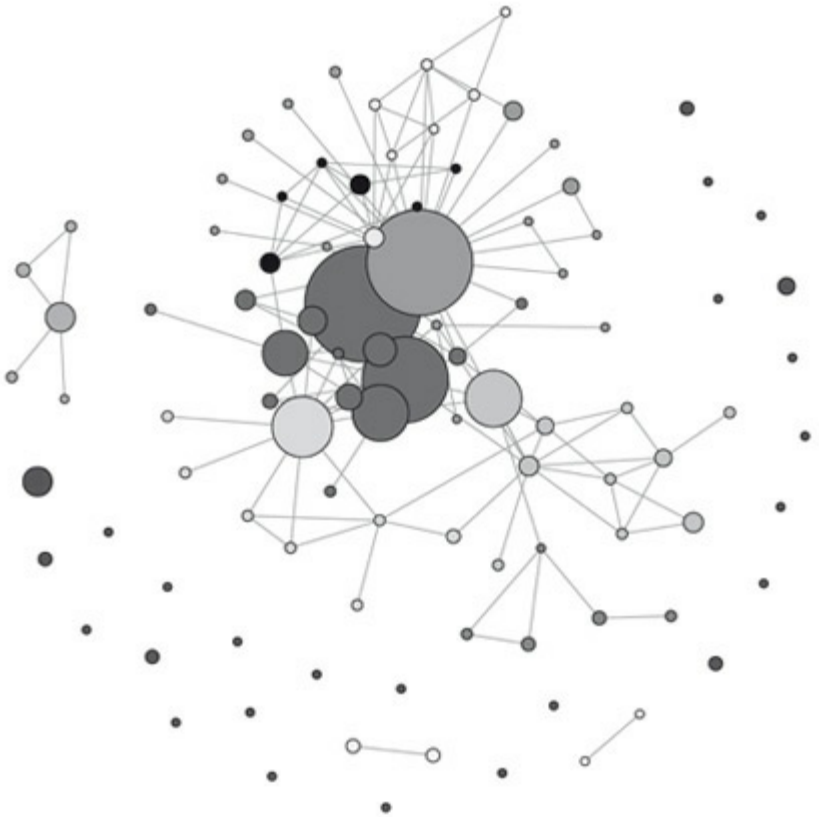
Niezależnie od tego, cały czas opóźniałam swoje odejście od Gmail-a. Był tak prosty, przyjazny i przydatny.

Wreszcie, projekt z Massachusetts Institute of Technology (MIT) przekonał mnie[43] do znalezienia nowej usługi e-mail. Grupa uczelnianych badaczy stworzyła narzędzie zwane Immersion, pozwalające wizualizować metadane kont Gmail.

Zezwolenie Immersion na dostęp do mojego konta Gmail zjeżyło mnie nieco, ale badacze obiecali, że usuną rezultaty swoich działań, więc się zgodziłam. Po paru minutach obliczeń, Immersion przedstawiło mi piękny

graf ilustrujący moje połączenia z 504 osobami, z którymi najczęściej wchodziłam w interakcje, czyli wymieniłam więcej niż 3 wiadomości. Według Immersion najwięcej razy kontaktowałam się z moją najlepszą przyjaciółką, tuż za nią znalazł się mąż. (Gmail informował mnie już, że to właśnie małżonek jest moim najczęstszym partnerem mailowym. Nie wiem, która informacja jest właściwa).

Graf ilustrujący sieć moich interakcji wyglądał tak:



Wynikało z niego jasno, że z około tuzinem osób wymieniałam e-maile znacznie częściej niż z kimkolwiek innym. Przypomniało mi to, jak unikalną sieć społeczną stworzyłam.

Zaniepokojona, podjęłam starania na rzecz wyplątania się z Gmail.

Przez krótki czas zastanawiałam się[44] nad uruchomieniem własnego serwera e-mail w domu, po tym jak natrafiłam na post na blogu zatytułowany „Zabezpiecz swoje e-maile przed NSA w 2 godziny". Porzuciłam jednak ten pomysł po przeczytaniu 8 akapitów tekstu, którego

autor założył, że „korzystam z systemu Debian Wheezy". Nie było wątpliwości, że to zadanie było dla mnie zbyt skomplikowane technicznie.

Rozejrzałam się więc za skrzynkami e-mail chroniącymi prywatność swoich użytkowników. Okazało się, że są ich dziesiątki – z nazwami takimi jak Hushmail, NeoMail czy CounterMail. Spodobał mi się zwłaszcza ten ostatni – płatna skrzynka e-mailowa, która przeszła wspominany przeze mnie wcześniej *test błotnistej kałuży.* Niestety musiałam ją wykluczyć, jako że była ze Szwecji. Moje e-maile, jako obywatelki USA, są chronione przez prawo. NSA musi przynajmniej „ograniczać do minimum" szpiegowanie wiadomości obywateli swojego kraju. Gdyby jednak agencja uznała mnie za cudzoziemca, ograniczenie to mogłoby być zniesione.

Pozostało mi więc tylko kilka amerykańskich opcji[45], między innymi Lavabit, teksańska usługa[46], której mógł używać Edward Snowden oraz Riseup, serwis prowadzony przez kolektyw z Seattle[47]. Po zapoznaniu się z ich polityką prywatności uznałam, że Riseup wydaje się nieco bardziej zachęcający. Oba serwisy gromadziły minimalną ilość danych użytkowników a także przeszły *test kałuży błotnej.* Jednak Riseup dodatkowo usuwał lokalizację z adresów mailowych[48], podczas gdy Lavabit twierdziło[49], że jest ona potrzebna na wypadek konieczności wykorzystania przez organy ścigania.

Dołączenie do Riseup nie było proste. Owszem, usługa była darmowa, ale musiałam zostać do niej „zaproszona" przez innego użytkownika. Szczęśliwie udało mi się uzyskać takie zaproszenie od Christophera Soghoiana, technologa z American Civil Liberties Union, a zarazem jednego z najbardziej paranoicznych osób jakie znam (co uważam za komplement).

Po tym wstępie rozpoczęłam proces rejestracji. Szybko jednak w zakłopotanie wprawił mnie kontrakt społeczny, o którego podpisanie zostałam poproszona.

Prosimy o nieużywanie usług riseup.net[50] w celu głoszenia, któregokolwiek z poniższych:

– poparcia dla kapitalizmu, dominacji czy hierarchii,

– koncepcji, że walka klas jest ważniejsza niż opresja rasowa czy płciowa,

– dyktatury proletariatu,

– polityki kontroli urodzeń.

Jeśli się z tym nie zgadzasz, to znaczy, że riseup.net nie jest dla ciebie.

Większość zasad nie budziła moich większych zastrzeżeń. Nie planowałam używać Riseup by podburzać do rewolucji, wzywać do kontroli urodzeń czy opowiadać się po którejkolwiek ze stron sporu o prymat walki klasowej nad hegemonią rasową/płciową. Nie było także prawdopodobne, żebym opowiedziała się za dominacją czy hierarchią.

Jednak rezygnacja z „poparcia dla kapitalizmu" była trudna. Ostatecznie pracowałam dla „Wall Street Journal" – gazety, która kiedyś promowała się hasłem „wyjątkowe doświadczenia w kapitalizmie". Starałam jednak siebie przekonywać, że moją rolą jako dziennikarki było obserwowanie i pilnowanie kapitalizmu, nie zaś jego bezkrytyczne popieranie. Być może bawiłam się słowami, ale postanowiłam zgodzić się z warunkami umowy społecznej Riseup.

Na tym jednak nie koniec. Musiałam znaleźć sposób na zarządzanie moimi e-mailami z poziomu komputera zamiast w sieci. Riseup pozwala użytkownikom[51] na gromadzenie wyłącznie niewielkiej ilości danych na swoich serwerach, co obniża koszty oraz, co jeszcze ważniejsze, oznacza, że rządy mają dostęp do mniejszej ilości informacji. Naturalnie Riseup obiecuje[52], że będzie „aktywnie walczył" z każdą próbą przejęcia danych użytkowników, co niewątpliwie jest zawsze łatwiejsze, jeśli nie ma czego przejmować.

Niezależnie od ograniczeń ilości danych Riseup, powinnam była już wcześniej przechowywać moje e-maile na komputerze zamiast w chmurze Gmail. Ustawa o prywatności w łączności elektronicznej (Electronic Communications Privacy Act) z 1986 roku[53] pozwala rządowi wejść w posiadanie e-maili gromadzonych u zewnętrznego usługodawcy po upływie 180 dni bez jakiegokolwiek nakazu. Wobec tego przechowywanie starych e-maili w jakimkolwiek innym miejscu poza domem jest, niestety, biletem do państwowego dragnetu.

Poszukiwałam programu poczty e-mail, które chroniłoby prywatność. Najlepszą opcją był darmowy, oparty na otwartej licencji projekt Thunderbird, który pozwalał na szyfrowanie wiadomości. Jednak Mozilla, na której infrastrukturze się opierał[54], wycofała się z tego projektu w 2012 roku.

Zgodnie z moją przewodnią zasadą „płacenia za jakość"[55] nabyłam

płatną wersję Thunderbird zwaną Postbox. (Wsparłam także pieniężnie kolektyw Riseup w nadziei utrzymania tej usługi przy życiu) Ściągnęłam zawartość swojego konta w Gmail i umieściłam ją w Postbox, a także podłączyłam do niego Riseup. Kiedy wszystko zaczęło działać, poczułam się wolna. Nagle mogłam w łatwy sposób przełączać się między dostawcami usług e-mail. Mogłam otrzymać wiadomość w Gmail i odpowiedzieć na nią ze swojego konta na Riseup.

Co dziwne, początkowo nie byłam przekonana do używania konta na Riseup. Bałam się, że ludzie nie będą chcieli mieć nic wspólnego z e-mailami nadchodzącymi z serwera antykapitalistycznego kolektywu. Wysłałam więc wiadomości z zapytaniem do osób, które mogłyby poczuć się zaniepokojone – wysoko postawionych ludzi w strukturach rządowych czy biznesie. Spytałam, czy przeszkadzałoby im, gdybym pisała do nich z adresu anarchistycznego kolektywu.

Odpowiedzi oscylowały pomiędzy „Hmm?" a „Co?". Nikt nie sprawiał wrażenia, że się tym przejmuje. Wtedy dotarło do mnie, że kiedy dołączyłam do Gmail, nigdy nie zapytałam nikogo, czy zgadza się, żeby jego maile były skanowane przez Google.

(Warto wspomnieć[56], że kilkoro internautów, którzy nie korzystali z Gmail złożyło pozew zbiorowy przeciwko Google za rzekome naruszenie ustawy o podsłuchach (Wiretap Act) – poprzez skanowanie ich e-maili kierowanych do użytkowników kont Gmail, a podchodzących z innych skrzynek pocztowych. Google twierdzi[57], że korzysta z domniemanej zgody. „Tak samo osoba wysyłająca list do kontrahenta nie może być zaskoczona, że wiadomość otworzy asystent adresata". Nie jestem pewna, czy mnie to przekonuje. W końcu zawsze pytam męża o zgodę, zanim otworzę list adresowany do niego).

Zrozumiałam, że zmieniając usługodawcę na takiego, który nie będzie skanować ich korespondencji, w istocie wyświadczam ludziom przysługę. Przestałam więcej pytać i zaczęłam używać Riseup we wszystkich zawodowych kontaktach.

Nie porzuciłam jednak Gmail-a całkowicie. Postanowiłam zachować konto, tak jak przez lata pozostawiałam przy życiu swoje konto AOL, które stopniowo zaczęło mi służyć do obsługi zakupów w internecie. Zdecydowałam traktować konto Gmail jako obsługujące moje „matczyne" e-maile – do umawiania zabaw moich dzieci, zapisywania ich na obozy oraz komunikowania się ze szkołą poprzez udostępniane w ramach Google

pliki.

Ostatecznie ściągnęłam wszystkie udostępniane przez Google pliki na mój dysk twardy. Przez to przestałam potrzebować się tam logować. I wreszcie wisienka na torcie: w przypadku gdybym zdecydowała się na sporadyczne wyszukiwanie przez Google, nie zostałoby ono skojarzone z moją tożsamością, bo nie byłam zalogowana. (Co prawda moje wyszukiwania w dalszym ciągu byłyby oznaczone adresem IP mojego komputera, o ile nie używałabym oprogramowania do jego *anonimizacji*).

Poczułam się, jakbym wspięła się na swoisty technologiczny Mount Everest. Przejęłam kontrolę na moim e-mailem, on nie sprawował jej już nade mną.

* * *

Moja euforia nie trwała długo.

W sierpniu 2013 roku Lavabit, usługa poczty elektronicznej, z której korzystał Edward Snowden, została nagle wyłączona. Jej założyciel, Ladar Levison[58], napisał, że wolał ją zamknąć niż „stać się współwinnym przestępstw przeciwko Amerykanom". Powiedział, że zamierza zwrócić się do Sądu Apelacyjnego Czwartego Okręgu, co sugerowało, że już walczył i przegrał w niższych instancjach.

Jak w wielu podobnych sprawach dotyczących nadzoru elektronicznego, Levison dostał zakaz rozpowszechniania informacji o wezwaniu, które skierowały do niego władze. Jednak po tym, jak niektóre z dokumentów stały się jawne[59], Levison ujawnił, że żądano od niego wydania kluczy szyfrujących, które odblokowałyby korespondencję wszystkich użytkowników. Innymi słowy, oczekiwano od niego by złamał *test błotnistej kałuży*. Stwierdził on, że byłoby to jak „poproszenie spółki Coca-Cola o podanie do wiadomości publicznej jej tajnej receptury".

Tego rodzaju sytuacja miała już miejsce w przypadku usługi szyfrującej e-maile. W 2007 roku Hushmail, dostawca usług, koncentrujący się na kwestii prywatności[60], dosadnie zasugerował, że został wezwany przez sąd do zainstalowania oprogramowania, które mogłoby przechwytywać hasło użytkownika podczas logowania do usługi, co pozwoliłoby rządowi na odszyfrowanie danych.

Mogłam zrozumieć, dlaczego Levison wolał zamknąć serwis w zgodzie ze swoimi zasadami niż dopuścić do zakłócenia prywatności

użytkowników. Nie byłam jednak w stanie nie współczuć[61] czterystu tysiącom ludzi, którzy stracili swoje konta e-mail bez jakiejkolwiek zapowiedzi. „Lata używania konta[62], zapisane e-maile i ważne szczegóły usunięte bez uprzedzenia. To żenujące", napisał jeden z użytkowników na stronie Lavabit na Facebooku. „To straszne. Dziękuję za namieszanie w moim życiu, „podsumował inny.

To mogłam być ja. Lavabit było w końcu jednym z moich faworytów, gdy poszukiwałam dostawcy poczty e-mail.

Po jego zamknięciu[63] kolejna firma chroniąca prywatność użytkowników, Silent Circle, zakończyła świadczenie usług. Poinformowała, że nie dostała żadnego wezwania ze strony władz, ale postanowiła uprzedzić ich ruch. „Wyczuliśmy pismo nosem i postanowiliśmy, że najlepiej będzie wyłączyć Silent Mail właśnie teraz", oświadczyła.

Z dnia na dzień Riseup stał się jednym z ostatnich dostawców usług chroniących prywatność. Kolektyw opublikował komunikat[64], który miał podnieść na duchu użytkowników: że będzie walczył z każdą próbą szpiegowania przez władze oraz pracuje nad „całkowicie nową infrastrukturą", która w jeszcze lepszy sposób będzie chronić e-maile użytkowników. Nie było to jednak w pełni pocieszające.

„Prędzej odłączymy zasilanie niż ukorzymy się przed represyjną inwigilacją rządową, niezależnie czy chodzić będzie o władze naszego, czy jakiegoś innego kraju", napisali liderzy kolektywu. Przypomnieli też użytkownikom o potrzebie wykonywania kopii zapasowych swoich e-maili.

Po trzykrotnym upewnieniu się, że skopiowałam wszystko na twardy dysk i zaszyfrowaną „chmurę", pomyślałam o tym, jak bardzo absurdalna stawała się moja przygoda z prywatnością.

Gromadziłam wszystkie swoje dane na wypadek apokalipsy. Co dziwniejsze, wydawała się ona czaić tuż za rogiem. Stawałam się *surwiwalistką* świata informacji.

9

POZNAJCIE IDĘ

Ida Tarbell była dziennikarką śledczą[1], która ujawniła nadużycia Standard Oil Company na przełomie XIX i XX wieku. Jest także moim alter ego.

Tworzenie fikcyjnej tożsamości stanowiło kluczową część mojej strategii zanieczyszczania danych [ang. *data pollution*]. Kiedy kupując coś w sieci albo logując się na różnych stronach musiałam podać jakieś informacje, najczęściej wpisywałam dane Idy, a nie swoje. Przecież nie istnieje powód, dla którego na każdej stronie wymagającej logowania miałabym się posługiwać moim prawdziwym nazwiskiem.

Oczywiście, zdeterminowany przeciwnik zapewne połączyłby fakty i zauważył podobieństwo pomiędzy mną a Idą. Jednak nie dążyłam do doskonałości. Po prostu chciałam sprawić, by podążanie moim śladem kosztowało tych, którzy mnie śledzą, więcej wysiłku, a także by nie mogli oni bez problemu przetwarzać moich danych.

Wybrałam Idę ze względu na to, że jest przedstawicielką pokolenia dziennikarzy, których podziwiam. Znani jako „demaskatorzy", dziennikarze śledczy tacy jak Ida Tarbell i Upton Sinclair obnażali drugie oblicze rewolucji przemysłowej, ujawniając fakt narzucania przez kartele cen monopolistycznych, czy opisując warunki pracy w rzeźni. Ich działalność przyczyniła się do sformułowania praw, które ograniczyły największe nadużycia tej epoki.

Wierzę, że obecnie jesteśmy w podobnym, przełomowym momencie. Podczas gdy nasze społeczeństwo zmierza w stronę gospodarki informacyjnej, prawo nie jest wciąż gotowe do kontroli wyłaniających się w niej gigantów. Niewiele rządowych i pozarządowych instytucji posiada wystarczającą wiedzę techniczną, by móc te firmy nadzorować. Obowiązek

ten w dużym stopniu spoczywa na współczesnych „demaskatorach", takich jak Edward Snowden, którzy ujawniają drugie oblicze rewolucji informacyjnej. Mam nadzieję, że jak tylko dostrzeżemy rozmiar nadużyć, znajdziemy sposób na ich powstrzymanie.

Nie byłam pewna, jak stworzyć wirtualną tożsamość Idy. Zdążyłam jedynie stwierdzić, że nie będzie miała fałszywego prawa jazdy. Jednak cała reszta, tj. fałszywy adres e-mail, telefon, adres, zdawała mi się możliwa do przełknięcia. Wkrótce trafiłam na grząski grunt kłamstw.

* * *

Zaczęłam niewinnie. Założyłam Idzie konto na Gmailu, co oznaczało wymyślenie jej daty urodzenia i kodu pocztowego. Zdecydowałam, że urodziła się w 1966 roku i mieszka w Berkeley w stanie Kalifornia.

Następnie zaczęłam dokonywać rezerwacji w restauracjach w imieniu Idy Tarbell. Był jeden problem – Ida nie miała komórki, a restauracje często prosiły o podanie telefonu kontaktowego.

Potrafiłam jednak przekonać niektóre z nich do zarezerwowania stolika bez podania numeru, obiecując, że zadzwonię w celu jej potwierdzenia. Zgadzano się na to. I nawet kiedy zdarzało się, że zapominałam oddzwonić, trzymano dla mnie stolik.

Odkryłam natomiast, że kłamstwo przychodzi mi z trudem: za każdym razem, kiedy wypowiadałam imię „Ida" czerwieniłam się i robiło mi się gorąco. Szybko zrozumiałam, że Ida potrzebuje konta na OpenTable, abym mogła dokonywać rezerwacji przez internet, nie musząc później kłamać przez telefon.

Jednak gdy rozpoczęłam proces rejestracji, strona poprosiła o podanie numeru kontaktowego. Wiem, że mogłam podać przypadkowy numer, ale jakoś nie potrafiłam. Opuściłam stronę z formularzem.

Podobnie było z hasłami. Problem nie leżał w technologii, ale w mojej głowie.

* * *

Nie umiem kłamać.

Gdy nie mówię prawdy, miotam się, nie patrzę prosto w oczy, a moją twarz oblewa rumieniec. Albo zaczynam nerwowo chichotać. Jestem tak

nieudolnym kłamcą, że kiedyś kolega wziął mnie na bok i powiedział, żebym nie próbowała kłamać, bo nie umiem tego robić.

Zawsze uważałam, że w wirtualnym świecie łatwiej jest oszukiwać niż w realu. Niektóre badania także na to wskazują[2]. W sieci unika się bowiem sygnałów pozawerbalnych towarzyszących kłamstwu. Jednak w moim przypadku tak nie było. Nie rozumiałam dlaczego tak się dzieje, dopóki nie trafiłam na badanie Jeffa Hancocka, psychologa z Uniwersytetu Cornell, który zajmuje się tym zagadnieniem.

W swoim eksperymencie z 2012 roku, Hancock poprosił 119 studentów[3], aby napisali tradycyjne CV albo stworzyli swój życiorys na publicznym profilu LinkedIn. Następnie przeanalizował wiarygodność obu grup. Studenci, którzy napisali tradycyjne *curriculum vitae*, byli bardziej skłonni do ubarwiania swojego doświadczenia zawodowego niż osoby poproszone o umieszczenie CV na LinkedIn. Jednak badani korzystający z portalu chętniej udzielali nieprawdziwych informacji o swoich hobby i zainteresowaniach. Hancock podsumował wyniki badania: „życiorysy na LinkedIn bardziej szczerze opisywały kwestie istotne dla pracodawców, takie jak dotychczasowe obowiązki czy umiejętności nabyte w poprzedniej pracy”[4].

We wcześniejszym eksperymencie, Hancock porównał rzeczywisty wzrost, wagę i wiek użytkowników portali randkowych z tym, jak przedstawiali je w sieci[5]. Okazało się, że większość przesadzała w niewielkim stopniu. Mężczyźni zazwyczaj oszukiwali na temat swojego wzrostu[6]: „dodawali sobie 2,25 cm, co my badacze nazywamy *niezłym zaokrągleniem*”.

Hancock uważa, że ludzie mogą być bardziej prawdomówni w Internecie niż w rzeczywistości, jeśli sądzą, że mogą zostać pociągnięci do odpowiedzialności za swoje słowa. W innych badaniach doszedł do wniosku, że im rozmowa jest mniej zobowiązująca, tym więcej kłamiemy[7]. Okoliczności – czyli to, czy chodzi o wirtualny czat czy rozmowę w cztery oczy – nie mają większego znaczenia. Im lepiej ludzie się ze sobą znają, tym bardziej rośnie ich prawdomówność. Hancock zakłada, że kłamanie przychodzi z większym trudem tym, którzy mają świadomość, że ich słowa zostaną zarejestrowane i będą oni za nie odpowiadać. Po przeprowadzonym audycie moich danych, jestem doskonale świadoma, że wszystko co robię jest, w ten czy w inny sposób, odnotowywane. Jest więc logiczne, że mam opory przed kłamaniem

w sieci.

Gdy już zrozumiałam swoją sytuację, stanęłam przed dylematem: „Czy z etycznego punktu widzenia powinnam pokonać swoją niechęć do kłamstwa, czy jednak nie?". Poszukując odpowiedzi na to pytanie, trafiłam w „objęcia" filozofów. Jedną z najbardziej nieprzejednanych postaw wobec kłamstwa prezentował osiemnastowieczny niemiecki myśliciel, Immanuel Kant[8]. Uważał on, że jest ono zawsze złe – nawet kiedy u waszych drzwi pojawi się morderca poszukujący niewinnej ofiary.

Jako matka natychmiast podważyłam kategoryczne podejście Kanta. Każda matka bowiem wie, że nie zawsze może mówić swoim dzieciom prawdę. Kiedy mój syn uciął sobie palec i czekaliśmy z nim na ostrym dyżurze, okłamałam go. Chirurg bowiem utknął w burzy śnieżnej i nie było wiadomo czy dotrze na czas do szpitala, aby go zszyć. Powiedziałam dziecku jedynie, że wszystko będzie dobrze. (Ostatecznie chirurg zszył mu palec, ale przyjazd do szpitala zajął mu prawie pięć godzin).

Według mnie, niektóre kłamstwa są akceptowalne. Które? Zainteresowałam się testem publicznym[9] [ang. *publicity test*] opisanym przez Sisselę Bok, pisarkę i filozofkę z Uniwersytetu Harvarda: „Które kłamstwa, i czy w ogóle jakieś, obroniłyby się przed opinią publiczną?".

Oto niektóre ze stawianych przez nią pytań:

- Czy istnieją wiarygodne alternatywy dla waszego kłamstwa?
- Jakie jest moralne usprawiedliwienie kłamstwa?
- Jaka jest relacja między wami, a okłamaną przez was osobą?
- Co złego, a co dobrego wyniknie z waszego kłamstwa?
- Co by się wydarzyło, gdyby każdy – znalazłszy się na waszym miejscu – kłamał?

W końcu czułam, że poruszam się po stałym gruncie. Zamierzałam wykorzystać fikcyjną tożsamość do transakcji handlowych, w których – według mnie – wymagano ode mnie więcej informacji, niż to było konieczne.

Przecież mogę pójść do kiosku, wręczyć pieniądze i kupić anonimowo papierową gazetę. Tymczasem zakup jakiegokolwiek wydania cyfrowego wymaga podania danych osobowych. Podobnie jest z bezpłatna subskrypcją. Dawniej chodziłam do lokalnej księgarni i kupowałam książki

za gotówkę. Dziś, w erze wymierania książek papierowych, funkcję mojego lokalnego sprzedawcy pełni Amazon. Czy jednak firmy oferujące produkty przez internet potrzebują czegoś więcej niż moich pieniędzy? To samo dotyczy restauracji, w których rezerwuję stolik.

Z pewnością, część z tych informacji, jeśli nie wszystkie, zostanie wykorzystana przeciwko mnie.

Zastanówmy się nad dwoma przypadkami.

W 2012 roku Międzynarodowe Zrzeszenie Przewoźników Powietrznych (International Air Transportation Association, IATA) wprowadziło nowe zasady[10], które umożliwiają liniom lotniczym oferowanie różnym grupom klientów tego samego produktu po różnych cenach. Dziennik „New York Times" ostrzegał, że ten nowy model dyskryminacji cenowej będzie opierał się na proponowaniu wyższych stawek osobom robiącym zakupy anonimowo oraz tym, które byłyby po prostu gotowe płacić więcej[11].

W 2013 roku towarzystwo ubezpieczeniowe Blue Cross Blue Shield of North Carolina zaczęło skupować od brokerów sprzedaży baz danych informacje o nawykach 3 milionów ubezpieczonych, dotyczących wydawania pieniędzy[12]. Firma twierdziła, że pozwoli jej to oznaczać osoby kupujące ubrania w rozmiarach dla puszystych i przesyłać im sugestie wdrożenia planu odchudzania.

Jak dla mnie, to wszystko jest początkiem nowej epoki nadużyć finansowych. Wielkie firmy dążą do pozyskania moich wrażliwych danych, aby osiągnąć nade mną przewagę. Czułam, że w tej relacji, kłamstwo jest usprawiedliwione. To bowiem sposób na przywrócenie równowagi.

Zatrzymałam się jednak nad ostatnim pytaniem Bok. Jak wyglądałby świat, w którym wszyscy podawaliby fałszywe dane?

Starałam się wyobrazić sobie taką rzeczywistość. Byłby to świat, w którym nie można by było ufać ludziom, których nie znało się osobiście; miejsce, w którym nie otwierałoby się wiadomości e-mail od znajomych naszych znajomych i nie wierzyłoby się rekomendacjom niepochodzącym z zaufanego źródła. Mogłoby się w nim zdarzyć, że słynny futbolista zostanie wrobiony w romans z poznaną w internecie kobietą, której tożsamość okaże się fikcyjna[13]. Będzie się pod nią skrywał zakochany w sportowcu mężczyzna. (Dla tych, którzy nie znają tej historii: opisałam właśnie przypadek Mantiego Te'o, wspomagającego drużyny futbolowej

Notre Dame). Być może wynika to z faktu, iż brakuje mi wyobraźni, ale wydaje mi się, że ten świat nie różniłby się specjalnie od tego, w którym obecnie żyjemy.

A co z odwołaniem się do głosu opinii publicznej? Rozmówcy, z którymi się konsultowałam, uważali, że pytania o etyczność niewinnych kłamstw są głupie. Mój mąż twierdził, że fikcyjna tożsamość jest w porządku, jeśli nie zamierzam wyrabiać sobie fałszywego dowodu. Chrzestna moich dzieci mówiła, że w ogóle nie ma się nad czym zastanawiać – ona sama używała paru fałszywych adresów e-mail do różnych celów. Kolega uznał, że jest to świetny pomysł i od razu sam stworzył sobie fałszywej tożsamość.

Bez wątpienia, próba była przeprowadzana na niewielkiej grupie. Mimo tego, doszłam do wniosku, że moje kłamstwa zdały test publiczny.

Z odkrytym na nowo zapałem przeorganizowałam wirtualną tożsamość Idy i ruszyłam do akcji. Tym razem na poważnie: zamierzałam wyrobić Idzie Tarbell kartę kredytową.

Pomysł z kartą kredytową podsunął mi kryptolog Jon Callas. Przyszedł do mojego biura, aby pokazać mi aplikacje szyfrujące połączenia i wiadomości w iPhonie[14]. Wspomniałam mu o moich dylematach dotyczących stworzenia solidnej alternatywnej tożsamości. Nie tracąc ani sekundy, wyciągnął z portfela i rozłożył przede mną wachlarz kart, wystawionych na różne nazwiska. Jedno z nich brzmiało: Dale B. Cooper (agent specjalny FBI z serialu „Twin Peaks" z lat 90.).

Powiedział, że to jest naprawdę proste. Wystarczy poprosić wystawcę karty o wyrobienie nowej, na inne nazwisko. Zostanie ona podłączona do waszego konta. Tak jak karty dzieci podłącza się do kont rodziców.

Aha, zrozumiałam. Tu właśnie pojawia się zagadnienie modelu zagrożenia. Nie było nim w tym przypadku ujawnienie tożsamości przed wystawcą karty. Chodziło o ukrycie jej przed resztą świata. Gdybym była podejrzana o popełnienie przestępstwa, prokurator mógłby wysłać do American Express sądowy nakaz wydania prawdziwych danych Idy Tarbell.

Zdecydowałam się więc na to. Próbowałam wyrobić nową kartę za pośrednictwem strony internetowej American Express, ale przeczytałam, że muszę tam zadzwonić. Zrobiłam to późnym wieczorem z biura, gdy nikogo nie było w pobliżu. Nadal czułam się onieśmielona. Nie chciałam, by usłyszał mnie ktoś z rodziny czy współpracowników.

Oczywiście konsultant działu obsługi klienta zareagował rutynowo

na moją prośbę o wydanie dodatkowej karty do konta. Zapytał o datę urodzin Idy, którą na szczęście wymyśliłam już przy zakładaniu konta e-mail. Gdy poprosił o podanie jej numeru ubezpieczenia społecznego, odpowiedziałam, że go nie znam. Bez zawahania przeszedł dalej. Powiedział, że karta powinna trafić do mojej skrzynki pocztowej w ciągu kilku dni.

Dni mijały, a karty nie było. A potem minął tydzień i jeszcze kolejne dwa. W końcu zadzwoniłam ponownie i poprosiłam o wydanie jeszcze jednej karty. Upłynął kolejny tydzień, a ta wciąż nie docierała.

W międzyczasie zaczęłam otrzymywać e-maile i telefony ze strony American Express z prośbą o podanie numeru ubezpieczenia Idy. Głos lektora sugerował: „Wciśnij 1, jeśli jesteś Idą; wciśnij 2, jeśli nią nie jesteś. Naciśnij 1, jeśli Ida jest dostępna; naciśnij 2, jeśli nie jest dostępna".

Czułam, że wpadłam w pułapkę – byłam i nie byłam Idą – więc się rozłączałam.

Zaczęłam się zastanawiać, czy to możliwe, że wysyłkę karty opóźniał brak numeru ubezpieczenia społecznego. W końcu się przełamałam i zadzwoniłam ponownie. Konsultantka infolinii poinformowała mnie, że karta trafi do mnie następnego dnia.

W istocie, otrzymałam ją nazajutrz. Była ładna, koloru zielonego, lekko lśniąca, z wytłoczonym nazwiskiem Idy. Nigdy nie szalałam tak za żadną kartą. Tego wieczoru z dumą pokazałam ją mojemu mężowi, po powrocie z pracy. „Och! Czemu mi nie powiedziałaś, że jesteś Idą Tarbell? Od tygodni wyrzucam listy kierowane na jej nazwisko", westchnął ciężko.

Nauczka na przyszłość: poinformujcie małżonka o tym, że zamierzacie stworzyć fikcyjną tożsamość.

* * *

Teraz Ida potrzebowała nowego adresu korespondencyjnego.

Przejrzałam u brokerów sprzedaży baz danych [ang. *data broker*] dotyczące mnie dokumenty. Stało się więc dla mnie jasne, że jeśli Ida zacznie otrzymywać listy na mój adres, trafi do rejestrów jako moja współpracownica albo członek rodziny.

Zaczęłam rozważać otwarcie skrytki pocztowej na nazwisko Idy, ale przy odbiorze przesyłek poczta wymaga przedstawienia dokumentu tożsamości. To by nie wyszło. Sprawdziłam magazyn UPS-u, ale zasady były takie

same.

Przekonałam więc przyjaciela, aby zaczął przyjmować listy adresowane do Idy. Mieszka w dużym bloku, w którym przesyłki wrzucane są do skrzynek podobnych do tych na poczcie. Jedyne, co musiałam zrobić, to przykleić imię i nazwisko Idy wewnątrz skrzynki. I już miała adres.

Z kartą kredytową i adresem, Ida miała nieskończone możliwości. Mimo to, chciałam zachować ostrożność w stosunku do jej kont internetowych.

Skonsultowałam się z Michaelem Sussmannem, byłym prokuratorem w Departamencie Sprawiedliwości, pracującym obecnie jako prawnik dla takich firm jak Google[15]. Powiedział mi, że usługodawcy internetowi zachowują na zawsze informacje dotyczące rejestracji. Z tego względu, powinnam zwracać uwagę, gdzie zakładam konto.

Wirtualne życie Idy zaczęło się w kawiarni z darmowym dostępem do sieci Wi-Fi, do której podłączyłam swojego laptopa. Usiadłam, zamówiłam cappuccino, otworzyłam komputer i uruchomiłam przeglądarkę Tor, która ukrywa IP komputera wykorzystując do tego szczególny rodzaj trasowania przesyłu danych przez sieć komputerów rozmieszczonych na całym świecie[16]. Wydawało się, że tym razem nadaję z Niemiec.

Po Torze surfuje się wolno. W ramach eksperymentu wpisałam stronę Uniwersytetu Nowojorskiego (www.nyu.edu) do wyszukiwarki Tor oraz do Firefoxa. Zmierzyłam czas. Uruchomienie strony w Torze zajęło 20 sekund, a w Firefoksie – 3 sekundy. Korzystając z wyszukiwarki Tor, miałam przynajmniej czas na wypicie kawy.

Zaczęłam od rejestracji w darmowym koncie Microsoft Outlook. Zacisnęłam zęby i wpisałam pomocniczy numer telefonu: 212-867-5309 (nawiązywał on do znanej piosenki Tommy'ego Tutone z lat 80.). Wyłączyłam funkcję reklamy ukierunkowanej.

Zadowolona z siebie, założyłam jej także profil na OpenTable, podając adres z poczty Outlook. Nie wpisałam numeru telefonu. Nie wiem, dlaczego wcześniej na to nie wpadłam. Następnie otworzyłam Idzie konto na Amazonie, podając jej numer karty kredytowej oraz adres mojego przyjaciela. Zrezygnowałam z usługi „Amazon betterizer", która umożliwiała tworzenie spersonalizowanych ofert[17].

Pierwszą książką, którą zamówiłam, był egzemplarz *Surveillance in the Stacks: The FBI's Library Awareness Program*[18]. To opublikowana w 1991 roku opowieść bibliotekarza, opisująca prowadzone przez FBI w latach 80.

działania. Celem agentów było skłonienie bibliotekarzy do węszenia w książkach, w których cudzoziemcy pozostawiali notatki. Program[19] przyczynił się do tego, że w praktycznie każdym stanie zostały wprowadzone prawa chroniące tajemnicę ewidencji bibliotecznej.

To miał być figiel: posłużyłam się fikcyjną tożsamością, aby zamówić książkę o tym, dlaczego poufność danych związanych z wypożyczeniam książek powinna być chroniona prawem.

* * *

Zajęło mi trochę czasu, aby zrozumieć, kiedy mogę być sobą, a kiedy powinnam udawać Idę.

Ida zamawiała wszystkie moje książki na Amazonie. Rezerwowała za mnie stoliki w restauracjach. Płaciła za posiłki, kiedy umawiałam się z kimś na wywiad. Wkrótce miałam dziesiątki kont w internecie założonych na Idę. Stworzyłam arkusz z jej wszystkimi loginami i hasłami.

Jednak dowiedziałam się też, czego Ida zrobić nie może. Próbowałam zapłacić kartą kredytową w sklepie sportowym Modell, gdy kasjer poprosił mnie o pokazanie dowodu tożsamości, którego dane pokrywałyby się z tymi na karcie. Zapłaciłam więc gotówką. Taką samą sytuację miałam w Old Navy, ale już nie w butiku marki Rag & Bone, gdzie Ida bez problemu kupiła sweter. Cóż, wydawało się, że Ida powinna trzymać się sklepów znanych projektantów.

Dzięki Idzie dowiedziałam się, w których miejscach jestem rozpoznawalna. Kiedy usiadłam w swoim ulubionym barze nieopodal biura, barmanka przywitała mnie słowami „Cześć, Julia". Byłam zdziwiona, że znała moje imię. Mimo, że nieraz rozmawiałyśmy przy kontuarze, nie przypominałam sobie, abym mówiła jej, jak mam na imię. Zdałam sobie sprawę, że musi kojarzyć je z karty płatniczej. Aby nie wzbudzać podejrzeń, schowałam więc do torebki kartę Idy Tarbell i zapłaciłam swoją, wystawioną na Julię Angwin.

Im częściej podawałam się za Idę, tym bardziej martwiłam się, że nadużywam jej tożsamości. Wkrótce nawet oceniono jej zdolność kredytową: Ida zaczęła otrzymywać oferty kart kredytowych od innych firm (American Express twierdzi, że nie sprzedaje danych swoich klientów, więc nie było wiadomo jak Ida trafiła na listę marketingową)[20]. Zrozumiałam, że jeśli przestanę być ostrożna, Ida trafi do bazy jakiegoś

brokera danych, oznaczona jako mój alias.

Doszłam do wniosku, że potrzebuję innych fikcyjnych tożsamości, aby odciążyć Idę.

* * *

Nie miałam jednak wystarczająco dużo siły, by stworzyć kolejną postać: wymyślić jej datę i miejsce urodzenia, a także nowe hasła. Brakowało mi odwagi, by jeszcze więcej kłamać.

Poszukiwałam prostszego i szybszego sposobu stworzenia fikcyjnej tożsamości.

Znalazłam wiele serwisów umożliwiających tworzenie jednorazowych adresów e-mail, umożliwiających przede wszystkim blokowanie wiadomości SPAM. Na przykład zakładając konto w portalu spamgourmet.com, zyskiwałam pulę bezpłatnych aliasów adresów pocztowych do podawania na stronach, na których się logowałam[21].

Znów jednak moje lenistwo wzięło górę: nie chciałam wymyślać kolejnych użytkowników przypisanych do oddzielnych adresów e-mail. Zaczęłam więc korzystać z darmowej usługi MaskMe, stworzonej przez Albine[22] – start-up działających w obszarze ochrony prywatności. Aplikacja umożliwiała stworzenie fałszywego adresu e-mail do każdego konta. Kiedy chciałam przeczytać artykuł na stronie ForeignPolicy.com i musiałam w tym celu utworzyć konto, MaskMe kreowała dla mnie adres e-mail: 18123a18@opayq.com. Później MaskMe przesyłała na moją skrzynkę e-maile kierowane na ten adres, do ustalonego przeze mnie limitu. Gdy ich liczba przekraczała ustalony pułap, usługa je blokowała.

Blokowanie e-maili sprawiało mi przyjemność. Gdy otrzymałam trzy wiadomości od firmy Klout, zajmującej się oceną widoczności osób w mediach społecznościowych, zablokowałam kolejne. Wcześniej zalogowałam się do jej serwisu, przeprowadzając swój społecznościowy audyt. Po otrzymaniu siedmiu e-maili od RecordedFuture.com, przedsiębiorstwa zajmującego się analizą wielkich zbiorów danych, także zablokowałam ich odbieranie.

Zarejestrowałam konto premium MaskMe, płatne 5 dolarów miesięcznie, które oferowało uruchomienie numeru telefonu z możliwością przekierowania go na dowolny, inny numer. Mogłam od teraz podawać kontakt do siebie bez obaw o to, że handlowcy będą wydzwaniać do mnie

od rana do nocy.

Zaczynałam radzić sobie coraz lepiej w tym biznesie opartym na oszukiwaniu. Najlepszym sposobem uczestniczenia w nim, była automatyzacja kłamstwa.

* * *

Ciężko jednak było zautomatyzować oszustwo przy kasie.

Oczywiście, zawsze mogłam płacić gotówką. Niemodna i nielubiana gotówka jest przede wszystkim anonimowa. Waluta amerykańska posiada numery seryjne, więc osoby ogarnięte paranoją na punkcie prywatności wymieniają ją, by uniknąć ryzyka bycia śledzonym. Jednak w moim modelu zagrożenia, polegającym na unikaniu dragnetów, gotówka była w sam raz.

Noszenie pliku banknotów jest nierozważne i niepraktyczne. Starałam się odzwyczaić od używania kart, ale wciąż wolałam nimi płacić, głównie ze względu na możliwość kontrolowania wydatków. Poza tym, nie znoszę wypychać sobie portfela rachunkami, aby móc je później rozliczyć.

Próbowałam używać karty przedpłaconej z limitem w wysokości 200 dolarów, którą kupiłam za gotówkę w lokalnej drogerii. Korzystałam z niej w trakcie mniejszych zakupów: płaciłam za lunch nieopodal biura, kawę czy za spodenki z J. Crew warte 27 dolarów. Podobało mi się, że na rachunku zamiast imienia widniał napis „MojaKartaPodarunkowa", a sprzedawcy bez mrugnięcia oka ją przyjmowali. Jednak gdy saldo na koncie zmniejszało się, przestawałam z niej korzystać. Czułam się głupio prosząc kasjera, by pobrał 5 dolarów i 32 centy z karty, a resztę gotówką. I nie znosiłam marnować pozostających na karcie pieniędzy.

Spróbowałam innego rozwiązania: wirtualnej karty kredytowej. Chodzi o numer karty do jednorazowego użytku, za pomocą którego można płacić u jednego sprzedawcy. W rzeczywistości jest to karta przedpłacona, wydawana do konkretnej transakcji. Otrzymałam taki jednorazowy numer w usłudze MaskMe Premium, która generowała dla mnie adresy e-mail i numery telefonów.

Pierwsza próba użycia karty okazała się porażką. Chciałam kupić nowe topy do jogi, ponieważ stare były poprzecierane. Znalazłam ubrania przez internet i umieściłam je w moim internetowym koszyku. Podałam swoje prawdziwe dane. Kiedy strona obliczyła kwotę, uwzględniającą koszt

przesyłki, MaskMe wygenerowała numer karty kredytowej z odmierzoną na transakcję sumą. Karta została odrzucona. Spróbowałam kolejny raz, ale z podobnym rezultatem: AUTORYZACJA PŁATNOŚCI ODRZUCONA.

Miałam związane ręce. Wydawało się, że MaskMe uważała, że zapłaciłam. Z informacji z karty kredytowej wynikało, że płatność została przyjęta. Jednak strona internetowa twierdziła, że transakcja nie została zrealizowana. Moje pieniądze wyparowały.

Po godzinie spędzonej na rozmowie z firmą Albine, zrozumiałam mój błąd: powinnam była podać adres Albine jako adres płatnika. W międzyczasie zadzwoniłam do administratora sklepu, wycofałam transakcję i zamówiłam bluzki przez telefon, korzystając ze swojej zwykłej karty.

Tydzień później spróbowałam ponownie, próbując kupić płytę CD Instytutu Smithsonian z dziecięcymi piosenkami ludowymi. Podałam adres Albine jako adres płatnika. Tym razem transakcja przeszła bez problemu. Uff. Oczywiście, całe to przedsięwzięcie wydawało się głupie, ponieważ nadal podawałam swoje prawdziwe dane do wysyłki. Zdecydowałam, że poszukam bardziej anonimowej waluty.

Miałam zamiar kupić *bitcoiny* – wirtualną cyfrową walutę, za którą szalało środowisko hakerów[23]. Jednak nie potrafiłam znaleźć miejsca, w którym mogłabym je nabyć przy użyciu karty kredytowej. Wszyscy prosili o podanie numeru konta bankowego albo o przelew internetowy. Zapewne wynikało to z faktu, że ludzie często dzwonili do wystawców kart, narzekając, iż nie otrzymali wirtualnej gotówki.

Bitcoiny mogą być stosowane na „czarnych rynkach", na których sprzedaje się broń i narkotyki[24]. Także tradycyjne firmy zaczęły już akceptować tę walutę. Gdy w maju 2013 roku Kashmir Hill, reporterka „Forbesa", przez tydzień posługiwała się wyłącznie *bitcoinami*, przeżyła głównie dzięki dostawcy żywności z San Francisco, który przyjmował płatności także w tej walucie[25].

Wszystkie transakcje w *bitcoinach* są rejestrowane i publiczne. Nie są powiązane z nazwiskiem, ale zdeterminowany śledczy z pewnością potrafiłby zidentyfikować osoby, które za nimi stoją. Nie był to więc rodzaj anonimowości, której poszukiwałam.

Im dłużej przyglądałam się anonimowym transakcjom cyfrowym, tym mniej mi się one podobały. Sprawiały wrażenie raju dla przestępców.

W 2007 roku start-up z branży cyfrowej waluty, E-gold, został oskarżony

o pranie brudnych pieniędzy[26]. Firmie zarzucono, że była świadoma faktu, iż z jej waluty korzystali złodzieje tożsamości, amatorzy pornografii dziecięcej i inni przestępcy. Rok później właściciele E-gold przyznali się do winy[27]. W 2013 roku, prokuratorzy federalni zamknęli Liberty Reserve, internetowy kantor wymiany walut, zapewniający anonimowość transakcji, po oskarżeniach, że służył on jako przykrywka do prania brudnych pieniędzy dla pedofili i innych kryminalistów[28]. Wartość ich nielegalnych operacji miała sięgać 6 mld dolarów.

„Gdyby Al Capone żył w dzisiejszych czasach, właśnie w ten sposób ukrywałby swoje pieniądze", powiedział Richard Weber, szef wydziału ścigania przestępstw Amerykańskiego Urzędu Podatkowego (Internal Revenue Service, IRS).

Niektórzy przewidują, że całkowita *anonimizacja* transakcji finansowych może spowodować rozpad społeczeństwa. W 1996 roku anarchista Jim Bell zamieścił na forum internetowym esej zatytułowany „Assasination Politics", opisujący jak anonimowe pieniądze mogłyby doprowadzić do usankcjonowania nagród finansowych dla ludzi potrafiących precyzyjnie „przewidzieć" czyjąś śmierć[29]. „Byłoby możliwe zorganizowanie tego w ten sposób, by nikt nie wiedział, kto otrzymuje nagrodę. Wiedzianoby jedynie, że jest ona wręczana". Bell opisał istnienie rynku przewidywania śmierci jako sposobu karania „tych, którzy łamią prawo" przez ustanawianie nagród za ich głowy. „Wyobraźcie sobie, jak potoczyłaby się historia ludzkości, gdybyśmy zawczasu pozbyli się Lenina, Stalina, Hitlera, Mussoliniego, Tojo, Kim Ir Sena, Ho Szi Mina, ajatollaha Chomejniego, Saddama Husajna, Muammara Kaddafiego i wielu innych, wliczając w to ich ewentualnych następców. A to wszystko za marnych parę milionów dolarów"[30].

Pomysł przyznawania nagród za głowy przywódców państw nie został ciepło przyjęty. W 1997 agenci IRS dokonali przeszukania domu Bella[31]. Został on oskarżony o utrudnianie działania wymiaru sprawiedliwości oraz fałszowanie numerów ubezpieczenia społecznego. Skazano go na jedenaście miesięcy pozbawienia wolności.

Niewątpliwie zaproponował on skrajną wizję. Jednak jego esej sprawił, że ponownie zaczęłam zastanawiać się nad pytaniem natury etycznej, postawionym przez Sisselę Bok. Co by się stało, gdyby wszyscy – znalazłszy się na moim miejscu – kłamali?

Zaczęłam rozumieć, że tym, do czego dążyłam nie była anonimowość,

a w istocie całkowita nietykalność. Pragnęłam być niepodatna to, co stanowiło konsekwencję dokonywania mało istotnych transakcji. Nie chciałam, żeby ludzie, z którymi jadłam lunch, mogli być podejrzewani o przekazywanie informacji dziennikarce. Nie chciałam, bym przez wzgląd na to, co kupowałam w sieci, była szufladkowana jako osoba, która dużo wydaje, a przez to wykluczana z grona osób, którym oferuje się rabaty. Nie chciałam być posądzana o anarchizm, tylko dlatego, że czytałam o *bitcoinach*. Z drugiej strony nie wykonywałam żadnych podejrzanych transakcji. To nie dlatego dążyłam do nietykalności.

Moja chęć uniknięcia konsekwencji zakupów w internecie, przypomniała mi rozważania antrolopoga Davida Graebera nad znaczeniem i moralnymi skutkami długu. W swojej książce *Debt: The First 5000 Years* opisuje zobowiązania, których nigdy nie powinno się spłacać, takie jak choćby długi wobec rodziców czy dług za bezinteresowną uprzejmość.

Tylko niektóre zobowiązania można uregulować za pomocą pieniędzy. Mają one pewne cechy wspólne. Są to świadczenia między jednostkami „potencjalnie równymi" ale „w danym momencie nie znajdującymi się w stanie równości", w kontekście których pieniądze wykorzystuje się do wyrównania rachunków. „Dług to po prostu wymiana, która nie została dokończona"[32].

Zrozumiałam, że wymarzona przeze mnie nietykalność przypominała pragnie zadłużonego. Pragnęłam, by po tym, jak moja transakcja dobiegła końca, moje zobowiązania zostały w pełni umorzone. By wrócić do stanu równowagi pomiędzy mną a wierzycielem.

Wygląda jednak na to, że w erze gospodarki opartej na danych osobowych, nigdy nie będę wolna od długów. Moje transakcje będą mnie wiecznie prześladować, podążając za mną i informując o wyborach, których dokonałam. Dopóki więc nie byłam w stanie znaleźć innego wyjścia, dopóty musiałam wyrównywać rachunki za pomocą Idy i mojej fikcyjnej tożsamości.

10

PRZETRZĄSANIE KIESZENI

Stałam niespokojnie pod Zegarem Światowym na Alexanderplatz w Berlinie. Właśnie przyjechałam do miasta[1], gdzie umówiłam się na spotkanie z Jacobem Appelbaumem, badaczem ds. cyberbezpieczeństwa. Ponieważ był wolontariuszem WikiLeaks, amerykański rząd potajemnie śledził jego skrzynkę e-mail, co zostało ujawnione w 2010 roku.

Nie miałam możliwości się z nim skontaktować – nie podał telefonu, adresu, kompletnie niczego. Po prostu musiałam czekać, aż pojawi się w ustalonym wcześniej miejscu.

Byłam gotowa przelecieć pół świata, aby się z nim zobaczyć. Jednak nie miałam żadnego planu awaryjnego na wypadek, gdyby się nie pojawił. Czułam się zdemaskowana.

Oto uwarunkowania pracy dziennikarza w świecie, w którym za pomocą telefonu można zdalnie śledzić czyjąś lokalizację. Z osobami posiadającymi wrażliwe informacje muszę spotykać się osobiście, bez korzystania z dobrodziejstw technologii.

Stałam więc jak jakaś dziwaczka pod zegarem, który przez dziesiątki lat służył za miejsce spotkań berlińczyków. Wszyscy wokół sprawdzali swoje telefony. Wyobrażałam sobie, że piszą właśnie do swoich znajomych, pytając gdzie są, podczas gdy tamci zapewniają, że zaraz się pojawią. To przywilej ery cyfrowej, z którego tym razem nie mogłam skorzystać.

Spojrzałam na mężczyznę z długimi włosami, który parkował swój rower. Czy to Jake? Zdałam sobie sprawę, że tylko raz widziałam jego zdjęcie w internecie. A zresztą, mógł przecież ukrywać swoją tożsamość, używając starego albo niewyraźnego zdjęcia.

Rowerzysta wyjął jednak komórkę, aby zadzwonić. Uznałam więc, że to nie on.

Kilka minut później, utkwiłam wzrok na człowieku w okularach w drucianych oprawkach, który nie zerkał w telefon. Może to on? Nawet nie spojrzał w moim kierunku, a po chwili zaczął machać do faceta po drugiej stronie placu.

W końcu, bez uprzedzenia, Jack pojawił się tuż obok mnie. Wyglądał dokładnie tak, jak się spodziewałam. Ponieważ moje zdjęcie łatwo znaleźć w internecie, rozpoznał mnie od razu. Odetchnęłam z ulgą, gdy ruszyliśmy do pobliskiej kawiarni, aby porozmawiać.

Przyznałam w końcu, że mam telefon w torebce. Wiem, że nie powinnam była go brać, ale wrzuciłam go do torby w ostatnim momencie. Byłam w obcym mieście i obawiałam się, że mogłabym go potrzebować.

– Wyłączyłam go – wyjaśniłam przepraszającym tonem.

– Ha! – zaśmiał się – Skąd wiesz, że jest wyłączony? Wyjęłaś z niego baterię? Możesz mieć na telefonie zainstalowane oprogramowanie szpiegujące, które zmusza urządzenie do przekazywania informacji, nawet kiedy wydaje się być wyłączone.

Miałam wrażenie, że Jake ma lekką paranoję. Jako działacz WikiLeaks jest często zatrzymywany na amerykańskiej granicy. Jest więc bardziej obeznany z zagrożeniami związanymi z inwigilacją niż większość osób. Jednak w tym przypadku miał rację.

Mniej więcej rok po naszym spotkaniu Ira „Gus" Hunt, szef ds. technologii w CIA, pochwalił się możliwościami Agencji w dziedzinie śledzenia urządzeń mobilnych[2]. „Macie świadomość, że ktoś może wiedzieć, gdzie się znajdujecie, w dowolnym momencie, ponieważ nosicie przy sobie telefon komórkowy, nawet jeśli jest wyłączony", powiedział Hunt w trakcie wystąpienia „The CIA's Grand Challenges with Big Data". „Mam nadzieję, że to wiecie? Prawda? No cóż, powinniście."

Do tej pory nie wiadomo, o jakiej technologii śledzenia mówił Hunt. W 2006 roku Federalne Biuro Śledcze (FBI) uzyskało nakaz sądowy[3], umożliwiający zainstalowanie w telefonie podejrzanego aktywowanej zdalnie pluskwy [ang. *roving bug*]. Agenci Biura mogli go podsłuchiwać, nawet gdy miał wyłączony telefon. Hunt potwierdzał to, z czego Jake i inni zdawali sobie doskonale sprawę: telefony komórkowe są najbardziej efektywnym urządzeniem służącym śledzeniu, nawet jeśli są nieaktywne.

* * *

W wywiadzie stosuje się metodę zwaną „przetrząsaniem kieszeni". Dawniej rozumiano to dosłownie – szukano skrawków papieru i innych drobiazgów, które można było znaleźć w czyjejś garderobie. Takie rzeczy często zawierały informacje o powiązaniach i kontaktach danej osoby. Numery telefonów, adresy czy numery kont pozwalały rozwinąć śledztwo.

Obecnie najważniejszą zawartość naszych kieszeni stanowią telefony komórkowe, które są miniaturowymi komputerami. Przechowujemy w nich książkę adresową, praktycznie wszystkie wiadomości, zdjęcia, muzykę, a nawet informacje o tym, w co gramy.

Co gorsza, nasz elektroniczny „kieszonkowy śmieć" można przejrzeć zdalnie. Dawniej pracownicy organów ścigania musieli najpierw kogoś aresztować, by móc przeszukać jego kieszenie. Teraz, zarówno rządowi jak i prywatni gracze dysponują zdalnym dostępem do informacji o naszej lokalizacji, a także do innych danych, które uzyskują przy współpracy z operatorami komórkowymi.

Najbardziej oburzającym przykładem monitoringu połączeń telefonicznych jest program ujawniony przez Edwarda Snowdena, byłego współpracownika Agencji Bezpieczeństwa Krajowego (NSA)[4]. Opierał się na ścisłej współpracy Agencji z operatorami telekomunikacyjnymi, którzy przez siedem lat przekazywali jej dane o każdej rozmowie telefonicznej realizowanej na terytorium USA. Prezydent Obama tłumaczył, że program po prostu „dobierał w pary" połączenia[5]. Przedstawił to bardzo oględnie: „Macie mój numer telefonu, który łączy się z waszym. W tej bazie danych nie ma danych osobowych, ani żadnych innych elementów. Jedyne co się tam znajduje, to informacje o numerach oraz o tym, kiedy i jak długo trwały rozmowy telefoniczne".

Również zdecydowana większość jednostek policji śledzi połączenia, na podstawie niejawnych wniosków o udostępnienie informacji, przesyłanych do operatorów sieci komórkowych z pominięciem procedury sądowej. W 2011 roku najwięksi dostawcy usług telekomunikacyjnych odpowiedzieli na 1,3 mln zapytań o dane abonentów (w tym ich lokalizację) ze strony organów ścigania[6]. Firma AT&T przyznała, że odpowiadała wtedy na 700 wniosków dziennie, co stanowiło liczbę trzykrotnie większą w stosunku do 2007 roku.

Ze względu na nasilanie się zjawiska śledzenia telefonów komórkowych

bez nakazu[7], niektórzy sędziowie zaczęli kwestionować ich legalność. Od 2005 roku ponad dwanaścioro sędziów magistrackich przedstawiło pisemne opinie oddalające wnioski o założenie podsłuchu na telefonie komórkowym. Rewoltę zapoczątkował w 2005 roku Stephen Smith, sędzia magistracki dla Południowego Dystryktu w Teksasie. Odmówił przekazania rządowi informacji o bieżącej lokalizacji telefonu. Smith zakwestionował sformułowane przez rząd, „kreatywne" uzasadnienie faktu ominięcia procedury uzyskania sądowego nakazu rewizji. Po decyzji Smitha, sędziowie z innych okręgów zaczęli odrzucać wnioski, w których brakowało nakazu.

Sądy wyższej instancji podzieliły się w sprawie dostępu do danych zawierających historię lokalizacji telefonu. W 2010 roku Sąd Apelacyjny USA dla Trzeciego Okręgu orzekł[8], że sędziowie okręgowi mogą, wedle uznania, żądać nakazu rewizji w sprawach o uzyskanie rejestrów z historią połączeń telefonicznych przy „utrudnionej możliwości zrozumienia intencji ustawodawcy w tym zakresie". Jednak w 2013 roku, Sąd Apelacyjny USA dla Piątego Okręgu podważył wyrok sędziego Smitha[9]. „Rozumiemy uzasadnione oczekiwanie użytkowników telefonów komórkowych, że informacje o ich lokalizacji pozostaną w domenie prywatności. (...). Jednak miejscem, gdzie można znaleźć rozwiązanie tego problemu, jest rynek lub proces polityczny", napisał sędzia Edith Brown Clement.

Dopóki Sąd Najwyższy nie wyda orzeczenia w tej sprawie, inwigilacja telefoniczna pozostanie w gestii prawa lokalnego.

* * *

Jak ważne są „kieszonkowe śmieci"? Informacja o tym, kiedy i do kogo dzwonimy, może ujawniać o nas tyle samo, co temat rozmowy.

Szpiedzy, którzy nie mogli odczytać wiadomości wroga, długo polegali na tzw. analizie ruchu, polegającej na identyfikacji schematów nadawania i odbierania wiadomości, ich czasu i długości. Podczas I wojny światowej Francuzi mieli problem z odszyfrowaniem niemieckiego kodu znanego pod nazwą ADFGVX[10]. Wiedzieli jednak, że był on stosowany do wydawania z wyprzedzeniem rozkazów i wskazówek, co pomogło im przewidzieć początek niemieckiej ofensywy wiosną i latem 1918 roku. Nawet kiedy Niemcy zmienili charakterystyczne dla nadawcy znaki przesyłane sygnałem radiowym, Francuzi mogli rozpoznać połączenia, wykorzystując

inne schematy. „Kilka dni przed operacją, liczba przechwyconych wiadomości była większa niż zazwyczaj", pisał w książce zatytułowanej *German Military Ciphers from February to November 1918* J.R Childs, porucznik armii amerykańskiej.

Podczas II wojny światowej, Japończycy przechytrzyli Stany Zjednoczone, tworząc fałszywą komunikację radiową. Przed atakiem na Pearl Harbor, przenieśli na ląd swoich radiooperatorów pokładowych[11]. W przekonaniu Amerykanów japońska flota powinna być nadal w porcie.

Stany Zjednoczone wyciągnęły wnioski z tego wydarzenia. W 1942 roku utworzono grupę analityków[12], która miała badać japońską komunikację radiową na Pacyfiku. Mimo że nie udało jej się złamać japońskiego szyfru do 1943 roku, jednostka była w stanie „zidentyfikować położenie wojsk, hierarchię dowodzenia oraz rozkaz rozpoczęcia bitwy".

W latach 50. NSA przeniosła analizę komunikacji z kart perforowanych do komputerów. Zadaniem analityka było „stworzenie obrazu śledzonego celu"[13], jak wynika z ankiety NSA, przeprowadzonej w 1982 roku. „Kiedy analityk zna już normalne zachowanie swojego celu, jest w stanie wykryć jego odchylenia, które raportuje jednostce wywiadowczej".

Takie „anomalie" mogą ujawnić naprawdę sporo informacji. W 2004 roku, libański Hezbollah schwytał, według różnych szacunków, około 100 szpiegów, w tym najpewniej kontakty CIA[14]. Było to możliwe, dzięki zidentyfikowaniu rzadko używanych telefonów komórkowych albo takich, z których korzystano w określonych miejscach przez krótki czas.

* * *

Im więcej dowiadywałam się o inwigilacji telefonów komórkowych, tym bardziej przekonywałam się, że przed dragnetami nie ma ucieczki.

Najbardziej oczywistym rozwiązaniem było zostawienie telefonu w domu. Jednak jako matka małych dzieci uważam, że nierozważne byłoby pozostawanie poza zasięgiem o jakiejkolwiek porze dnia i nocy. Mój mąż się z tym zgadzał. Zdecydowałam więc, że moim następnym krokiem będzie zakup „palnika" [ang. *burner*]. Określenie to w slangu oznacza telefon na kartę, z którego korzysta się przez krótki okres, a następnie porzuca.

Telefony na kartę nie są jednak doskonałym rozwiązaniem. Śledczy,

wkładając w to odpowiedni wysiłek, mogą powiązać „palnik” z waszymi danymi, na podstawie schematu połączeń i lokalizacji, z których są one wykonywane. Z drugiej strony, anonimowy zakup takiego telefonu oznacza, że jeśli nawet wasze dane zostaną sprzedane lub zarchiwizowane przez rząd, śledzącym sporo czasu zajmie powiązanie tych danych z waszą prawdziwą tożsamością.

Uznałam, że spróbuję. Zastanawiałam się nad wyborem aparatu i ostatecznie zdecydowałam się na telefon z systemem Android, ponieważ w porównaniu do iPhone’a oferował więcej aplikacji zapewniających ochronę prywatności. Wybór operatora był o wiele trudniejszy. Żaden bowiem nie oferował opcji braku przechowywania danych. Według dokumentu organów ścigania, do którego dotarł związek American Civil Liberties Union[15], większość takich firm przechowuje szczegóły billingów przez ponad dwa lata, a AT&T przez okres od pięciu do siedmiu lat. Ostatecznie, uznałam, że wszystkie sieci, poza AT&T, są takie same, więc zdecydowałam się na tanią ofertę Virgin Mobile.

Najlepszy sposób na zakup „palnika” polega na nabyciu go za gotówkę, z dala od domu. Wyciągnęłam 200 dolarów w gotówce i wybrałam się do sklepu na środkowym Manhattanie, który wydawał się zapewniać wystarczającą anonimowość. Kasjerka nalegała, abym nacisnęła kilka ekraników na terminalu płatniczym, mimo że nie korzystałam z karty. Następnie zaproponowała mi rabat na dodatkową gwarancję, pod warunkiem, że wpiszę swoje dane osobowe do urządzenia. Później, na tej samej zasadzie, zaoferowała mi zniżkę na telefon. Grzecznie odmówiłam, ale zmuszona do ciągłego odmawiania, czułam się jak przestępca. Gdy wychodziłam ze sklepu z telefonem w torbie, czułam się jakbym niosła kontrabandę. Spojrzałam do góry, aby sprawdzić czy nad drzwiami nie są zainstalowane kamery. Żałowałam, że nie miałam na sobie czapki z daszkiem.

Następnym krokiem był zakup w innym sklepie, za gotówkę, karty przedpłaconej ważnej przez 30 dni. Wiedziałam, że będę miała problem z jej regularnym doładowywaniem, jeśli będę opierać się wyłącznie na gotówce. Wróciłam do domu i użyłam karty kredytowej Idy Tarbell, aby kupić *pre-paid* w Virgin Mobile. Nie zamierzałam być kompletnie anonimowa. Chciałam jedynie, aby ci, którzy mnie śledzą, musieli włożyć trochę więcej pracy w namierzenie mnie.

* * *

Nie podawałam innym mojego numeru do telefonu na kartę. Zamiast tego, przekazałam mężowi, opiekunce do dzieci i kilkorgu znajomych numer telefonu z MaskMe, który kupiłam w Abine. Ustawiłam to tak, że wszystkie połączenia kierowane na maskujący numer, były przekazywane do „palnika".

Problem polegał na tym, że korzystając z maskującego numeru, nie mogłam wykonywać połączeń ani wysyłać wiadomości tekstowych. Mogłam tylko je odbierać. Gdybym odpisała, wiadomość zostałaby wysłana z numeru pre-paida.

Coraz bardziej zbliżałam się w swych działaniach do granicy prawa. Podszywanie się pod dany numer telefonu, w celu dokonania oszustwa, jest bowiem nielegalne. W 2010 roku Prezydent Obama podpisał ustawę o prawdziwości identyfikatora dzwoniącego (Truth in Caller ID Act)[16], na mocy której zdelegalizowano szereg działań „obliczonych na przekazanie odbiorcy mylących bądź nieprawdziwych danych dzwoniącego, w celu dokonania oszustwa, wyrządzenia mu krzywdy lub pozyskania jakiejkolwiek rzeczy, mającej wartość".

Oczywiście, nie zamierzałam używać fałszywego numeru, aby kogokolwiek oszukać czy skrzywdzić. Mimo tego, nawet gdyby udało mi się stworzyć imitację numeru, i tak moje połączenia ujawniłyby moją tożsamość. Gdy przeglądałam rejestr połączeń realizowanych przeze mnie z podstawowej karty, uznałam, że mój schemat komunikacji jest bardzo przewidywalny (i raczej nudny). Każdego dnia około godziny 18. dzwonię do męża. Codziennie, albo prawie codziennie, rozmawiam ze zmieniającą się obsadą ekipy opiekunów moich dzieci, składającej się z mojej mamy, brata i kilkorga przyjaciół. Inne połączenia wpisują się w szerszy wzorzec.

Postanowiłam korzystać z telefonu na kartę wyłącznie w celach zawodowych. Podczas podróży służbowej do Waszyngtonu, przez trzy pełne spotkań i wywiadów dni, korzystałam tylko z niego. Wzięłam też iPhone'a, ale trzymałam go wyłączonego w hotelu, chcąc z niego korzystać tylko w celach prywatnych.

Jednak ciężko było nosić telefony oddzielnie. Kiedy utknęłam w korku, siedząc w taksówce, a chciałam zadzwonić do domu, użyłam „palnika". Gdy wróciłam do pokoju hotelowego, zapomniałam wyłączyć telefon na kartę, choć powinien być wyłączony, by telefony nie logowały się

w tych samych lokalizacjach.

Zrozumiałam co miał na myśli Mike Perry, samozwańczy „weganin inwigilacji", mówiąc, że używanie innych telefonów do różnych rodzajów kontaktów zmniejszyło jego szanse na utrzymanie bliskich relacji.

* * *

Przeładowałam mój telefon na kartę aplikacjami chroniącymi prywatność. Niemal natychmiast je znienawidziłam.

Do poruszania się po sieci pobrałam oprogramowanie maskujące, które przepuszczało mój ruch internetowy przez serwery rozsiane po całym świecie. Dzięki temu strony internetowe, które odwiedzałam przez telefon, nie wiedziały, skąd się łączę. (Oczywiście mój operator komórkowy wiedział skąd jestem, a przynajmniej wiedział skąd pochodzi Ida).

Myślałam, że przeglądarka Tor, z której korzystałam, aby założyć konta dla Idy, działała wyjątkowo wolno na laptopie. Przekonałam się jednak, że w telefonie jest jeszcze bardzo bardziej powolna. Była jak żółw i wyładowywała całą baterię. Ze stoperem sprawdziłam, że Torowi aż 14 sekund zajmowało rozpoczęcie trasowania, a kolejnych 6 sekund – uruchomienie wyszukiwarki stron www. Ostatecznie, proste wyszukanie hasła „pogoda w Nowym Jorku" zajmowało 43 sekundy. Oznaczało to, że trzeba było ponad minuty na znalezienie informacji o pogodzie.

Dla porównania: uruchomienie wyszukiwarki Google Chrome i wyszukanie hasła „pogoda w Nowym Jorku", zajmowało na moim iPhonie tylko 9 sekund.

Harlo Holmes, szefowa ds. metadanych w Guardian Project[17], tworzącym oprogramowanie Tor dla systemu Android, powiedziała, że przeglądanie stron www przy użyciu Tora trwa dłużej, ponieważ pomiędzy moim telefonem, a odwiedzaną stroną jest więcej „uskoków". „Bez wątpienia, w przypadku oprogramowania Tor mamy do czynienia z kompromisem pomiędzy prędkością a anonimowością", przyznała.

Ostatecznie, zrezygnowałam z Tora i zainstalowałam na telefonie aplikację DuckDuckGo. Uruchomienie jej i znalezienie informacji o „pogodzie w Nowym Jorku" zajmowało tylko 15 sekund. Trwało to wciąż dłużej niż w Google'u, lecz nie w nieskończoność, jak w przypadku Tora.

Zorientowałam się zresztą, że w ogóle unikam wyszukiwarek

internetowych. Pewnego wieczoru, kiedy wyszłam ze znajomym na drinka, stwierdziliśmy, że chcemy coś zjeść. Ale gdzie? Tak jak robi to dziś wiele osób, wyjęliśmy telefony. Próbowałam znaleźć jakieś rekomendacje przez DuckDuckGo, ale ponieważ wyszukiwarka nie wie, gdzie się znajduję, właściwe ustawienie współrzędnych zajęło mi trochę czasu. Podczas gdy ja wpisywałam: „restauracje meksykańskie, Madison Square, Nowy Jork", mój znajomy zdążył już znaleźć odpowiednie miejsce w pobliżu.

Załamana, zadzwoniłam do Moxie'ego Marlinspike'a, twórcy aplikacji z których korzystałam, zapewniających bezpieczeństwo rozmów i wiadomości (zresztą łatwych w użyciu)[18]. Marlinspike jest jednym z najinteligentniejszych i najbardziej utalentowanych hakerów telefonów. Zapytałam go, dlaczego tak trudno jest korzystać z tych wszystkich maskujących narzędzi.

„Nie ma tak naprawdę rynku dla oprogramowania zapewniającego prywatność konsumenta", powiedział. Działalność jego i większości deweloperów telefonów komórkowych, dla których liczy się prywatność (takich jak Guardian Project), finansowana jest głównie z grantów.

Marlinspike przyznał, że starał się przyciągnąć utalentowanych programistów, którzy mogliby pracować dla start-upów z Doliny Krzemowej. Swój ostatni grant wykorzystał na to, by wysłać zespół deweloperów na Hawaje i pozwolić im przez tydzień pracować na plaży. Jednak Marlinspike działa na niewielką skalę. Jego aplikacje, takie jak RedPhone i TextSecure, funkcjonują wyłącznie na Androidzie, a większość moich znajomych korzysta z iPhone'ów. Nie mogę więc szyfrować połączeń za pomocą jego aplikacji.

Roześmiał się, gdy opowiedziałam mu o moich zmaganiach z Torem: „Zawsze, gdy korzystam z tej wyszukiwarki i działa szybko, obawiam się, że źle ją skonfigurowałem". I dodał: „Z większości tych narzędzi nie da się normalnie korzystać. Są naprawdę straszne. Musimy się z tym pogodzić".

* * *

Tymczasem branża monitoringu połączeń komórkowych stworzyła jeszcze bardziej zaawansowane narzędzia, umożliwiające śledzenie lokalizacji.

Pęd prywatnego sektora ku rozwinięciu zdolności do określenia lokalizacji każdego urządzenia na świecie rozpoczął się wraz z praktyką

zwaną wardrivingiem[*16]. Pierwszy raz udałam się na *wardriving* w 2002 roku w asyście techników operatora kablówki, którzy pokazali mi, na czym to polega. Gdy jeździliśmy w kółko samochodem, technik siedzący w fotelu pasażera trzymał laptopa, na którym uruchomione było oprogramowanie skanujące obszar pod kątem występowania na nim sieci Wi-Fi. Kiedy znajdowaliśmy niezahasłowany punkt dostępowy Wi-Fi, zatrzymywaliśmy się i obserwowaliśmy ruch internetowy na ekranie komputera. Nie odczytywaliśmy go, choć mogliśmy.

W 2003 firma Skyhook z Bostonu zaczęła zarabiać na tego typu działaniach[19]. Rozmieściła ona samochody, które skanowały nazwy i siłę sygnału hot spotów Wi-Fi. Firma nie odczytywała danych o tym ruchu, a jedynie określała na mapie położenie sieci Wi-Fi na świecie. „Przez pierwsze cztery, pięć lat, ludzie myśleli, że jesteśmy wariatami", mówi twórca Skyhook, Ted Morgan.

Pomysł Skyhook się opłacił. Okazało się bowiem, że punkty dostępu Wi-Fi są na tyle gęste, że mogą przekazywać precyzyjne informacje o lokalizacji. Działa to następująco: telefon wykrywa sieci Wi-Fi w pobliżu, znajduje ją w bazie Skyhook i wykorzystuje zdobyte informacje do określenia lokalizacji.

Lokalizowanie telefonów za pomocą Wi-Fi okazało się znacznym udoskonaleniem w stosunku do poprzednich metod – pomiarów triangulacyjnych z wykorzystaniem stacji przekaźnikowych BTS albo satelit GPS, których sygnały mogły być blokowane przez budynki czy inne przeszkody.

Wkrótce pojawiła się konkurencja dla Skyhook. W 2007 roku firma Google zaczęła używać swoich pojazdów Street View do prowadzenia wardrivingu i tworzenia własnej bazy Wi-Fi. Po tym, jak samochody Google'a przyłapano na przeglądaniu haseł do skrzynek e-mail i innych osobistych danych, firma zaprzestała tych działań, a do zbierania informacji o sygnałach Wi-Fi zaczęła wykorzystywać telefony działające na systemie Android.

W 2010 roku Apple zaczął tworzyć własną bazę Wi-Fi, wykorzystując do zbierania danych telefony iPhone. W istocie, Google i Apple używały telefonów konsumentów do prowadzenia wardrivingu. (Powinno się to chyba określać *warphoningiem*).

W międzyczasie takie działania podejmowali też producenci aplikacji telefonicznych i reklamodawcy. W 2010 roku zajmujący się aspektami

prywatności zespół dziennikarzy śledczych z „Wall Street Journal", któremu przewodziłam[20], wziął pod lupę 101 aplikacji telefonicznych i odkrył, że 47 z nich przekazuje dane o lokalizacji użytkowników innym firmom. Aż 45 aplikacji nie miało polityki prywatności, z której wynikałoby, w jaki sposób wykorzystywane są pozyskiwane dane.

Start-upy ścigały się ze sobą, chcąc stworzyć urządzenia, które przechwytywałyby sygnał sieci bezprzewodowej z telefonów użytkowników zbliżających się do danego miejsca. Niektóre przedsiębiorstwa zainstalowały takie systemy w galeriach handlowych, by śledzić ludzi robiących zakupy[21]. Renew, firma marketingowa z Londynu zainstalowała nawet elementy śledzące [ang. *trackers*] w koszach na śmieci, by móc obserwować ludzi, którzy przechodzili obok[22]. (Przedsiębiorstwo zaprzestało tej działalności, gdy zażądali tego przedstawiciele dzielnicy finansowej)[23].

Kaveh Memari, prezes Renew, przekonywał, że system zadziałał, ponieważ aż 80 proc. londyńczyków nie wyłącza funkcji Wi-Fi po wyjściu z domu albo z biura[24]. „Istnieje szansa, że nawet jeśli nie widzimy was pierwszego, drugiego, czy trzeciego dnia, ostatecznie i tak was złapiemy. Wystarczy, że namierzymy was choć jeden raz".

Nagle dostawcy bezprzewodowego internetu stracili monopol na wiedzę o lokalizacji użytkowników telefonów. Oczywiście to nie powód, by przestali handlować tymi danymi.

W 2012 roku, Verizon uruchomił przedsięwzięcie pod nazwą Precision Market Insights[25]. Operator zaczął oferować informacje o „wieku, rasie, płci, kodzie pocztowym w miejscu zamieszkania, pracy, zakupach i innych", a także dane o zwyczajach związanych z korzystaniem z urządzeń mobilnych „włączając w to informacje o odwiedzanych stronach, pobranych i używanych aplikacjach, trendach w przeglądaniu stron" i inne.

W 2013 roku firma AT&T również zdecydowała się na sprzedawanie informacji o lokalizacji abonentów i ich zwyczajach w sieci[26]. Śledzenie położenia użytkowników telefonów stało się dla wielu łakomym kąskiem. W odpowiedzi na zainteresowanie, zaczęto organizować konferencje takie jak: „Location Intelligence"[27] w Waszyngtonie, „Geoweb Summit"[28] w Nowym Jorku czy „Location Business Summit" USA w San Jose w Kalifornii[29].

W 2012 roku, na konferencji „Signal”[30] w Chicago, firma JiWire zajmująca się analityką lokalizacji[31], opisała wnioski jakie wyciągnęła z profilowania zachowania użytkowników ponad 7 mln urządzeń. „To gdzie jesteście mówi o was więcej niż jakiekolwiek inne dane”, przyznał David Staas, prezes JiWire[32].

* * *

Oczywiście, wszystkie firmy śledzące lokalizację, twierdzą, że zebrane przez nie dane są anonimowe. Gromadzą jedynie garść liczb, które odpowiadają numerom seryjnym waszych telefonów.

„Obecnie nie pozyskujemy i nigdy nie będziemy pozyskiwać informacji związanych z adresami, telefonami, e-mailami etc.”, napisał w liście do senatora Ala Frankena Will Smith, prezes specjalizującej się w usługach lokalizacji firmy Euclid[33]. Była to reakcja na projekt ustawy przygotowany przez wspomnianego senatora z Minnesoty[34], wprowadzająca wymóg uzyskania przez tego typu firmy pozwoleń na śledzenie lokalizacji użytkowników.

Euclid pomagała handlowcom w identyfikacji klientów za pośrednictwem sygnałów Wi-Fi wysyłanych przez ich telefony komórkowe, a także poprzez adresy MAC (kontrola dostępu do medium transmisyjnego)[35], które są unikalnym identyfikatorem przypisanym do konkretnego urządzenia, przypominającym numer seryjny. Firma Euclid przyznała, że od momentu rozpoczęcia działalności w 2011 roku, naliczyła 50 mln urządzeń w sklepach swoich kontrahentów.

Smith wyjaśnił, że zbierając wyłącznie anonimowe informacje, Euclid respektuje „prawo do prywatności konsumentów”. Jednak prawda jest taka, że dane o lokalizacji przekazują najwięcej informacji o konkretnej osobie[36]. W 2013 roku, badacze z MIT i belgijskiego Université Catholique de Louvain przez 15 miesięcy studiowali dane o położeniu ponad 1,5 miliona osób. Odkryli, że w przypadku 95 proc. uczestników badania, do ich zidentyfikowania wystarczyły cztery elementy związane z miejscem ich pobytu w danym momencie. „Ślady przemieszczania się konkretnej osoby są absolutnie unikalne”, przyznali badacze. „Informacje o mobilności są jednymi z najbardziej wrażliwych danych, które obecnie są zbierane”, dodali.

Położenie można przewidywać. Badacze z Microsoftu odkryli[37], że dane dotyczące miejsca pobytu danej osoby można wykorzystywać do precyzyjnego prognozowania jej przyszłej lokalizacji. Ustalili to, korzystając z informacji o lokalizacji przekazywanych przez trzystu wolontariuszy. Najłatwiej było przewidywać lokalizację danej osoby w środy, najtrudniej – w weekendy. „Podczas gdy wasze położenie w odległej przyszłości jest zazwyczaj niezależne od ostatniego miejsca pobytu, to z dużym prawdopodobieństwem można przewidzieć waszą lokalizację w nadchodzącym tygodniu".

Zdaje się, że w przypadku tego typu danych nie można mówić o anonimowości. Firmy potrafią bowiem na ich podstawie ustalić nie tylko to, gdzie znajdujemy się obecnie, lecz również, gdzie będziemy przebywać za tydzień.

* * *

Aby ograniczyć możliwość śledzenia mojej lokalizacji, wyłączyłam Wi-Fi w obydwu telefonach i obiecałam sobie, że nigdy więcej go nie uruchomię. Wyłączyłam także usługi lokalizacji w urządzeniach. Zmieniłam nawet nazwę mojego domowego routera, dodając do niej rozszerzenie _nomap, aby wykreślono mnie z bazy danych Google's Location Service[38].

Zidentyfikowałam 58 firm, które zdawały się działać w branży usług lokalizacji, od reklamodawców przez podmioty śledzące telefony za pośrednictwem śmietników po dostawców internetu. Spośród nich jedynie 11 przewidywało możliwość wycofania zgody na przetwarzanie danych osobowych użytkownika. Skwapliwie z tego skorzystałam.

Nadal byłam daleka od wydostania się z tego dragnetu. Zdecydowałam się częściej wyłączać telefon, by nie można było stale śledzić mojej lokalizacji. Rozważałam przełączanie się na tryb samolotowy, jednak nie chciałam stale grzebać w ustawieniach.

Uznałam, że wygodniej będzie umieścić telefon w torbie blokującej sygnał. Takie torby nazywane są „klatkami Faradaya"[39], od nazwiska angielskiego naukowca Michaela Faradaya, który odkrył, że pokrycie pomieszczenia warstwą metalu blokuje promieniowanie elektromagnetyczne. Klatki Faradaya stosowane są w służbie zdrowia, wojsku i innych sektorach, w których ludzie chcą zapobiec interferencji

elektromagnetycznej między urządzeniami[40].

Kiedy powiedziałam byłemu agentowi CIA, Johnowi Strauchsowi, że chciałabym mieć klatkę Faradaya dla mojego telefonu, zaśmiał się i zasugerował mi prostą sztuczkę, którą w razie konieczności mogłam wykonać w dowolnej chwili: „Możesz po prostu owinąć telefon folią aluminiową”[41].

Zadziałało. Obłożyłam folią telefon na kartę i starałam się na niego dodzwonić. Nie odpowiadał. Wrzuciłam więc owinięty telefon do torebki i wybrałam się do Nowego Jorku na spotkania.

Trzymałam urządzenie w torebce i odwijałam wyłącznie między spotkaniami, kiedy nikt nie patrzył. Łączenie się z siecią, pobieranie wiadomości, e-maili czy informacji o nieodebranych połączeniach, trwało kilka minut. Po wszystkim, zadowolona, ponownie zawijałam telefon i chowałam do torebki.

Pod koniec dnia folia była w kompletnym nieładzie: pognieciona i porwana w kilku miejscach. Ponowne zawinięcie telefonu stawało się coraz trudniejsze, bo starałam się łatać powstałe dziury. Kiedy kolega, Jeremy Singer-Vine, zobaczył mój wynalazek z folii aluminiowej, zaczął ironizować i zaproponował mi własną klatkę: „Mam torebkę Faradaya, z której nie korzystam. Chcesz?”.

Kilka dni później, Jeremy przyniósł mi piękną srebrną torebkę z zamknięciem Velcro, która nie przepuszczała sygnału. Mój telefon doskonale się w niej mieścił. Pokochałam ją.

Folia aluminiowa robiła ze mnie wariatkę. Torebka Faradaya czyniła mnie interesującą; wszyscy znajomi chcieli taką mieć.

* * *

Oczywiście byłam ciekawa, kto jest twórcą mojej torebki Faradaya. Jeremy przedstawił mnie Adamowi Harveyowi.

Umówiłam się z nim na kawę w centrum. Kościsty Adam powiedział mi, że połączeniem mody i działań o charakterze antyinwigilacyjnym zainteresował się podczas studiów magisterskich w Nowym Jorku w 2009 roku[42].

Jego pierwszym tak zwanym ubraniem maskującym była „kopertówka przeciwko paparazzi”. Jest to torba, która w odpowiedzi na błysk fleszy odbija białe światło, niszcząc zdjęcie. „Wierzę, że fotografowane osoby

również powinny móc odpowiedzieć na błysk fleszy", wyznał. Kopertówka nie cieszyła się powodzeniem, ale skłaniała do refleksji nad alternatywnymi sposobami ochrony prywatności w miejscach publicznych. W swojej pracy dyplomowej Harvey zaproponował fryzury oraz makijaż uniemożliwiające rozpoznanie danej osoby przez oprogramowanie służące identyfikacji twarzy. Jednak system nie był zbyt praktyczny: stylizacje wymagały noszenia włosów na twarzy albo malowania jej części na czarno.

Ostatecznie wpadł więc na pomysł stworzenia klatek Faradaya dla telefonów komórkowych. Początkowo próbował zaprojektować spodnie z kieszeniami poprzeplatanymi bawełnianymi i srebrnymi nićmi, które blokowałyby sygnał telefoniczny. Uznał jednak, że takiego projektu nie da się zrealizować. Zaczął więc pracować nad rękawem dla telefonu komórkowego, który nazwał OFF-Kieszeń.

Wyznał, że klatka, którą trzymam w ręku, była prototypem. Zmniejszała siłę sygnału z nadajnika o 80 decybeli[43]. „Aby być w pełni zabezpieczonym, sygnał musi spaść o ponad 95 decybeli". Nowa torebka, którą miał zamiar wprowadzić, obniżała siłę sygnału o 100 decybeli. „Wierzę, że prywatność nie będzie nam w pełni dana jako prawo. Musi zostać skomercjalizowana, aby ludzie zaczęli się jej domagać, płacąc za nią", powiedział mi.

* * *

Choć wydałam pieniądze, nie osiągnęłam zbyt wiele. Zarówno mój maskujący numer telefonu jak i „palnik" były raczej zabawkami niż prawdziwą tarczą, chroniącą informacje o mojej lokalizacji czy sieci kontaktów.

Umieszczanie telefonu w klatce Faradaya działało. Jednak oznaczało praktycznie to samo, co pozostawienie telefonu w domu. Nie byłam bowiem dostępna, dopóki go z niej nie wyjęłam.

Doświadczenia z prywatnością telefonów komórkowych były jak dotąd moją największą porażką.

11

PROCEDURA WYJŚCIA

Kiedy powiedziałam bratu, że zamierzam zlikwidować swój profil na LinkedIn, powiedział, że jestem szalona. „Stracisz w ten sposób możliwość znalezienia kolejnej pracy".

Nie mogłam pozwolić sobie na przepuszczenie jakiejś oferty. Moja branża – prasa – znalazła się w zasadzie na równi pochyłej. Nawet jeśli nie potrzebowałam propozycji pracy w danej chwili, było jasne, że w nieodległej przyszłości będzie to na wagę złota.

Z drugiej strony nie mogłam znaleźć usprawiedliwienia dla dalszego utrzymywania profilu na LinkedIn, biorąc pod uwagę to, jak bardzo eksponował on moją sieć kontaktów. Ustawienia prywatności portalu pozwalały na to, by ukryć moje „połączenia" z innymi, jednak zgodne z jego polityką prywatności „ludzie mogą zawsze widzieć wspólne kontakty z danym użytkownikiem".

Oznacza to, że jeśli macie z kimś wspólny kontakt na LinkedIn, obydwojgu z nas będzie wyświetlać się ta znajomość. Może wydawać się to nieszkodliwe, ale w istocie rzeczy nie różni się bardzo od bazy danych o połączeniach, budowanej przez Agencję Bezpieczeństwa Krajowego (NSA). To potężny dragnet powiązań.

W polityce prywatności LinkedIn widnieje także inny niepokojący zapis[1]: „Nie udostępniamy ani nie sprzedajemy danych osobowych, których nie umieściliście na LinkedIn". Zgaduję więc, że przedmiotem handlu mogą być wszystkie wszystkie te dane, które umieściłam na swoim profilu. Portal twierdzi[2], że nie handluje danymi osobowymi, ale sprzedaje usługi umożliwiające rekruterom wyszukiwanie danych użytkowników i kontaktowanie się z nimi.

Co dostawałam w zamian za eksponowanie wszystkich tych informacji? Rzadko korzystałam z LinkedIn. Miałam 220 kontaktów, 27 nieprzeczytanych wiadomości oraz 570 oczekujących zaproszeń. Nawet gdyby rekruter spróbował skontaktować się ze mną tą drogą, prawdopodobnie nie zauważyłabym tego.

Kusiła mnie jednak wizja wykorzystania LinkedIn w bliżej nieokreślonej przyszłości: że pomoże mi znaleźć pracę, gdy będę tego potrzebować. Specjalista ekonomii behawioralnej Dan Ariely określił to „irracjonalną potrzebą pozostawienia sobie otwartych drzwi".

Ariely opisał doświadczenie, które przeprowadził. W ramach eksperymentu studenci grali w grę komputerową, w której pokazywano im troje drzwi – czerwone, niebieskie i zielone. Każde prowadziły do wirtualnego pokoju, w którym, klikając myszką, gracze mogli zarobić określoną sumę pieniędzy. Celem pierwszego etapu gry było zarobienie jak największej kwoty przy określonej liczbie kliknięć.

Kiedy rozgrywka się rozpoczęła, szybko stało się jasne, że gracze, którzy wybrali jeden pokój i w nim pozostali, osiągali najlepsze wyniki. Jednak nawet kiedy zostało to już wyjaśnione z ekonomicznego punktu widzenia, gracze w dalszym ciągu woleli pozostawić sobie wszystkie drzwi otwarte. „Nie mogli znieść widoku zamkniętych drzwi[3]. Cały czas towarzyszyło im irracjonalne podniecenie myślą, że pozostawiają sobie opcje do wyboru"[4].

Problem polega na tym, że ludzie nie znoszą doświadczać straty, nawet jeśli dotyczy rzeczy mało istotnych. Doskonale opisywało to moje odczucia względem opuszczania LinkedIn. Na kilka miesięcy stało się to moją obsesją. Skontaktowałam się z dwoma ekspertami w dziedzinie pozycjonowania w wyszukiwarce internetowej[5], by dowiedzieć się, czy moja rezygnacja z portalu rzeczywiście utrudni innym możliwość odnalezienia mnie w internecie. (Nie utrudni). O tym, czy powinnam „wyciągnąć wtyczkę" rozmawiałam też z przyjaciółmi i rodziną.

Wszystko to dotyczyło strony, na której nie logowałam się od niemal dwóch lat. Strony, której hasła zostały już zhakowane, a system zabezpieczeń obnażony[6]. Strony, która dosłownie zalewała mnie e-mailami. Strony, która nie była mi wcale potrzebna do opisania zawodowych osiągnięć, ponieważ zamieściłam już swój pełny życiorys na własnej witrynie internetowej. Oto czym jest irracjonalny lęk przed stratą.

W końcu podjęłam decyzję i zamknęłam konto. LinkedIn poinformował

mnie, że po dokonaniu przeze mnie tego wyboru, w ciągu 30 dni przeprowadzi depersonalizację wszystkich wpisów związanych z moim kontem[7].

W kulturze, w której ludzie oceniają innych w tym samym stopniu na podstawie ich cyfrowych śladów, co dającej się zaobserwować w rzeczywistości osobowości, usunięcie swoich danych z sieci stanowiło akt odwagi. Teraz musiałam zwyczajnie liczyć na to, że przyszli pracodawcy znajdą mnie w inny sposób.

* * *

Wycofanie się z rynku danych osobowych to eksperyment z zaufaniem.

W świecie cyfrowym profile na stronach takich jak LinkedIn czy Facebook, pozwalają budować zaufanie pomiędzy ludźmi, którzy nigdy nie poznali się na żywo. Siłę sieci społecznościowych stanowi fakt, że wasze „kontakty" lub „znajomi" służą za potwierdzenie waszej wiarygodności. „Publiczne okazanie sieci kontaktów stanowi bezwzględnie weryfikację tożsamości", napisali w 2004 roku w swojej pracy badawczej o mediach społecznościowych Judith Donath i Danah Boyd[8].

Łatwiej jest potwierdzić czyjąś wiarygodność, kiedy spotyka się go na żywo. Naukowcy odkryli, że ludzie dokonują zaskakująco trafnych ocen innych w ciągu zaledwie trzydziestu sekund od ich poznania[9]. Dodatkowy czas spędzony z nimi zwykle nie poprawia już wyniku. W sieci ludzie mają do dyspozycji mniej narzędzi do oceny wiarygodności. Zdjęcia zamieszczane w internecie notorycznie wprowadzają w błąd[10], daty urodzenia mogą być nieprawdziwe, zaś e-maile wysyłane przez złodziei mogą wyglądać, jakby wysyłał je wasz bank.

Donath, która jest członkiem Berkman Center for Internet and Society na Uniwersytecie Harvarda, przeprowadziła fascynujące badania[11], porównując aspekty zaufania w sieci do wyzwań, z jakimi zmagają się zwierzęta, próbując rozróżnić prawdziwe i zwodnicze sygnały, które odbierają. Weźmy przykład świetlika z rodzaju Photuris, który imituje zachowanie samicy świetlika z rodzaju Photinus[12]. Niczym *femme fatale* uwodzi on samca świetlika z rodzaju Photinus, atakuje go i na końcu zjada. To przykład zwodniczego sygnału.

Z drugiej strony, przyjrzyjmy się wielkim rogom jelenia. Zwierzę nie jest w stanie utrzymać masywnego poroża, jeśli samo nie jest duże i silne.

„Zarówno potencjalni rywale, jak i partnerki, nie muszą bezpośrednio sprawdzać siły jelenia; wystarczy, że spojrzą na wielkość jego rogów", pisze Donath[13]. To przykład prawdziwego sygnału.

Donath twierdzi, że kontakty w sieci cyfrowej postrzegane są jako prawdziwe sygnały. Jeśli nieznana mi osoba jest przyjacielem mojego przyjaciela, to być może zasługuje na trochę mojego zaufania[14]. Jednocześnie presja jaka wiąże się z tworzeniem tożsamości w sieci wywołuje napięcie pomiędzy „prywatnością a wiarygodnością"[15]. Upubliczniony rejestr zachowań danej osoby bywa pomocny w budowaniu jej wiarygodności. Badaczka twierdzi jednak, że „jeśli wszystko musi dziać się pod prawdziwym nazwiskiem, może to studzić pewne odruchy albo czynić ludzi bardzo podatnymi na atak".

Donath pracuje nad sposobami tworzenia systemów uwiarygadniających pseudonimy. „Jeśli zamierzam ocenić jakość dezodorantu, nie potrzebuję ujawniać wszystkim w sieci mojego prawdziwego nazwiska. Pseudonimy stanowią klucz do zachowania prywatności w internecie".

W hołdzie dla Donath stworzyłam na LinkedIn profil pod swoim internetowym pseudonimem: Ida Tarbell. Ida nie ma żadnych „kontaktów", ale dzięki niej mogę logować się do portalu i przyglądać temu, co się tam dzieje. Łagodzi to jednocześnie moje irracjonalne poczucie straty po opuszczeniu LinkedIn.

* * *

W trakcie przygotowywania się do opuszczenia Facebooka, zasięgnęłam rady u pewnej świeżo upieczonej absolwentki, Gaebrielli Todesco.

Usunęła ona swoje konto z Facebooka podczas przerwy bożonarodzeniowej w czasie ostatniego roku studiów na Politechnice Kalifornijskiej w San Luis Obispo[16]. Pragnęła zostać nauczycielką w liceum i nie chciała, by przyszły pracodawca mógł zobaczyć zdjęcia obrazujące jej studenckie życie. „Istnieją fotografie, zwłaszcza te z czerwonymi kubeczkami[*17], które mogą narazić mnie na duże problemy. Przestraszyłam się tego, więc wszystkie usunęłam."

Związek Gaeby z Facebookiem był skomplikowany. Przez pierwszy rok uczelnianego życia wraz z przyjaciółmi nieustannie logowała się do portalu i umieszczała na nim zdjęcia z imprez, na których wszyscy trzymają

czerwone kubeczki.

Utknąwszy wraz z trzema współlokatorkami w akademiku, bez samochodu, popadła w „dziwne uzależnienie" od Facebooka. „Nie było nic innego do roboty poza wchodzeniem na Facebooka, wrzucaniem zdjęć lub śledzeniem ludzi"[17].

Niczym prawdziwy nałogowiec, Gaeby wielokrotnie próbowała skończyć z Facebookiem. Przez pierwsze trzy lata studiów porzucała Facebook na czas Wielkiego Postu. Gdy miała problemy ze swoim chłopakiem, odcinała się od portalu na całe tygodnie. „Zmień mi hasło, a kiedy postanowię, że chcę wrócić do sieci, po prostu mi je podasz", Gaeby instruowała przyjaciółkę, chcąc skończyć z Facebookiem z dnia na dzień.

Dziewczyna znała się na ustawieniach prywatności Facebooka i nigdy nie pozwoliła, by jej profil stał się całkowicie otwarty. Ograniczyła dostęp do zdjęć i „tablicy". Gdy miała rozstać się z chłopakiem, usuwała informację „status związku", co czyniło wydarzenie mniej publicznym, gdy faktycznie do niego dochodziło[18]. Usuwała także albumy i znaczniki ze zdjęć, których nie chciała pokazywać znajomym.

Nie była jednak przekonana, że to wystarczy. Jesienią ostatniego roku studiów, planując już karierę pedagoga, zaczęła cenzurować własne posty[19]. Poprosiła współlokatorki, by pytały ją o zgodę przed udostępnieniem wspólnych zdjęć na Facebooku. „Jesteśmy w tym razem. Stanowimy dobry zespół".

Do grudnia zrozumiała, że łatwiej będzie opuścić Facebooka niż skutecznie go kontrolować. Po tym jak przeczytała artykuł o nauczycielce, która straciła pracę z powodu zdjęcia zamieszczonego na Facebooku, postanowiła na stałe z niego zrezygnować.

24 grudnia 2010 roku ściągnęła na twardy dysk wszystkie swoje zdjęcia, po czym usunęła konto. Przez chwilę brakowało jej Facebooka. „Na początku czułam, że chciałabym w jakimś zakresie wrócić". Wkrótce jednak zaczęła doceniać czas, który odzyskała, gdy przestała co chwila sprawdzać Facebooka.

Kiedy spotkałam się z nią ponownie rok później, pracowała już w wymarzonym zawodzie i była zadowolona, że porzuciła portal. Cieszyła się, że jej uczniowie nie mogą jej tam znaleźć.

Oczywiście momentami brakowało jej Facebooka. O pogrzebie kolegi z liceum, który zmarł nagle, dowiedziała się już po fakcie. „Zdałam sobie

sprawę, że gdybym była na Facebooku, z pewnością wiedziałabym, kiedy odbędzie się ceremonia. Czułam się wyjęta poza nawias”[20].

Z drugiej strony było coś intrygującego w tym, że nie ma ona konta na Facebooku. „To czyni mnie tajemniczą i wyjątkową”, mówiła.

* * *

Kiedy dołączałam do Facebooka 26 czerwca 2006 roku, posiadanie konta oznaczało, że jest się powiązanym z elitarnym uniwersytetem. W owym czasie jego użytkownikiem można było zostać pod warunkiem, że posiadało się adres e-mail takiej uczelni lub jednej z niewielu szkół średnich. Właściwie założyłam sobie skrzynkę pocztową jako absolwentka mojej uczelni tylko po to, żeby dołączyć do Facebooka.

Moja motywacja była natury dziennikarskiej: zbierałam informacje do książki na temat sieci społecznościowej MySpace i chciałam zrozumieć rynek serwisów społecznościowych. Gdy jednak trafiłam na nauczyciela matematyki, który był dla mnie wielką inspiracją w liceum, czy dziewczynę, która ukradła mi chłopaka na studiach, sprawiło mi to wielką frajdę. Podobało mi się, że mogę sprawdzić, co słychać u dziennikarza z Pakistanu, który w czasie stażu odwiedził kiedyś moje biuro.

Facebook wielokrotnie naruszał jednak zaufanie użytkowników. Straciłam już rachubę, ile to razy firma zmieniała swoją politykę prywatności, zmuszając mnie do zagłębiania się w ustawienia w celu odzyskania kontroli nad własnymi danymi. Warto przyjrzeć się chaosowi, w jakim znajduje się prywatność na Facebooku. Łatwo wówczas zrozumieć, że firma postrzega użytkowników bardziej jako towar na sprzedaż niż klientów. Stanowisko portalu jest poniekąd zrozumiałe – użytkownicy nie płacą przecież za usługę. Z mojego punktu widzenia nie czyni go to jednak bardziej atrakcyjnym.

W 2007 roku Facebook uruchomił usługę o nazwie Beacon, która miała pomagać ludziom „dzielić się” ze znajomymi informacjami o dokonanych w sieci zakupach. Gdy Sean Lane kupił na Overstock.com pierścionek z diamentem, który miał być bożonarodzeniową niespodzianką dla jego żony, z zaskoczeniem odkrył, że Facebook automatycznie poinformował o tym fakcie jego 720 znajomych, włączając w to małżonkę[21]. W 2009 roku portal zgodził się zapłacić 9,5 mln dolarów odszkodowania[22] w ramach ugody w związku ze złożonym przeciw niemu pozwem

zbiorowym. Jednocześnie wycofał się z usługi Beacon.

Zamiast jednak porzucić pomysł zamieniania użytkowników w darmowe reklamy produktów, Facebook powrócił do niego w 2011 roku, tym razem pod postacią produktu o nazwie Sponsored Stories[23]. Pozwalał on reklamodawcom nabywać prawa do postów użytkowników i wyświetlać je ponownie, przed ich znajomymi, w charakterze reklamy. Po kolejny pozwie zbiorowym, w 2013 roku Facebook zgodził się zapłacić 20 mln dolarów w ramach ugody[24]. Znowu jednak, zamiast odejść od tego rozwiązania, Facebook zmienił tylko język polityki prywatności[25], wyraźnie zaznaczając, że ma prawo wykorzystywać zdjęcia i posty użytkowników w reklamach. Innymi słowy, Facebook toczył trwającą sześć lat batalię o to, by móc zamieniać konwersacje swoich użytkowników w reklamy na sprzedaż. (Google zdążyło w tym czasie dołączyć do batalii, uruchamiając podobny program o nazwie „rekomendacje społeczenościowe" [ang. *shared endorsements*], który zamienia recenzje, oceny i komentarze użytkowników w reklamy)[26].

Przełomowy moment w moich relacjach z Facebookiem nastąpił w grudniu 2009 roku, kiedy to portal wprowadził nagle do polityki prywatności zmiany[27], polegające m.in. na upublicznieniu listy znajomych użytkownika. Wcześniej lista była niedostępna. Jako dziennikarka mam obowiązek chronić moje źródła informacji. Zaś jako istota ludzka wolę, by nie towarzyszyła mi skryta w cieniu widownia, gdy wchodzę w interakcję ze znajomymi.

Wściekła, napisałam felieton w „Wall Street Journal" ogłaszając[28], że Facebook sprzeniewierzył poufność przyjaźni, wobec czego zaczynam traktować go jako otwarte forum, takie jak Twitter. Całkowicie otworzyłam swój profil – zaczęłam przyjmować wszystkie zaproszenia do grona znajomych, nawet te od naprawdę odrażających osobników, a także usunęłam z niego wszelkie osobiste szczegóły. (Facebook zgodził się później z zarzutami stawianymi przez Federalną Komisję Handlu, że działa nieuczciwe i wprowadza użytkowników w błąd. Do ugody doszło jednak dopiero po dwóch latach od wprowadzenia zmian – zbyt późno, żeby robiło to dla mnie różnicę)[29].

Moje podejście do Facebooka należałoby określić mianem „prywatności poprzez niejasność". Miałam nadzieję, że mieszając prawdziwe dane (moich znajomych) z fałszywymi danymi (ludzi, których nie znałam), uda mi się ukryć rzeczywiste relacje, łączące mnie z innymi ludźmi.

Zdałam sobie jednak sprawę, że oczyszczam z pewnych treści wszystkie swoje posty, próbując trafiać do szalenie zróżnicowanego audytorium. Wśród ich odbiorców znajdowali się m.in. mój szef, źródła informacji, rodzice przyjaciół moich dzieci oraz nieznajomi, spotkani podczas wycieczki do Brazylii. Odkryłam, że coraz mniej mam do powiedzenia publiczności o takim składzie. W 2012 aktualizacje mojego statusu stały się całkowicie bezwartościowe. Zrozumiałam, że moje podejście całkowicie uniemożliwiało mi nawiązywanie na Facebooku prawdziwych relacji.

Niemniej, w dalszym ciągu nie byłam gotowa całkowicie opuścić portal. Chciałam zachować możliwość szukania ludzi i bycia wyszukiwaną.

Rozważałam uszczuplenie listy znajomych do takiej, która zawierałaby jedynie niewielką liczbę bliskich przyjaciół, ale zdałam sobie sprawę, że w rzeczywistości nie utrzymuję intensywnych kontaktów z przyjaciółmi i rodziną poprzez Facebook (korzystamy raczej z e-maili, SMS-ów i rozmawiamy przez telefon). Kiedy zaś myślałam o pozostawieniu szerszej listy znajomych, wracała kwestia nieustannej ekspozycji moich kontaktów.

Grzebiąc w ustawieniach prywatności Facebooka[30], dotarłam do informacji, że w dalszym ciągu nie można było całkowicie chronić listy swoich znajomych. Punkt regulaminu brzmiał: „Użytkownicy Facebooka, nawet jeśli nie widzą listy twoich znajomych, będą widzieć listę waszych wspólnych kontaktów".

Dla dziennikarki, nawet taki poziom jawności był zbyt duży. Wyobraźmy sobie, że pracownik niskiego szczebla pewnej instytucji nawiązuje znajomość z dziennikarzem, żeby podzielić się z nim informacjami. Jeśli rzecznik tej instytucji zauważy, że pracownik ten ma kontakt z dziennikarzem, może doprowadzić do zdemaskowania go jako źródła informacji. Był to argument przeciwko zawężeniu mojej listy kontaktów wyłącznie do tych osób, które faktycznie mogę znać.

Zastanawiałam się nad zwyczajnym usunięciem profilu. Jednocześnie w irracjonalny sposób obawiałam się, że w ten sposób utracę jakieś opcje.

Sądziłam, że będzie mi brakowało trzech rzeczy związanych z Facebookiem: (1) Możliwości wysyłania prywatnych wiadomości do ludzi, do których nie posiadałam aktualnych danych kontaktowych; (2) Bycia powiadamianą o tym, że zostałam oznaczona na jakimś zdjęciu lub w poście (zwykle zresztą od razu prosiłam o to, by mnie odznaczono); (3) Możliwości bycia „wyszukaną", jako dziennikarka czy autorka, przez ludzi, którzy cenili moje pisarstwo.

Zdecydowałam się więc na usunięcie wszystkich znajomych z Facebooka – a było to ponad sześćset osób – i pozostawienie sobie gołego profilu, służącego do prostych celów: wysyłania wiadomości, usuwania znaczników i bycia wyszukiwaną przez innych.

Usuwanie znajomych okazało się trudne. Paskudnie się czułam, usiłując usunąć z kontaktów kolegę z zajęć z rachunku różniczkowego czy cofnąć polubienie strony poświęconej zbliżającemu się spotkaniu absolwentów mojej szkoły średniej.

Skończyło się na tym, że musiałam zapłacić mojej asystentce Courtney Schley, by klikała za mnie opcję „usuń z grona znajomych".

Zajęło jej to siedem godzin. Gdy już było po wszystkim, poczułam jakby kamień spadł mi z serca.

* * *

Wkrótce odkryłam nieoczekiwaną zaletę życia bez Facebooka: ludzie nie oczekiwali już ode mnie, że wiem co dokładnie się u nich dzieje.

Byłam na obiedzie z przyjacielem, którego nie widziałam od prawie dziesięciu lat. Zaczął mówić o swoich wakacjach we Włoszech, zupełnie jakbym znała szczegóły, po czym nagle przerwał. „No tak, nie bawisz się w Facebooka". Cofnął się i zaczął od początku, który, swoją drogą, wiązał się z narodzinami jego dziecka – to wydarzenie także umknęło mojej uwadze.

Miałam w końcu wytłumaczenie tego, dlaczego nie jestem na bieżąco z aktualizacjami statusów znajomych, co przynosiło mi wielką ulgę. Gdy dołączyłam do portalu, sądziłam, że strumień informacji buduje pewien rodzaj zażyłości w relacjach z dalszymi znajomymi. Zagłębiłam się w temat, odkryłam jednak, że jest to tylko wrażenie, które może wprowadzać w błąd.

Poczułam to na własnej skórze podczas służbowego wyjazdu do Chicago w 2009 roku, gdy spotkałam się ze znajomym ze studiów[31].

Nie widziałam go siedemnaście lat, lecz myślałam, że jestem na bieżąco z jego życiem, dzięki statusom, które aktualizował na Facebooku i Twitterze. Wiedziałam, że niedawno stracił pracę i przeniósł się do nowego mieszkania. Znałam nawet jego zmagania związanie z instalacją łącza DSL w nowym lokum. Kiedy więc spotkaliśmy się oko w oko, nie pytałam go „Jak się masz?". Zamiast tego przyjęłam już pewien

stopień zażyłości i zagaiłam: „Jak idzie Ci poszukiwanie pracy?”

Odbyliśmy cudowną rozmowę, ale po jej zakończeniu czułam, że czegoś w niej brakowało. Zadzwoniłam więc do niego i zapytałam o to, o co nie udało mi zagadnąć podczas spotkania: „Co naprawdę u ciebie słychać?”

Okazało się, że było mu ciężej niż zakładałam. Gdy stracił pracę, był właśnie w trakcie kupowania apartamentu. Miał w związku z tym problemy z uzyskaniem kredytu hipotecznego. Ponieważ zobowiązał się już opuścić dotychczasowe lokum, musiał na gwałt znaleźć nowe miejsce do życia. Przyznał, że jego statusy dotyczące tej sytuacji były „zawoalowane”, nie chciał bowiem obciążać ludzi zbyt dużą ilością informacji.

Poczułam się głupia i naiwna. Dałam się bowiem wprowadzić w stan obojętności przez cyfrową pogawędkę. Przyrzekłam sobie, że od tej pory będę zawsze pytała znajomych z sieci „co naprawdę u nich słychać”.

Biorąc pod uwagę, że nie miałam już znajomych na Facebooku, ryzyko, że dam się zwieść fałszywemu poczuciu zażyłości, stawało się coraz mniejsze.

* * *

Innego rodzaju eksperyment z zaufaniem stanowi usunięcie danych osobowych z baz handlowych. W tym przypadku chodzi o zaufanie, jakim darzy się mafijnego egzekutora. Przekazujecie haracz, ale nigdy nie wiecie, czy to załatwi sprawę.

Wielu brokerów danych wymagało ode mnie podania wrażliwych informacji, takich jak numer prawa jazdy czy ubezpieczenia społecznego, bym mogła wycofać zgodę na przetwarzanie danych. Jeden podmiot zażądał nawet ode mnie numeru karty kredytowej. W każdym przypadku musiałam kalkulować: czy można ufać, że dana strona nie nadużyje moich danych, czy też lepiej nie sprzeciwiać się wykorzystywaniu przez nią danych, które już zgromadziła i nie przekazywać jej niczego więcej?

Podczas mojego osobistego audytu stworzyłam listę 212 brokerów danych. Spośród nich wyłącznie 92 pozwalało na wycofanie zgody na przetwarzanie danych osobowych. Dwa podmioty żądały z tego tytułu opłaty – Mugshots.com chciał 399 dolarów za usunięcie wzmianki o mnie, zaś SearchBug.com oznajmił, że usunięcie informacji z jego „rejestrów premium” opartych na dostępnych publicznie danych kosztuje 27,95

dolarów. Postanowiłam je pominąć.

Zdecydowana większość, dokładnie 65 podmiotów, wymagała podania konkretnych danych osobowych przed rozpoczęciem procedury usuwania informacji. O numer dowodu osobistego, ubezpieczenia społecznego czy karty kredytowej prosiło 35 brokerów. Podania numeru telefonu żądało 10, podczas gdy 24 domagało się przesłania adresu domowego. Tyle samo brokerów żądało przesłania formularza rezygnacyjnego drogą mailową lub faksem.

Przytłoczona rozmiarem zadania, postanowiłam zwrócić się ku swojej naczelnej zasadzie „płacenia za jakość". Chciałam kupić sobie pomoc.

Przeciwko dużym brokerom danych, którzy sprzedają informacje między innymi wyszukiwarkom osób[32], postanowiłam wykorzystać usługę TrustedID Catalog Choice – firmy, która zaczynała od walki ze SPAM-em. Za 35 dolarów Catalog Choice obiecywała wyrwać mnie ze szponów 9 największych amerykańskich brokerów sprzedaży danych, takich jak Acxiom czy Experian.

W odniesieniu do wyszukiwarek osób [ang. *lookup sites*][33], wykupiłam za 209 dolarów dwuletni abonament usługi o nazwie DeleteMe, oferowanej przez Abine. To ten sam bostoński start-up, który stworzył wykorzystywane przeze mnie maskujące numery telefonów, adresy e-mail i karty kredytowe. Dzięki DeleteMe moje dane miały zostać wycofane z 17 największych wyszukiwarek osób, takich jak Intelius czy Spokeo.

Po paru tygodniach wydawało się, że moje dane w większości zniknęły z wyszukiwarek. Kiedy szukałam mojego nazwiska w Spokeo zauważyłam, że pojawiają się wyłącznie wyniki wskazujące na lokalizację w Idaho, Wyoming i Utah – stanach, w których nigdy nie mieszkałam. Na WhitePages.com nie było żadnych wyników dla hasła „Julia Angwin".

Jednak po dwóch miesiącach moje dane w dalszym ciągu wyświetlały się w największych wyszukiwarkach – Intelius[34], US Search i ZabaSearch. Zadzwoniłam do Jima Adlera, dyrektora ds. prywatności w Inteliusie, jednego z niewielu przedstawicieli firm brokerskich, którzy uczestniczyli w konferencjach poświęconych prywatności i odbierali telefony od jej obrońców. (W międzyczasie zdążył odejść z firmy i dołączyć do pewnego start-upu zajmującego się wielkimi zbiorami danych).

Zweryfikował informacje, które mu przekazałam i odkrył, że Intelius nie otrzymał od Abine mojego wniosku o zaprzestanie przetwarzania danych. Kiedy skontaktowałam się z Abine, firma stwierdziła, że niepowodzenie

w przesłaniu wniosku z wycofaniem zgody spowodowane było „błędem” w procesie[35].

Z pewną dozą podejrzliwości, sprawdziłam ponownie czy inne wnioski wysyłane za pośrednictwem Abine przyniosły skutek. Tak jak przypuszczałam, moje dane w dalszym ciągu wyświetlały się na USA People Search – stronie, z której miały zostać usunięte. Okazało się, że portal ten nie przyjmuje wniosków od pośredników, wyłącznie od osoby zainteresowanej[36].

Prawniczka Abine, Sarah Downey, przeprosiła mnie i zwróciła pieniądze. Powiedziała jednak, że brokerzy danych celowo utrudniają procedurę wycofywania zgody na przetwarzanie danych. „To jeden z powodów, dla których zawsze tak mocno zabiegałam o poprawki do ustaw, mające pomóc radzić sobie z działalnością brokerów sprzedaży danych osobowych: to problem prawny, a firmy takie jak nasza, nie mogą wychodzić poza prawo, próbując pomagać klientom. Robimy co możemy, ale to nie zawsze wystarcza”[37].

Dużo trudniej było zweryfikować, czy wnioski z wycofaniem zgody na przetwarzanie danych osobowych rozesłał Catalog Choice. Brokerzy sprzedaży baz danych nie upubliczniają informacji, które są w ich posiadaniu. Skontaktowałam się więc z każdym z osobna, pytając o to, czy moje dane zostały usunięte z ich rejestrów.

Rezultaty okazały się zatrważające. Catalog Choice nie udało się skutecznie złożyć w moim imieniu ponad połowy wniosków. Nie powiodło się ich dostarczenie do LexisNexis i Datalogix. Firma wysłała wycofanie zgody na przetwarzanie moich danych do Epsilonu, ale zostało ono rozpatrzone wyłącznie w odniesieniu do jednej z dwóch baz danych. Wnioski trafiły także do I-Behavior oraz KBM Group, które poinformowały mnie, że nie uznają przekazanych przez pośrednika – Catalog Choice.

Rzeczniczka firmy wyjaśniła mi, że kłopoty z LexisNexis oraz Datalogix spowodowane były „problemem technicznym”, który wystąpił w dniu, w którym usiłowano złożyć wnioski[38]. Kiedy poprosiłam o zwrot pieniędzy, zgodziła się.

Dostałam więc cenną lekcję: nie zawsze można kupić prywatność. Stanowi ona dobro o charakterze ulotnym, trudne do zweryfikowania. Niestety, firmom zbyt łatwo przychodzi eksploatowanie tej jej właściwości dla zysku.

* * *

Próba załatwienia sprawy za pieniądze nie przyniosła rezultatów. W dalszym ciągu miałam do złożenia ponad 50 wniosków.

Postanowiłam pominąć podejrzanie wyglądające strony, które żądały podania bardzo osobistych informacji w zamian za usunięcie danych z ich rejestrów. Nie czułabym się komfortowo, podając moje nazwisko, adres e-mail i numer telefonu serwisowi FreePhoneTracer.com, umożliwiającemu „wsteczne wyszukiwanie i lokalizację dowolnego numeru telefonu", by wycofać moje dane z jego bazy[39].

Nie zdecydowałabym się też na podanie numeru karty kredytowej MyLife.com, który sugerował, że jest to niezbędne do „odzyskania przeze mnie mojego profilu". Na stronie widniał zapis: „Po udanej weryfikacji posiadacza profilu, w możliwie szybkim terminie podejmiemy próbę realizacji wniosku o ograniczenie lub wycofanie zgody na przetwarzanie danych"[40].

W pozostałych przypadkach karnie przesłałam numer prawa jazdy i wypełniłam internetowe formularze. Spędziłam prawie sześćdziesiąt godzin, zgłaszając wnioski i sprawdzając, czy moje dane zostały faktycznie usunięte. Courtney, moja analityczka, spędziła kolejnych sześćdziesiąt godzin na tworzeniu arkusza zawierającego ponad dwustu brokerów danych.

Jednak jedna strona – PeopleSmart.com – zbiła mnie z tropu. Myślałam, że z niej zrezygnowałam, jednak Courtney powiedziała, że tego nie zrobiłam. Byłam wtedy w Nowym Jorku, podczas gdy ona przebywała w Japonii, gdzie pracowała przez parę miesięcy, gdy jej mąż był na stypendium.

Wymieniałyśmy się nieustannie e-mailami i w końcu dotarło do nas, że na ekranach naszych komputerów widziałyśmy zupełnie co innego. W Japonii Courtney mogła wyświetlić moje dane na PeopleSmart. W Nowym Jorku informacje o mnie wyglądały na zablokowane. Wydawać się mogło, że portal usunął mnie z wyników wyszukiwań w Stanach Zjednoczonych, ale udostępniał dane o mnie w wyszukiwaniach międzynarodowych. „To jest TAKIE podstępne!", napisała Courtney w e-mailu.

Zdawało się to wyjątkowo nieuczciwe w przypadku firmy, która twierdziła, że działa w obszarze „innowacji prywatności"[41]. W zakładce

„Co nas wyróżnia” na swojej stronie internetowej PeopleSmart wymieniało „łatwość i swobodę wycofania danych”[42]. To miało czynić ją inną od pozostałych wyszukiwarek osób, spośród których „nie wszystkie w pełni usuwały dane osobowe, nawet na wyraźne żądanie zainteresowanego”.

Zabawa w internetowego detektywa doprowadziła mnie do zaskakującej konstatacji, że firma ta była tak naprawdę popularnym start-upem z Doliny Krzemowej o nazwie Inflection. Informacje na stronie www opisują go jako „start-up działający w obszarze wielkich zbiorów danych”, który chwali się oferowaniem pracownikom premii w postaci rejsów jachtem, medytacji, jogi czy wycieczek w góry. Wysłałam do nich pełnego jadu maila, domagając się wyjaśnień.

Trzeba przyznać, że prezes firmy, Matthew Monahan, odpisał niemal od razu i obiecał przyjrzeć się sprawie[43]. Dzień później przesłał mi szczegółową odpowiedź[44], tłumacząc, że firma korzysta z innych źródeł danych dla międzynarodowej wersji serwisu i dlatego informacje o mnie nie zostały stamtąd usunięte. „Nie mieliśmy złych zamiarów. Nie zarabiamy na zagranicznych użytkownikach. Nie przewidujemy nawet opcji międzynarodowych płatności. Wyszła z tego komedia omyłek”[45].

Mohanan powiedział mi, że założył Inflection wraz z młodszym bratem Brianem w 2006 roku, nie mając dokładnego wyobrażenia o tym, w co się przeistoczy. Matthew rzucił studia na Uniwersytecie Południowej Kalifornii, żeby założyć start-up sprzedający e-booki ze wskazówkami... jak dostać się na studia. (Było to jeszcze zanim nastały czasy książek elektronicznych, więc chodziło o zwykłe PDF-y do pobierania). Brian studiował na Harvardzie. Ich pomysły były co nieco mgliste. „Zdecydowaliśmy się przenieść do Kalifornii, tuż obok Facebooka i spróbować sił w tej nieprzynoszącej wielkich zwrotów branży”, powiedział mi Matthew. Stwierdzili, że ich pierwszym celem powinno być ucyfrowienie publicznych rejestrów.

Pieniądze zarobione przez Matthew na sprzedaży e-bookowego biznesu zainwestowali w opracowanie technologii, pozwalającej na digitalizację rejestrów sądowych i administracyjnych. Ich pierwszym produktem był CallerID – po wprowadzeniu do wyszukiwarki numeru telefonu, można było odnaleźć jego właściciela. „Nie był to szczyt finezji”, wspomina Matthew. Tuż po uruchomieniu usługi, tzw. wsteczne wyszukiwanie numerów telefonów poddano publicznej krytyce. W 2008 roku bracia

uruchomili więc podobny serwis, pozwalający odnaleźć numer telefonu danej osoby po podaniu jej nazwiska. Firma szczyciła się bazą 90 mln numerów telefonicznych[46]. Parę miesięcy później Intelius przestał świadczyć usługę, pod presją firmy Verizon i obrońców prywatności[47].

Bracia postanowili przestawić się na historyczne rejestry danych publicznych. W 2009 roku uruchomili GenealogyArchives.com, który później przeistoczył się w Archives.com, zapewniający dostęp do cyfrowych rejestrów z przeszłości. W 2012 roku ich przedsięwzięcie odkupił za 100 mln dolarów Ancestry.com[48].

Po tym nieoczekiwanym przypływie gotówki, bracia mogli przejść na emeryturę. Postanowili jednak zainteresować się usługami wyszukiwania osób. Przeorganizowali PeopleSmart.com, uruchomili stronę weryfikującą kandydatów do pracy GoodHire.com, a także zaczęli rozwijać nowy serwis, Identity.com, który miał pomagać ludziom zarządzać ich danymi osobowymi w sieci. „Nie czuję, że nasza praca dobiegła końca. Nie mógłbym teraz skupić się na czymkolwiek innym niż na poprawie naszych produktów”[49].

Matthew powiedział mi, że starali się uczynić procedurę wycofania zgody na przetwarzanie danych możliwie najprostszą. Na PeopleSmart wypełnia się elektroniczny formularz. Nie trzeba przy tym podawać numeru prawa jazdy, ani wysyłać wniosku pocztą. „Uważamy, że ten proces często utrudnia się celowo”.

Wspomniał także, że doznał rozczarowania, czytając e-mail ode mnie, informujący go o problemach z usunięciem danych. „Poświęciliśmy tyle czasu, żeby to działało”.

Problem stanowił według niego algorytm dopasowujący. Ich komputerom nie udało się połączyć „Julii Angwin”, która zrezygnowała z ich usług w Ameryce z „Julią Angwin”, której dane gromadzone były w drugiej bazie danych, do użytku międzynarodowego.

Jeden z powodów, dla których się to nie udało: „Nie poprosiliśmy cię o numer ubezpieczenia społecznego. Nie używamy go do łączenia zestawów danych. Musimy zatem korzystać z kombinacji innych elementów”. (Monahan powiedział mi potem, że proces usuwania danych został usprawniony, wobec czego błąd nie powinien się już pojawiać).

Oczywiście, mogło to być z ich strony niezamierzone, nie mogłam jednak oprzeć się wrażeniu, że na rynku danych osobowych takie błędy się opłacają. Jeśli usunę swoje dane ze wszystkich dostępnych baz, uczyni je

to jeszcze rzadszym aktywem. Tym samym staną się jeszcze cenniejsze dla tych, którzy chcą je wykorzystać.

* * *

Pod wszystkim, czułam, że więcej straciłam niż zyskałam w całym procesie wycofywania zgody na przetwarzanie moich danych. Doświadczyłam poczucia straty, kiedy zamykałam swoje konta. Martwiłam się, że odcięłam sobie możliwość znalezienia w przyszłości pracy. Ograniczyłam także swoją „wiarygodność". Trudniej było mnie teraz zweryfikować w gospodarce danych osobowych.

Mimo wszystkich strat, które poniosłam, nie zdołałam w pełni wycofać informacji o mnie z sieci. W dalszym ciągu znajdowały się w posiadaniu najgorszych graczy – tych, którzy uniemożliwiali mi zniknięcie z ich baz. Nawet zaś ci, którzy wyrazili na to zgodę, nie mówili wcale o usunięciu danych, a jedynie ich „zablokowaniu".

Spośród wszystkich dragnetów, z którymi miałam do czynienia, ten właśnie najbardziej wprowadzał w błąd, co do możliwości decydowania użytkowników o tym, czy chcą pozwolić na przetwarzanie ich danych, czy też sobie tego nie życzą.

12

KORYTARZ LUSTER

Kiedy Rayne Puertos zaczynała pracę w sklepie ze sprzętem komputerowym w Tampie na Florydzie[1], nie starała się ukrywać swojej orientacji seksualnej, ale nie chciała też rozmawiać o niej otwarcie z nowo poznanymi kolegami. Jej preferencje zostały obnażone z siłą huraganu, gdy zalogowała się na swoim koncie na Facebooku, na wspólnym komputerze w pokoju socjalnym. Jeden z kolegów zajrzał jej przez ramię i zapytał, dlaczego wszystkie reklamy wyświetlające się na jej stronie są reklamami adresowanymi do osób homoseksualnych.

Wydały ją, ku jej rozgoryczeniu, spersonalizowane reklamy Facebooka.

„Jestem otwarta, jeśli chodzi o kwestię mojej orientacji seksualnej. Ale do pracy nie przychodzę po to, by rozmawiać o moim prywatnym życiu", powiedziała mi. Po tym wydarzeniu, zaczęła wchodzić na swój profil wyłącznie z telefonu, już nie ze wspólnego komputera.

Rayne została wydana przez niewinny z pozoru dragnet: korytarz luster, który tworzą reklamodawcy, opierając się wyłącznie na przemiataniu danych osobowych w sieci.

* * *

Branża reklamy internetowej stworzyła jeden z najbardziej rozbudowanych dragnetów na świecie.

Większość stron internetowych pozwala firmom tworzącym śledzące reklamy na szpiegowanie odwiedzających je użytkowników i podążanie ich tropem w sieci. Jak wynika z raportu spółki Krux Digital, specjalizującej się w analizowaniu technologii cyfrowych umożliwiających

trackowanie, w 2013 roku aż 328 firm śledziło odwiedzających 50 najpopularniejszych stron internetowych[2]. Było to dwukrotnie więcej niż w 2011 roku, gdy liczbę śledzących internautów firm oszacowano na 167.

Informacje gromadzone przez branżę są niezwykle szczegółowe. Ashley Hayes-Beaty była zaszokowana[3], dowiedziawszy się, że firma tworząca śledzące reklamy, umieściła na jej komputerze plik zawierający kod: 4c812db292272995e5416a323e79bd37. Umożliwiał, bez jej wiedzy, na zidentyfikowanie jej jako dwudziestosześcioletniej mieszkanki Nashville w stanie Tennessee. Ponadto, firma stworzyła listę jej ulubionych filmów, na której znalazły się m.in. „50 Pierwszych Randek", „Narzeczona dla Księcia", czy „Zakochana Złośnica". Oburzyła się, gdy powiedziałam jej, co zawiera jej profil: „Cóż, chciałam wierzyć, że posiadam jeszcze jakiś sekret, ale najwidoczniej nie!". I dodała: „Stworzony przez nich profil jest zasadniczo prawdziwy".

Siedemnastoletnia Cate Reid nie wiedziała dlaczego wyświetlają jej się wyłącznie reklamy związane z odchudzaniem, dopóki moja koleżanka z „Wall Street Journal" nie pokazała jej, że sieć reklamowa na Yahoo! skategoryzowała ją jako kobietę w wieku między 13. a 18. rokiem życia, zainteresowaną odchudzaniem.

Natomiast Google właściwie zidentyfikował dziesiątki lajków dziesięcioletniej Jenny Maas[4], oddanych na zwierzęta, fotografię, „wirtualne światy" i atrakcje *online*, takie jak animowane grafiki. „Nie chcę, aby wszyscy wiedzieli co robię, itd.", powiedziała mojemu redakcyjnemu koledze Steve'owi Stecklowowi, kiedy pokazał jej, co wie o niej Google.

Firmy zajmujące się śledzeniem użytkowników w internecie twierdzą, że informacje, które uzyskują są anonimowe, a tym samym nieszkodliwe. Typowa odpowiedź: rzecznik Google odpowiada, że śledzenie dziewczynki było oparte na „anonimowej aktywności wyszukiwarki". I dodaje: „Nie wiemy czy korzysta z niej jeden czy wielu użytkowników, ani kim oni są".

Pojawia się jednak coraz więcej dowodów na to, że informacje o zachowaniu internautów mogą umożliwiać identyfikację osób. W 2006 roku dziennik „New York Times" przeczesał anonimową bazę wyszukiwań opublikowaną przez AOL i wskazał stojącą za nią osobę – sześćdziesięciodwuletnią kobietę o nazwisku Thelma Arnold[5]. W 2008 roku badacze z Uniwersytetu w Teksasie przejrzeli udostępnioną przez Netflix anonimową bazę wypożyczeń filmów. Odkryli, że „nieprzyjaciel,

który ma choćby niewielką wiedzą o danej osobie, może z łatwością zidentyfikować ją w bazie danych subskrybentów”[6].

Ponadto, wiele stron nieumyślnie dzieli się nazwiskami odwiedzających je osób z firmami tworzącymi śledzące reklamy. W 2012 roku mój zespół z „Wall Street Journal” zalogował się do prawie siedemdziesięciu popularnych serwisów i odkrył, że w jednym na cztery przypadki strona przekazywała jakiemuś obcemu podmiotowi prawdziwą nazwę użytkownika, adres e-mail i inne dane osobowe (takie jak nazwisko)[7]. Jeden z większych portali randkowych wysyłał nawet informacje dotyczące orientacji seksualnej i skłonności do używek.

Także opcje takie jak „Lubię to!” na Facebooku czy „Podaj dalej” na Twitterze umożliwiają identyfikację użytkowników po imieniu, nawet jeśli ci niczego nie klikają. W 2012 roku, mój redakcyjny zespół odkrył, że wśród tysiąca największych witryn internetowych, aż 75 proc. zawierało kod z portali społecznościowych, umożliwiający łączenie nazw użytkowników z ich aktywnością w sieci.

Oczywiście, firmy te twierdzą, że nawet spersonalizowane śledzenie jest anonimowe. „Oferujemy wam reklamy na podstawie danych o was, co nie oznacza, że można was zidentyfikować”, mówi Erin Egan, członek zarządu ds. prywatności Facebooka.

Jak widać, stąpamy po kruchym lodzie. Ale czy dla Rayne miało to jakieś znaczenie, że Facebook najpierw „określił” jej preferencje, a dopiero później ją wydał?

* * *

Korytarz luster, stworzony przez reklamodawców, wciąż jeszcze jest dość prostym narzędziem. Homoseksualiści widzą reklamy przeznaczone dla gejów. Ludzie zainteresowani żeglarstwem oglądają ogłoszenia z nim związane. Kiedy prowadziliśmy z mężem remont naszego domu i kupowałam przez internet wanny, przez miesiąc osaczały mnie reklamy wanien.

To wszystko wydaje się raczej niewinne, a przypadki ujawnienia jakichś danych są sporadyczne. Jednak profesor Ryan Calo z Uniwersytetu Waszyngtonu kreśli przerażającą wizję korytarza luster w przyszłości[8]. Odwołuje się do badania przeprowadzonego na Uniwersytecie Stanforda, z którego wyraźnie wynika, że nasza ocena danego polityka będzie dużo

bardziej pozytywna, jeśli jego zdjęcie delikatnie połączone zostanie z naszym własnym zdjęciem. Chodzi o taką zmianę w fotografii, która jest nie do wykrycia, ale powoduje, że odbiorca staje się bardziej otwarty na przekaz polityka.

„Okazuje się, że bardziej lubimy te osoby, które wyglądają podobnie do nas", twierdził Calo. „Teraz wyobraźmy sobie portale społecznościowe, które oferowałyby podobne usługi, umożliwiając reklamodawcom łączenie wizerunku ich rzeczników ze zdjęciami profilowymi użytkowników". Calo nie wie, czy ktokolwiek stosuje tę metodę. Jednak twierdzi, że czai się ona tuż za rogiem w świecie wszechobecnych, podążających za nami, reklam.

Skoro technolodzy żywienia potrafią opracować śmieciowe jedzenie, które zmusza nasze kubki smakowe do sięgania po więcej, a firmy z branży gier liczbowych potrafią produkować jednorękich bandytów zachęcających do coraz częstszego grania, to czemu marketingowcy nie mieliby zaprojektować wirtualnej obecności, manipulującej nami na nowe sposoby?

Mój zespół ujawnił także działania firm, które polegają na zmienianiu cen produktów i usług w zależności od lokalizacji użytkownika. Calo przewiduje, że już wkrótce firmy znajdą sposób na to, by dopasowywać ceny do stopnia podatności użytkownika na reklamę – na przykład podnosić je, gdy ten jest zmęczony po ciężkim dniu pracy.

Ludzie mogą być też manipulowani, by przekazywali o sobie więcej informacji, niżby chcieli. Firmy wykorzystają takie dane, by dowiedzieć się, w jaki sposób najlepiej dotrzeć do konkretnej osoby. W trakcie pewnego eksperymentu, badacze z Uniwersytetu Carnegie Mellon odkryli, że ludzie chętniej przekazywali dane o sobie, gdy obiecywano im iluzoryczną kontrolę nad nimi[9].

Calo twierdzi, że rynkowa manipulacja przede wszystkim „kieruje w stronę zysku"[10]. Marketingowcy z pewnością są gotowi użyć wszelkich środków, aby skłonić nas do sięgnięcia po droższe produkty lub do nieprzemyślanego zakupu. Mogą w tym celu wykorzystać informacje, które im zostawiamy: nasz cyfrowy ślad.

W grę wchodzą prawdziwe zyski. Benjamin Reed Shiller, profesor ekonomii z Uniwersytetu Brandeis, przeanalizował dane dużej grupy internautów i doszedł do wniosku, że Netflix mógłby zwiększyć swoje zyski o 1,4 proc., jeśli wprowadziłby spersonalizowane ceny oparte

na historii przeglądania stron[11]. Zauważył, że te dane pozwalają przewidywać gotowość użytkowników do płacenia dużo trafniej, niż standardowe dane demograficzne. „Sugeruje to, że dyskryminacja cenowa pierwszego stopnia może się przekształcić z koncepcji teoretycznej w praktyczną i bardzo się upowszechnić".

* * *

Chciałam zablokować opcję śledzenia reklam. Jednak najpierw musiałam przebrnąć przez wszystkie nieprawdziwe informacje dotyczące ich blokowania.

Niektórzy wierzą, że korzystając z opcji „incognito" w Google Chrome albo z „trybu prywatnego" w Internet Explorer nie będą śledzeni *online*. Nie jest to prawdą.

Tryb incognito jest zabezpieczeniem prywatności przed jednym tylko jej zagrożeniem[12] – osobą, z którą współużytkujecie komputer. Po zamknięciu sesji po prostu usuwa „ciasteczka", które zostały w jej trakcie aktywowane. Jednak, strony, które odwiedzamy w trybie incognito nadal zbierają o nas dane, to samo dotyczy elementów śledzących [ang. *trackers*] na tych stronach.

Mówiąc zupełnie szczerze, tryb incognito został stworzony w jednym celu: do przeglądania stron z pornografią. Usuwa „ciasteczka" [ang. *cookies*] ze stron porno, aby wasz małżonek nie dowiedział się o waszej praktyce. Jednak strony i reklamodawcy doskonale wiedzą, co oglądaliście.

Nie był to mój model zagrożenia. Musiałam więc szukać dalej. Kolejnym krokiem było przyjrzenie się możliwości wycofania się z rynku reklamy internetowej[13]. Wymagałoby to jednak z mojej strony zainstalowania na komputerze „ciasteczek", które sygnalizowałyby firmom reklamowym, że nie chcę być śledzona. Rozwiązanie wydawało się dość kontrowersyjne. Jak u Orwella: musiałam dać się śledzić, aby nie być śledzoną.

Nawet wówczas jednak miałabym szansę uwolnić się od zaledwie 96 firm, podczas gdy – według najświeższych badań – takich śledzących podmiotów było na rynku ok. 300[14]. Branża reklamowa twierdziła, że przedsiębiorstwa ujęte na liście odpowiadają za większość śledzących reklam w internecie. Mimo to, wolałam zdecydować się na kompleksową blokadę wszystkich firm, które gromadzą moje *dossier*. Uznałam więc,

że nie skorzystam z możliwości, którą w tym zakresie oferowała branża.

Następnie włączyłam opcję „nie śledź" w swojej wyszukiwarce. W ten sposób do firm wysyłany jest sygnał, że nie chcę być monitorowana. Był to jednak zaledwie gest polityczny, ponieważ branża nie poczuwa się do obowiązku zaprzestania śledzenia użytkowników, którzy włączyli tę opcję.

Ostatecznie, zdecydowałam się na skromniejszy krok. Pewnej nocy, kiedy dzieci już spały, usiadłam przy komputerze i zainstalowałam dwa najpopularniejsze rozszerzenia do mojej wyszukiwarki Firefox.

Pierwszy, Adblock Plus, blokował wyświetlanie reklam[15], przede wszystkim uniemożliwiając reklamodawcom umieszczanie na moim komputerze śledzących „ciasteczek". Jako że zawód dziennikarza, który wykonuję, opiera się w znacznym stopniu na przychodach z reklam, nie jestem zwolenniczką ich blokowania. Jednak zdecydowałam, że spróbuję, w imię obrony przed byciem obserwowaną.

Drugi, NoScript blokował zarówno kod komputerowy zwany JavaScript, jak i program Flash, przed automatycznym ładowaniem się na stronie bez mojej zgody[16]. JavaScript może być wykorzystywany do umieszczenia na komputerze użytkownika całej gamy technologii śledzących, w tym „ciasteczek". Pozwala nawet obserwować wasze ruchy myszką na stronie. Ma jednak wiele przydatnych zastosowań.

Natychmiast Firefox zaczął dławić się i zwolnił. Kiedy kliknęłam na stronie Apple, chcąc umówić spotkanie w Genius Bar, nic się nie wydarzyło. Musiałam ustanowić wyjątek w oprogramowaniu NoScript dla Apple, aby strona mogła wykorzystywać JavaScript.

Tak samo było ze stroną Amazon.com. Myślałam, że wszystko co chciałam zamówić jest niedostępne, szybko jednak zrozumiałam, że nie o to chodzi. Musiałam zezwolić na działanie JavaScript.

Po dwóch dniach, byłam gotowa zrezygnować. Odwiedziny dosłownie każdej strony wymagały ode mnie podjęcia szeregu decyzji, z których skryptów korzystać. Moja córka stała nade mną i śmiała się, podczas gdy ja próbowałam załadować daną witrynę i zarządzać wszystkimi pozwoleniami. Jakby tego było mało, Adblock wchodził w konflikt z zainstalowanym przeze mnie programem 1Password. Ostatecznie musiałam odinstalować Adblock, aby 1Password działał.

Zostałam jednak przy NoScript. W końcu, gdy zrozumiałam, o co chodzi, zaczęłam się martwić. Dlaczego sklep, w którym robiłam zakupy przez

internet, FreshDirect, chciał ładować skrypty pięciu innych firm, kiedy wybierałam produkty? Wydawałam we FreshDirect dużo pieniędzy, oczekiwałam więc, że nie będzie stwarzał jakiejś trzeciej stronie możliwości obserwowania mnie, gdy robię zakupy.

Oto, komu FreshDirect pozwalał mnie obserwować:

- Firma reklamy internetowej należąca do Google – Double-Click[17];
- AddThis[18], firma która szczyci się śledzeniem ponad 1,3 mld użytkowników miesięcznie;
- ConvergeTrack[19], która przedstawia się jako oferująca „jedną z najbardziej zaawansowanych technologii raportowania i śledzenia";
- Bazaarvoice[20], która rzekomo „łączy setki milionów konsumentów ze sobą nawzajem, a także z markami, które kupują";
- IBM Coremetrics[21], która oferuje klientom „generowane automatycznie, spersonalizowane rekomendacje produktów w oparciu o analizę bieżących i historycznych zwyczajów zakupowych".

To przepis na finansowe nadużycia. Można sobie wyobrazić, że niebawem IBM przeanalizuje moje zwyczaje i doradzi FreshDirect, by pobierała ode mnie więcej pieniędzy, gdy będę robić zakupy późnym wieczorem, gdy jestem zmęczona; albo że prędzej zaakceptuję wyższą cenę masła orzechowego niż steków.

Zapytałam FreshDirect o relacje z tymi firmami[22], ale rzeczniczka nie chciała odpowiedzieć na moje pytania. „Witaj Julia, nie weźmiemy udziału w tej rozmowie, ale cieszymy się, że się do nas odezwałaś", odpisała z fałszywą życzliwością.

Kiedy przeczytałam politykę prywatności FreshDirect[23] wcale nie poczułam się lepiej. Regulamin mówił: „Dzielimy się zagregowanymi, anonimowymi danymi demograficznymi z naszymi partnerami i reklamodawcami. Ten sposób przetwarzania danych uniemożliwia identyfikację konkretnych osób".

Jednak strona oferowała możliwość wycofania zgody na przetworzenia danych użytkownika. Wystarczyło wysłać w tym celu e-mail. Tak też zrobiłam.

To doświadczenie wyprowadziło mnie z równowagi. W prawdziwym

życiu supermarket nie sprasza przedstawicieli sześciu innych firm, by pokazać im kupujących. Dlaczego więc w cyfrowym świecie jest na to przyzwolenie?

* * *

Pewnym pocieszeniem może być fakt, że człowiek, który stworzył mechanizm śledzących reklam, czuje się źle z tym, że jego wynalazek jest wykorzystywany w taki sposób.

W 1995 roku, Daniel Jaye, absolwent Uniwersytetu Harvarda, szukał sposobu, by dorobić się na gorączce internetowej[24]. W tym czasie zajmował się przetwarzaniem danych w bazach funduszu inwestycyjnego Fidelity Investments. Było to równie odpowiedzialne, co żmudne zajęcie. Chciał robić coś ciekawszego. Dołączył więc do założycieli bostońskiego start-upu Engage Technologies, który starał się wprowadzać do internetu strategie marketingu bezpośredniego, poprzez tworzenie list potencjalnych nabywców produktów takich jak podręczniki.

Daniela interesowało, jak wskazać potencjalnych nabywców. Wątpił, by ludzie chcieli wypełniać internetowe formularze, by dzielić się swymi zainteresowaniami. „Bardzo szybko doszedłem do wniosku, że doskonałym źródłem informacji o preferencjach klientów będzie historia przeglądania stron".

Zaczął wykorzystywać proste pliki tekstowe, zwane „ciasteczkami" do identyfikacji komputerów osób, które przeglądały konkretne strony. Wcześniej, pliki „ciasteczek" były stosowane do zapamiętywania loginów i haseł użytkowników. On wpadł na pomysł, że „ciasteczka" mogą posłużyć także do gromadzenia informacji o zachowaniach internautów w sieci.

Tym, co było porywające w tej metodzie, była anonimowość. Internauta mógł być zidentyfikowany wyłącznie na podstawie numeru „ciasteczka" [ang. *cookie ID*], stanowiącego szereg cyfr, przypisanego do komputera. Dan uważał, że jego metoda stanowi udoskonalenie tradycyjnego marketingu bezpośredniego, polegającego na sprzedawaniu i kupowaniu list z danymi osobowymi.

Jednak nie był to jeszcze ten czas. Internet był zupełną nowością i nieliczni reklamodawcy, płacący za ogłoszenia, nie interesowali się ich precyzyjnym ukierunkowywaniem, ani anonimowym, ani jawnym.

W większości były to firmy technologiczne, które chciały wzbudzić szum wokół swojego wejścia na giełdę.

W tym okresie spółka Engage Technologies znalazła się w oku cyklonu na rynku dot-comów. Firma należała do konglomeratu internetowych spółek[25], złożonego z podmiotów takich jak AltaVista, Lycos i stron zakupowych – Shopping.com oraz Furniture.com. Jego powstanie było wynikiem szału zakupowego pewnego przedsiębiorcy, Davida Wetherella.

Jesienią 1999 roku, Wetherell pojawił się na okładce magazynu „BusinessWeek" jako „apostoł internetu". Jego konsorcjum, CMGI, symbolizowało *boom* na spółki internetowe. Wycena rynkowa tego podmiotu sięgała 10 mld dolarów, mimo że rocznie odnotowywał on straty rzędu 127 mln dolarów[26], a jego przychody sięgały zaledwie 176 milionów. W 2001 roku, bańka dot-comów na giełdzie pękła. Kwartalne straty CMGI wyniosły 1 mld dolarów, a cena akcji spadła do jednego dolara. Dan odszedł z firmy, która wkrótce upadła. Jednak idea wykorzystywania „ciasteczek" przetrwała.

W międzyczasie Dan uznał, że kolejną wielką ideą będzie prywatność[27]. W 2001 roku założył wyspecjalizowaną w tej dziedzinie firmę programistyczną, zwaną Permissus. Jego pomysł polegał na sprzedaży przedsiębiorstwom rozwiązań, umożliwiających śledzenie danych ich klientów, gdy ci poruszają się po ich systemach.

Jednak firmy nie miały ochoty zmieniać sposobu wykorzystywania przez nie danych. Po kilku latach biznes Dana padł, a on sam wrócił do korzeni – branży reklamy internetowej. Był rok 2007. Rynek firm internetowych wyłaniał się znowu, na zgliszczach dot-comów. Dan dołączył do start-upu TACODA (skrót od: „skoordynowane namierzanie danych"), którego celem było opracowanie podobnych profili internautów, jakie swego czasu zamierzała wykreować firma Engage. „Zaczęliśmy zastanawiać się nad targetowaniem behawioralnym, czyli zdolnością do wskazania, że np. dana osoba spędza 30 proc. swojego czasu na czytaniu wiadomości międzynarodowych, 20 proc. na oglądaniu gadżetów i 20 proc. na oglądaniu futbolu", powiedział mi.

By móc przyjrzeć się zachowaniu ludzi w internecie z lotu ptaka, TACODA musiała śledzić ich w wielu obszarach. Zaczęła więc płacić administratorom stron www za umieszczanie „ciasteczek" na komputerach odwiedzających ich użytkowników.

Oznaczało to istotną rynkową zmianę. Wcześniej strony śledziły

internautów wyłącznie w imieniu współpracujących z nimi reklamodawców. Teraz zaczęły sprzedawać dane odwiedzających praktycznie każdemu. Stało się to niezwykle popularne, ponieważ strony miały problem ze sprzedażą przestrzeni reklamowej, a TACODA oferowała szybkie pieniądze.

Wkrótce, śledzenie w internecie stało się intratnym biznesem[28]. W 2007 roku TACODA została sprzedana firmie AOL za 275 mln dolarów, Google zapłacił 3,1 mld dolarów za Double-Click[29], a Microsoft wydał 6 mld dolarów na zakup agencji reklamy internetowej aQuantative[30].

Rozprzestrzeniające się trackowanie uderzyło jednak w wydawców wielkich tytułów prasowych, takich jak „Wall Street Journal" czy „New York Times". Reklamodawcy nie musieli już ponosić zwiększonych kosztów docierania ze swoimi ogłoszeniami do ich czytelników. Mogli teraz śledzić ich ruch także na innych stronach i wykupywać na nich tańsze reklamy.

Dane dotyczące odwiedzających stały się towarem. Wirtualne domy aukcyjne[31] takie jak BlueKai zaczęły oferować je w trybie ciągłym. BlueKai sprzedawał codziennie 18 mln informacji[32] o zachowaniu internautów za 0,1 centa za sztukę[33].

Aukcja mogła rozpocząć się w dowolnym momencie: kiedy trafialiście na stronę, wasze dane były sprzedawane temu, kto proponował za nie najwięcej. Zwycięzca mógł wyświetlić wam spersonalizowaną reklamę. Jednak *gorączka danych* spowodowała, że niektóre firmy zaczęły korzystać z jeszcze bardziej inwazyjnych metod.

W 2010 roku Dan zaczął się poważnie zastanawiać się nad konsekwencjami wirtualnego Dzikiego Zachodu, do którego rozwoju się przyczynił. Martwił go trend polegający na coraz częstszym dobieraniu danych o zachowaniach w sieci z danymi osobowymi oraz tymi, zdradzającymi preferencje zakupowe ludzi poza siecią.

Działało to następująco: użytkownik logował się na stronie internetowej, która żądała podania adresu e-mail, imion i innych danych identyfikacyjnych. Firma działająca na tej stronie, na przykład Acxiom, pobierała plik z tymi danymi, w zamian instalując „ciasteczko" na urządzeniu użytkownika. Zawierało ono informacje plasujące tę osobę w wybranych segmentach – w tym dane z rejestru wyborczego, adres zamieszkania, wysokość dochodu, historię kredytową, posiadany samochód itd. Technicznie wciąż były one anonimowe. Jednak

do możliwości precyzyjnego wskazania osób, które opisywały, było stąd bardzo blisko. Jeśli reklamodawca wie o was wszystko, to czy naprawdę ważne jest, czy zna też wasze nazwisko?

Łączenie informacji dotyczących zachowań w internecie z tymi spoza sieci tłumaczy dlaczego sześćdziesięciosiedmioletnia Linda Twombly z Nashua w Hampshire była bombardowana reklamami internetowymi kandydatów republikańskich w wyborach z 2010 roku[34]. Przedsiębiorstwo Rapleaf, wykorzystując takie właśnie metody, zaklasyfikowało ją jako konserwatystkę, o poglądach republikańskich, zainteresowaną Biblią aktywną działaczkę lokalną.

„Kurczę blade!", wykrzyknęła Linda, gdy moja redakcyjna koleżanka Emily Steel odszyfrowała informacje na jej temat z pliku będącego w posiadaniu Rapleaf. „To tak, jakby obserwował mnie jakiś strażnik! To nie wróży nic dobrego". Dan martwił się, że rozwiązanie to, przy takim zastosowaniu, narusza anonimowość, którą przecież starał się wbudować w system na etapie jego projektowania[35]. „Kiedy działacie w branży, w której szafuje się danymi, nie istnieje możliwość, by mieć je pod kontrolą"[36].

W 2011 założył firmę Korrelate. Miał nadzieję z jej pomocą przywrócić prywatność domenie śledzenia w internecie. Celem Korrelate było udowodnienie firmom, że ich reklamy *online* mogą zachęcać do zakupu produktów, bez trwonienia danych konsumentów. W wirtualnych pomieszczeniach czystych [ang. *clean room*], wykorzystując zaawansowane metody matematyczne, jego zespół pracował nad anonimizacją danych wykorzystywanych do łączenia informacji o zachowaniach w sieci i poza nią. Chodziło o to, żeby sprzedawca aut marki Honda wiedział, która reklama skłoniła klienta do nabycia produktu, bez naruszania prywatności tego klienta. Według Dana, powszechność śledzenia była nieunikniona. Zależało mu jednak na tym, by zapobiec możliwości identyfikacji osób w sieci.

* * *

Pod pewnymi względami ludzie walczący z podążającymi za nimi „ciasteczkami" toczą decydującą walkę.

Ponieważ coraz więcej ludzi jest świadomych tego zjawiska, marketingowcy poszukują nowych technologii śledzenia. Google

opracowuje już metodę, która nie korzysta z „ciasteczek", a przypisuje unikalny identyfikator każdej wyszukiwarce[37]. Część handlowców kieruje się ku technologiom „pobierania odcisków palców", umożliwiającym identyfikację użytkowników nawet w sytuacjach, gdy blokują oni możliwość śledzenia poprzez różne programy. „Jeśli nie chcecie, by ktoś wiedział, co robiliście w internecie, nie łączcie się z siecią", mówił prezes jednej z takich spółek[38].

Być może najbardziej niepokojące w tym wszystkim jest to, że kolejnym plikiem *cookie* ma być nasza twarz. Gdy technologie rozpoznawania twarzy zostaną udoskonalone, zjawisko korytarza luster przestanie dotyczyć wyłącznie sieci internetowej. Po wejściu do sklepu, będziecie rozpoznawani przez sprzedawcę, dysponującego tymi samymi zestawami danych o was, które dziś wykorzystują strony internetowe.

Firma FaceFirst oferuje sieciom handlowym narzędzie[39], które instaluje się w obiekcie celem fotografowania osób przekraczających próg sklepu. „Gdy pojawi się w nim klient istniejący w waszej bazie FaceFirst, natychmiast otrzymacie e-mail lub SMS z informacjami na jego temat oraz zdjęciem", wyjaśnia firma w swojej broszurze reklamowej. Pewien pragnący zachować anonimowość dyrektor handlowy opisał, w jaki sposób korzysta z tej technologii w rozmowie z „LP Magazine", pismem kierowanym do przedstawicieli tzw. branży zapobiegania stratom [ang. *loss-prevention industry*][40]. „Tom Smith, wiceprezes ds. zarządzania bezpieczeństwem w Store-Mart", jak go nazwano, powiedział, że jego sieć handlowa o pseudonimie „Store-Mart" korzysta z tego rozwiązania, by identyfikować złodziei.

Działa to następująco: rabuś zostaje przyłapany w sklepie Store-Mart. Następnie zostaje sfotografowany i poproszony o podpisanie oświadczenia, że więcej się w nim nie pojawi. Jeśli jednak wraca, kamery, dzięki wykonanemu wcześniej zdjęciu, rozpoznają go w pięć sekund. Odpowiednie zawiadomienie trafia do pracownika sklepu, który prosi delikwenta o opuszczenie budynku.

Oczywiście, istnieje ryzyko, że system błędnie wytypuje złodzieja, co zniechęci jakiegoś zwykłego klienta do korzystania z usług sieci. „Dla mnie jest to przerażające – fałszywy alarm, motyw chłopca, który ostrzegał przed wilkami", mówił Smith. „Na razie nie zdarza się to często: może 6 razy na 100 alarmów".

FaceFirst tworzy już wizję przyszłości, w której sprzedawcy mogliby

korzystać z rozwiązania w celach marketingowych. W broszurze reklamowej czytamy: „Stwórzcie bazę danych dobrych klientów, rozpoznajcie ich, gdy przekraczają wasze progi i pozwólcie, by poczuli się właściwie obsłużeni”[41]. Pozostawiono bez komentarza to, jak sprzedawcy mieliby traktować nabywców, których wyjątkowo nie lubią, na przykład kupujących wyłącznie na wyprzedażach albo osoby, które tylko mierzą, a nie kupują.

Jestem święcie przekonana, że nie zyskałabym na tym korytarzu luster opartym na rozpoznawaniu twarzy. Gdyby sprzedawcy zorientowali się, że jestem zabieganą, pracującą matką, przedkładającą wygodę ponad oszczędność, z pewnością skierowaliby mnie do droższych produktów. Niewiele mogłam w tej sprawie zrobić. Starałam się usunąć jak najwięcej moich zdjęć z sieci, by nie wspierać tworzenia baz umożliwiających rozpoznawanie twarzy. Zapłaciłam malarzowi, aby naszkicował mnie z fotografii i zaczęłam używać tego szkicu na Twitterze i Facebooku. Zatrudniłam także fotografkę do sesji, z której zdjęcia chciałam wykorzystywać przy promocji książek. Miały one rozmywać moje rysy tak, by nie były rozpoznawane przez algorytm.

Granicę wyznaczał mój strój. Nie zamierzałam nosić czapki z daszkiem ze światełkami LED[42], dla zmylenia kamer, ani dresu przeciwko dronom, blokującego obrazowanie termiczne[43] – zaprojektowanego przez Adama Harveya, tego od torby Faradaya dla mojego telefonu.

* * *

Wciąż jednak byłam na wojnie. Po miesiącu korzystania z NoScript, postanowiłam przetestować jego skuteczność. Zadzwoniłam więc do Ashkana Soltani, eksperta w dziedzinie technologii śledzenia reklam[44].

Pierwszy raz spotkałam Ashkana, gdy ukończył studia w Szkole Informacji na Uniwersytecie Kalifornijskim w Berkley. Prowadził tam kompleksowe badania nad różnymi typami śledzenia reklam. Przekonałam go, by zaczął robić podobne rzeczy na potrzeby „Wall Street Journal”. Był doradcą ds. technologii w wielu śledztwach dziennikarskich dotyczących prywatności. Od tamtej pory, Ashkan już dwukrotnie składał zeznania w związku z prywatnością w internecie przed amerykańskim Kongresem (w swoim jednym jedynym garniturze) i stał się wyrocznią w dziedzinie śledzenia reklam.

Zgodził się sprawdzić, czy moje metody blokowania trackingu były skuteczne. Zmieniłam kilka ustawień w mojej wyszukiwarce internetowej, zgodnie z jego sugestią, i – *voilá* – cały mój ruch internetowy przechodził przez jego komputer w Waszyngtonie.

– Dobrze, dobrze, wejdź na jakąś stronę – powiedział.

Kliknęłam na swoją służbową stronę, „WSJ.com". Ashkan zaczął odczytywać nazwy śledzących mnie firm, które dostrzegł w ruchu internetowym. „Twitter, BlueKai, DoubleClick".

– Co?! – wrzasnęłam. Myślałam, że je wszystkie zablokowałam.

Ashkan wytłumaczył mi, że strona „WSJ.com" przesyłała moje dane do BlueKai, firmy prowadzącej aukcje reklam, która to przekazuje je do Google i Yahoo!. Choć NoScript blokował JavaScript, to nie mógł powstrzymać niewidocznych dla niego skoordynowanych działań pomiędzy tymi podmiotami.

Jeśli chodzi o Twittera, to zapomniałam, że wcześniej zalogowałam się na swoim profilu, pozwalając na instalację „ciasteczek". Przez to Twitter widział, że odwiedziłam „WSJ.com".

To jest właśnie problem ze śledzeniem w internecie – jeśli choć raz wpuścicie kogoś do „namiotu", będzie mógł już zawsze was podglądać.

– Jest zdecydowanie gorzej niż myślałam – stwierdziłam.

– Dokładnie to samo powiedziałaś mi trzy lata temu, kiedy rozmawialiśmy po raz pierwszy – zaśmiał się.

Ashkan pokazał mi ustawienia ukryte głęboko w sekcji „historia przeglądania", umożliwiające wyłączenie „ciasteczek" od podmiotów trzecich jak Twitter, które śledziły mnie na innych stronach, tylko dlatego, że wcześniej zalogowałam się na ich profilu[45]. Jednak nie było ustawień blokujących zakulisową wymianę informacji, do jakiej dochodziło na stronie „Wall Street Journal".

Próbowałam skorzystać z oprogramowania AdBlock Plus, ale BlueKai przedostawał się przez te filtry. Adblock Plus był zresztą stworzony do blokowania reklam, a nie mechanizmów śledzących. BlueKai nie jest reklamodawcą, jest firmą, która skupuje dane użytkowników i sprzedaje je na aukcjach. Na tej samej zasadzie dawały sobie radę z programem inne firmy oferujące analitykę, takie jak Omniture, która tworzy profile użytkowników.

To było podręcznikowe studium przypadku na temat modelu zagrożenia. Adblock Plus został stworzony dla osób, które chciały uniknąć reklam.

NoScript jest dla użytkowników, którzy dostrzegają niebezpieczeństwo w konkretnych technologiach, w tym przypadku JavaScript.

Mój punkt widzenia był inny: chciałam zablokować mechanizmy śledzące, bez względu na to czy są powiązane z reklamami czy konkretną technologią. To doprowadziło mnie do zupełnie innej technologii blokowania: firm, które tworzą listy narzędzi do monitorowania [ang. *trackers*].

Wraz z Ashkanem skorzystaliśmy z propozycji kilku przedsiębiorstw, które zarządzają takimi listami. Z zaskoczeniem odkryliśmy, że najlepszą ofertę ma Ghostery. Byłam sceptyczna wobec tej firmy, odkąd została kupiona przez spółkę doradczą działającą w branży reklamy internetowej. Poza tym Ghostery z założenia zezwala na śledzenie. Jednak gdy znalazłam ustawienia umożliwiające wyłączenie wszelkich mechanizmów śledzących, dostrzegłam, że jest to najlepsze z możliwych rozwiązań.

Ashkan obserwował mój ruch, gdy przechodziłam z „WSJ.com" do HuffingtonPost i Gawker.com. Nie pojawiły się żadne firmy z analityką danych. Nie było BlueKai. W istocie, zauważyłam, że wyświetla się niewiele reklam. „Ruch jest rzeczywiście najczystszy. Jednak nic nie ochroni cię w pełni", powiedział Ashkan.

* * *

Ghostery mnie zaintrygowało. Dlaczego to właśnie branża reklamowa miała mi dostarczyć najlepszą broń przeciwko sobie?

W 2009 rok, przedsiębiorca David Cancel stworzył Ghostery jako darmowe oprogramowanie, mające pokazać ludziom narzędzia do śledzenia znajdujące się na każdej stronie[46]. Rok później sprzedał rozwiązanie firmie świadczącej usługi reklamowe Evidon[47], która obiecała, że pozostanie ono darmowe i nie będzie pozyskiwało i przetwarzało danych użytkowników do celów reklamowych. Evidon tylko częściowo zrealizował obietnicę. Serwis pozostał darmowy, lecz firma zaczęła sprzedawać stronom i reklamodawcom zgromadzone i przeanalizowane dane z Ghostery. Trzeba jednak oddać Evidonowi, że prosił użytkowników o dołączenie do anonimowego panelu Ghostery, zamiast uruchamiać go domyślnie. Dołączyło do niego 8 milionów użytkowników (ja nie).

Andy Kahl, dyrektor ds. analiz danych w Evidon, powiedział mi,

że wśród nabywców danych często były firmy zajmujące się monitorowaniem ruchu, chcące mieć na oku swoją konkurencję. Zatem Evidon stworzył pewien rodzaj instytucji rozliczeniowej dla takich spółek, pozwalającej im podglądać się wzajemnie.

Skorzystałam na tej grze walczących ze sobą „wywiadów". Kiedy zdecydowałam się na usługę, Ghostery zdążyło już stworzyć jedną z najbardziej kompleksowych list[48] technologii śledzących[49], stosowanych przez ponad 1600 firm. W pierwszym miesiącu korzystania przeze mnie z usługi, Ghostery dodał do niej sto nowych narzędzi. Jednocześnie pozytywne nastawienie firmy do śledzenia uderzało we mnie. Ghostery co do zasady pozwalało na monitorowanie, zatem musiałam grzebać w ustawieniach, by blokować wszystkie mechanizmy śledzące. Po miesiącu korzystania z Ghostery zauważyłam, że pewne elementy śledzące przedostają się przez narzędzie. Kahl wyjaśnił mi, że usługa nie blokuje automatycznie nowych elementów, pojawiających się na liście trackerów. Pokazał mi ustawienia pozwalające na zablokowanie tych świeżo do niej dopisanych. Pachniało mi to podstępem, ale Kahl zapewniał mnie, że zamiarem Ghostery było budowanie we mnie świadomości, że to ja o wszystkim decyduję. „Stale upewniamy się u naszych użytkowników, czy robimy dobrze. Jedynie wówczas, gdy naprawdę dobrze wykonujemy swoją robotę, możemy zbierać dane, które interesują branżę", powiedział.

Czułam się trochę nieswojo, znając motywy działania firmy. Miała przynosić zyski branży internetowego monitoringu, a nie ludziom korzystającym z jej narzędzi.

* * *

Dużo lepsze były motywy, które stały za oprogramowaniem Disconnect, stworzonym przez uciekiniera ze świata technologii śledzących.

Brian Kennish, inżynier w Google, stworzył pierwsze programy blokujące mechanizmy śledzące po przeczytaniu artykułu mojej redakcyjnej koleżanki Emily Steel[50]. W wydaniu „Wall Street Journal" z 2010 roku opisywała ona, jak w niezamierzony sposób Facebook przesyłał nazwiska użytkowników do firm zajmujących się reklamą śledzącą. Kennish nie mógł uwierzyć, że portal złamał zasadę anonimowości, której śledzący obiecali przestrzegać. Zajmował się reklamą

w Google przez prawie sześć lat i wiedział, że firma jest zobowiązana do zachowania anonimowości danych związanych ze śledzeniem.

Ghostery nie blokowało jeszcze mechanizmów śledzących na portalach społecznościowych. Tego wieczoru Kennish wrócił do domu i zaprojektował skromny program, Facebook Disconnect, który deaktywował opcję Facebooka, umożliwiającą śledzenie jego użytkowników na różnych stronach[51]. W ciągu dwóch pierwszych tygodni to darmowe oprogramowanie nie wzbudziło sensacji. Zostało pobrane zaledwie 50 tys. razy[52]. Jednak gdy zyskało pewną popularność, Kennish zaczął zastanawiać się nad mechanizmem śledzącym w Google. „Lista wyszukiwań w Google, Yahoo! i Bing mówi o was tyle samo, co historia przeglądania stron. Zrozumiałem, że muszę opuścić Google, żeby się tym zająć".

Odszedł z Google w listopadzie 2010 roku. W grudniu uruchomił darmowy program Disconnect[53], który blokował możliwość gromadzenia przez Google informacji o zapytaniach wprowadzanych do wyszukiwarki, gdy użytkownik był zalogowany do Gmaila albo innych usług Google. Unieszkodliwiał on także mechanizmy śledzące portali społecznościowych, takich jak Facebook, Twitter, Google+, Yahoo! i Digg.

Disconnect natychmiast stał się popularny. Jednak Kennish nie wiedział, czy da się na tym zarobić. Inne programy blokujące elementy śledzące były darmowe, więc nie mógł pobierać opłat za subskrypcję. Trwał „wyścig zbrojeń" i trzeba było nadążać za rozwojem technologii śledzenia. Potrzebował funduszy na ten cel.

Początkowo pracował z domu i żył z oszczędności. W październiku 2011 roku zebrał 600 tys. dolarów od inwestorów (wliczając to założyciela Ghostery, Davida Cancela)[54].

Pojechałam odwiedzić Kennisha w sierpniu 2012 roku. Jego zespół czterech inżynierów tłoczył się w salce konferencyjnej jednego z budynków w Dolinie Krzemowej, należącego do wspierającej ich kapitałowo spółki Highland Capital. Okna były zasłonięte i jedyne światło pochodziło z ekranów komputerów. Mieli tam kosz do gry w koszykówkę, ale oderwał się od ściany i jedyne co po nim pozostało to taśma, którą był przymocowany. Na stołach porozrzucane były przekąski z Costco. Tablica szkoleniowa była wypełniona statystykami wykorzystania ich oprogramowania – przydatny rekwizyt na wypadek, gdyby inwestor zatrzymał się i zapytał, co nowego[55].

Kennish nie prowadzi, więc odwiozłam go wypożyczonym samochodem do mieszkania, które wynajmuje z paroma kolegami. Było to chyba najbrzydsze mieszkanie w tym dość ładnym bloku. W środku było czysto, ale ascetycznie: jedyną dekorację stanowiły pojedyncze łóżko i kanapa. „Mam raptem pięć rzeczy", ostrzegł mnie, zanim otworzył drzwi do swojego pokoju.

W środku znajdował się leżący na podłodze podwójny japoński materac. W garderobie były trzy pary spodni, cztery pary butów i kilka koszulek, ułożonych w kostkę, na podłodze. Poza komputerem było to wszystko, co posiadał. „To pewnie z tego powodu jestem tak wkręcony w dane. Nie ma nic poza tym. Wszystko, co posiadam, to dane", powiedział[56].

Podczas obiadu w Polo Alto, wyznałam Brianowi, że jego motywy są dla mnie nie do końca zrozumiałe. Przedsiębiorcy wybierali zwykle życie mnicha, zakładając, że z czasem zbiją fortunę. Czy naprawdę sądził, że uda mu się dorobić na słabiutkim rynku programów chroniących prywatność?

Powiedział mi, że wierzy, iż rynek prywatności w końcu się rozwinie. Najpierw użytkownicy „odłączą się" od elementów śledzących. Z czasem firmy zaczną płacić użytkownikom, aby „połączyły się" z nimi ponownie. Ostatecznie będą z tego pieniądze.

„Jestem kapitalistą. I chcę zmienić świat", wyznał.

Chciałam wesprzeć Briana. Jego podejście było zbieżne z moją filozofią płacenia za usługi. Jednak jego oprogramowanie blokowało jedynie portale społecznościowe, a ja zamierzałam zablokować wszystko. W momencie, w którym przeprowadzałam testy z Ashkanem, Ghostery odłączało mechanizmy śledzące także na portalach społecznościowych. Nie było więc potrzeby korzystania z Disconnect.

W końcu, w kwietniu 2013 roku, Kennish wypuścił na rynek nowe oprogramowanie. Lista zablokowanych elementów śledzących była dłuższa niż ta, którą oferował Ghostery. Program miał jednak wady. Gdy chciałam kupić produkty spożywcze we FreshDirect, Disconnect nie tylko zablokował wszystkie elementy śledzące, lecz także przycisk „zamów" na stronie z potwierdzeniem zamówienia.

Mimo to, przełączyłam się na Disconnect i wpłaciłam datek, używając swojej maskującej, jednorazowej karty kredytowej.

Uznałam, że w tym „wyścigu zbrojeń", muszę wspierać finansowo powstańców. Gdy zabraknie konkurencji, łaska serwisów takich jak Ghostery prędzej niż później się skończy.

Mój wybór przypomniał mi początki ruchów związanych z żywnością organiczną. Często półki z jedzeniem organicznym w supermarketach były zapełniane zasuszonymi i zepsutymi produktami. Jednak wraz z upływem czasu, gdy ludzie zaczęli kupować organiczne jabłka, jakość zaczęła się poprawiać. Obecnie ekologiczne owoce i warzywa wyglądają dobrze, a nawet lepiej niż te przemysłowe.

Z mojego punktu widzenia, korzystanie z Disconnect przypominało zakup produktów organicznych w czasach, gdy dopiero zaczęły się pojawiać. Zdecydowałam, że będę wspierać rynek oprogramowania chroniącego prywatność, nawet jeśli jego oferta nie zawsze będzie tak dobra jak produkty konkurencji.

13

SAMOTNE KODY

Na trzy dni przed moim przyjęciem urodzinowym, zorientowałam się, że nikt się na nim nie pojawi, jeśli będę próbować komunikować się z moimi gośćmi za pomocą szyfru.

Miesiąc przed przyjęciem wysłałam do nich wszystkich e-mailem książkę *Secret New York: An Unusual Guide*. Tydzień później przesłałam im tą samą drogą klucz, który opisywał, jak znaleźć w niej poszczególne słowa i znaki. Na przykład (12,2,3,1) oznaczało: dwunasta strona, drugi wiersz, trzecie słowo, pierwszy znak.

Gdy kończył się czas, wysłałam e-mailem ostateczne zaproszenie napisane szyfrem. Brzmiało ono tak:

(377,23,7) (197,136)
(61,4,3) (29,27,4,1) (23,3,8,1) (23,4,10,1)
(87,26,25) (25,27,3) (25,27,4)
(393,1,2) (123,2)
(95,30,11) (389,26,12) (159,41,4) (179,16,13) (113, 14,14)

Odszyfrowane mówiło:

Przyjęcie prywatne
Dzień: 26 września, godzina: 18.00
Miejsce: Druga Aleja, nr 411/2
Kupić za gotówkę bilet na metro

Tydzień przed imprezą zaczęłam się denerwować. Zaprosiłam pół tuzina moich najbliższych przyjaciółek, ale dotąd tylko jedna z nich wspomniała, że odszyfrowała moje zaproszenie.

Spróbowałam delikatnie wybadać inną.

– To co robisz w przyszłym tygodniu?

– Och, jestem w podróży biznesowej – odpowiedziała.

Gdyby wiedziała, że organizuję przyjęcie, na którym nie będzie mogła się pojawić, wspomniałaby o tym. Tak ustaliłam, że nie odszyfrowała mojego zaproszenia.

Niestety szyfry nie poddają się łatwo ciągłemu dopasowywaniu kalendarza, które poprzedza dziś uczestnictwo w proszonych kolacjach.

Inna przyjaciółka, z zawodu lekarz, doktor nauk medycznych, wyznała w końcu, że próbowała odszyfrować wiadomość, ale jej się nie udało. „Skarbie, strasznie cię lubię... ale tylko nie to", napisała. „Nie mam tyle cierpliwości albo inteligencji, aby rozwiązać zagadkę do czasu twojego przyjęcia!".

Trzy dni przed imprezą zdałam sobie sprawę, że nikt nie przyjdzie, oprócz może jednej przyjaciółki, która sama zadzwoniła, żeby mi powiedzieć, że zdekodowała wiadomość. Anulowałam więc swoją rezerwację w restauracji – oczywiście dokonaną na nazwisko Idy – i oddzwoniłam do niej z informacją, że sprawa jest nieaktualna.

Dzień ten nadszedł i przeszedł, a nikt z reszty moich gości nie wspomniał o przyjęciu. Dwa tygodnie później zorganizowałam kolejne, używając już zwykłych, niezakodowanych e-maili. Było całkiem udane.

Lekcja, jaką wyniosłam z przygody z przyjęciem, potwierdziła się, gdy zaczęłam eksperymentować z szyfrowaniem: komunikowanie się kodem to raczej niepopularne zajęcie.

* * *

Nie mogłam za porażkę z dekodowaniem winić moich przyjaciół.

Książka szyfrów, którą im wysłałam, była trudna z dwóch powodów: (1) zaproszenie przyszło oddzielnie od książki, wymuszając na nich utrzymywanie kontroli nad oboma; a (2) użycie książki kodów do odczytania informacji nie było łatwe.

Nowoczesny, komputerowy dekryptaż prawdopodobnie rozwiązałby

oba problemy.

Dzisiaj komputery w magiczny sposób dokonują całości szyfrowania i dekodowania. A co jeszcze bardziej zadziwiające, nie ma już książek kodowych. Przechowuję w moim komputerze klucz, który jest tajny i znany tylko mnie. Mam też klucz publiczny, który umieszczam na stronie internetowej, żeby ktoś go sobie pobrał. Oba pozwalają mi szyfrować i odszyfrowywać wiadomości bez pomocy książki kodowej.

Podobnym wyzwaniem było skłonienie ludzi do korzystania z szyfrowanych e-maili. Nawet wielu z moich przyjaciół hakerów odmówiło używania szyfrów w korespondencji ze mną – niektórzy twierdzili, że wątpią w moją zdolność prawidłowego szyfrowania, inni mówili, że nie ufają z kolei sobie w kwestii korzystania z tego nadzwyczaj skomplikowanego systemu.

Przyjrzyjmy się, jak wyglądało tworzenie przeze mnie własnego systemu kodowania e-maili.

Po pierwsze ściągnęłam od GNU Privacy Guard darmowe oprogramowanie szyfrujące do zarządzania moimi kluczami[1]. Tworząc klucz, musiałam szybko ruszać myszą, żeby pomóc go zbudować generatorowi losowych liczb. Gdy już go uzyskałam, umieściłam go w serwerze kluczy publicznych, aby inni mogli go sobie wyszukać.

Potem pobrałam program zwany Enigmail, który miał pracować z Postboxem, czyli oprogramowaniem używanym przeze mnie do zarządzania skrzynką pocztową[2]. (GPG jest zaprojektowany do pracy z oprogramowaniem poczty elektronicznej, które instalujecie na swoim komputerze, a nie z e-mailem łączącym was z internetem[3]).

Nie potrafiłam jednak zmusić Postboxa i Enigmail-a do współpracy. Strona z pomocą Postboxa odpowiedziała, żeby we wszystkich sprawach kontaktować się z Enigmail-em[4]. Na forach pomocowych Enigmail-a twierdzono natomiast, że Postbox stworzył własną wersję Enigmail-a, która nie jest obsługiwana przez starszą odsłonę[5].

Wpadłam więc w lukę pomiędzy dwoma programami, które – choć miały działać wspólnie – nie współpracowały. Przyprawiło mnie to o lekkie mdłości. Zeszłam do salonu, nalałam sobie kieliszek wina i zaczęłam zastanawiać się nad tym, dlaczego aż tak bardzo męczą mnie techniczne aspekty usuwania błędów. Nie mam w końcu problemów z pisaniem i nadpisywaniem, co przecież powinno być podobne. Mimo to usuwanie błędów komputerowych zawsze mnie osłabiało. Pamiętam te

godziny spędzane w laboratorium komputerowym college'u nad próbami usunięcia błędów z moich programów – i to samo uczucie mdłości, i tę samą rozpaczliwą chęć ucieczki.

Uznałam, że moim problemem jest niepewność. Czytam dużo, więc znam świat pisania. Gdy poprawiam moje teksty, często odwołuję się do technik stosowanych przez innych autorów. Ale nie orientuję się tak dobrze w technicznym krajobrazie. W związku z tym, gdy usuwam błędy techniczne, czuję się tak, jakbym potykała się w ciemności, nie mając żadnych punktów odniesienia.

Oczywiście istnieją gdzieś podręczniki z instrukcjami. Skwapliwie pobrałam instruktaż CryptoParty, który zawierał pomocne ilustracje, krok po kroku opisujące instalowanie szyfrowania e-maili[6]. Jednak był on przeznaczony dla programu poczty Thunderbird, a nie Postbox, którego używałam. W świecie błyskawicznie zmieniających się narzędzi technologicznych trudno o aktualne podręczniki.

Po wypiciu kieliszka wina i krótkim namyśle, zebrałam się na odwagę i wróciłam na piętro, żeby spróbować raz jeszcze. Wciąż jednak nie potrafiłam nic zrobić i poddałam się po kolejnej rundzie. W końcu poprosiłam o pomoc bardziej sprawną technicznie koleżankę z pracy, która w ciągu godziny znalazła instrukcje (było ich parę) i skłoniła te dwa rodzaje oprogramowania do zgodnej współpracy.

Teraz potrzebowałam tylko wyszukać osoby chętne do wymiany zaszyfrowanych e-maili. Mogłam znaleźć ich wiele na liście z serwera kluczy GPG, ale nie było oczywiste, że wymienione tam postaci były tymi samymi, które znałam w realnym życiu.

Na przykład po ujawnieniu przez Snowdena tajnych informacji, znalazłam na serwerze kluczy publicznych GPG trzy przypisane Edwardowi Snowdenowi. Jeden był dla adresu e-mailowego Lavabit, drugi dla Booz Allen, a trzeci dla ItAllGoesToTheSamePlaceAnyway@anydomain.com. To ostatnie, to przypuszczalnie coś, co w czyimś pojęciu miało być żartem.

Ale któż może wiedzieć, czy te pierwsze dwa były autentyczne (jak się okazało, Snowden używał chyba adresu Lavabit w celu dotarcia do rosyjskich obrońców praw człowieka)?[7]. Oto dlaczego niektórzy ludzie organizują przyjęcia z „podpisywaniem kluczy", podczas których mogą się z spotkać osobiście z każdym, kogo klucz mają zamiar pobrać.

Podpisywanie klucza przypominało mi dodawanie znajomych

na Facebooku. Skoro istotą kryptografii ma być tajność, czemu miałabym tworzyć kolejną, publiczną listę ludzi, z którymi się komunikuję? A poza tym, jak bardzo mogę im zaufać? Zamiast tego umieściłam więc na swojej stronie internetowej „odcisk palca" mojego klucza – 40-znakowy ciąg liter i cyfr – dla każdego, kto chciałby sprawdzić, że ja to ja[8].

Gdy miałam już działający system, wymienianie zaszyfrowanych e-maili z kilkoma współpracownikami i sprawnymi technicznie przyjaciółmi było zwykłą igraszką. Wiadomości pojawiały się w mojej skrzynce w postaci długaśnych bloków przypadkowych cyfr, liter i symboli, a kiedy wprowadziłam swoje hasło, ten przypadkowy ciąg w magiczny sposób zamieniał się w treść e-maila.

Zaczęłam już się cieszyć życiem swoich zaszyfrowanych e-maili, kiedy na pewnej konferencji wpadłam Christophera Soghoiana, technologa ACLU. Snowden ujawnił właśnie pierwsze wiadomości i dyskutowaliśmy nad potrzebą szyfrowania e-maili.

„Bardzo nie lubię używać GPG", powiedział mi Soghoian[9]. „To tak skomplikowane, że szansa, iż się pogubimy, jest ogromna. Boję się, że wmówi się użytkownikom fałszywe bezpieczeństwo i napiszą coś, co może wpędzić ich w kłopoty".

Wyznał, że swój klucz główny [ang. *master key*] trzyma na zaszyfrowanym twardym dysku w zamkniętej szufladzie w swoim biurze. Natomiast podklucze, które są ważne przez rok, na karcie czipowej w portfelu. Aby odczytać lub napisać szyfrowanego e-maila, wkłada kartę czipową do czytnika w laptopie, a potem wprowadza dodatkowe hasło.

Natychmiast oprzytomniałam. Nie miałam klucza głównego ani podkluczy, a nawet nie wiedziałam, że ich potrzebuję. Mój klucz nie znajdował się ani w szufladzie, ani na karcie czipowej; był w moim laptopie.

Później, na pokonferencyjnym poczęstunku, lamentowałam w obecności Davida Robinsona, konsultanta prawnego i technicznego, który pomógł Uniwersytetowi Princeton założyć Centrum Działań IT, nad swoją niekompetencją w kwestii GPG. Robinson pokazał mi wtedy stronę internetową, która sprawiła, że poczułam się lepiej[10]. To była prywatna strona Karla Fogela, znanego autora programów komputerowych. Widniał na niej jego klucz publiczny wraz z takim zastrzeżeniem: „Nie mam zaufania do swoich umiejętności korzystania z GnuPG... Pilnowanie (przed możliwymi atakami na GPG) wymagałoby stałej czujności, czemu nie

jestem w stanie podołać. A więc, jeśli jest ważne, żeby wasza wiadomość dla mnie była rzeczywiście tajna, proszę o kontakt, zanim ją wyślecie. Coś wymyślimy”[11].

* * *

Wadą szyfrowania kluczami publicznymi jest to, że w kwestii ich ochrony polega się na ludziach.

Dawniej, gdy istniały jeszcze książki kodowe, to specjalni posłańcy wozili je między szpiegami i pracownikami wojskowego wywiadu. A jednak również teraz musimy strzec przechowywanych w naszych komputerach kluczy prywatnych tak skutecznie, jak tamci wywiadowcy pilnowali swoich książek.

Tymczasem jest to w zasadzie niewykonalne. Komputery i smartfony są rozrzutne, dosłownie wylewają z siebie dane, gdy tylko połączą się z internetem. A nasze książki kodów mogą zostać przechwycone nawet na granicy, gdzie służby regularnie wyłapują narzędzia informatyczne i bez nakazów kopiują ich całe zawartości. W 2010 roku śledczy ze Straży Imigracyjnej i Celnej[12] podnieśli alarm z powodu planowanej podróży Davida House’a, współpracownika Bradleya Manninga, tj. tego szeregowca, który wyniósł dokumenty rządu amerykańskiego do WikiLeaks. Gdy House wrócił z Meksyku, został odprowadzony na bok na przesłuchanie, a jego urządzenia zostały skonfiskowane. (House pozwał Departament Bezpieczeństwa Wewnętrznego i ostatecznie doprowadził do ugody, w ramach której rząd zgodził się na zniszczenie pobranych z jego sprzętu elektronicznego danych[13]).

Im więcej dowiadywałam się o przeszukaniach na granicy, tym bardziej martwiłam się, że także moje dane – kontakty, kody i hasła – są zagrożone. Postanowiłam więc nie przewozić przez granicę żadnych informacji. Na podróż biznesową do Europy wzięłam stary laptop mojego męża i pojechałam bez telefonu. Na laptopie nie było żadnych plików ani e-maili. Do swoich plików wchodziłam przez zaszyfrowaną chmurę SpiderOak, a e-maile ściągałam z internetu.

Problemem były jednak moje klucze. Chciałam podczas pobytu zagranicą korzystać z szyfrowania, przewiozłam więc mój tajny klucz w USB, zamierzając zniszczyć go przed powrotem do Stanów. Niemniej nie zaplanowałam, jak zniszczyć dysk, i kiedy nadszedł czas wyjazdu, nie

miałam serca tłuc go hotelową lampką. Zamiast tego wykasowałam po prostu jego zawartość i liczyłam na łut szczęścia. I rzeczywiście, traf chciał, że kiedy przybyłam do Nowego Jorku, przemknęłam przez stanowisko celników bez żadnych problemów.

Podróżowanie bez danych było zaskakująco relaksujące. Co wieczór logowałam się do poczty elektronicznej i – *voilà* – niczego nie traciłam. A przy tym byłam w stanie w dużo większym stopniu skupić się na pracy, bez rozpraszającego telefonu i syreniego śpiewu permanentnej komunikacji.

Uznałam, że przekraczanie granicy bez danych jest nie tylko pożyteczne z punktu widzenia ochrony prywatności, ale także korzystne dla mojego zdrowia psychicznego.

* * *

Wciąż jednak ryzykowne było trzymanie mojej książki kodów na komputerze i narażanie się na zagrożenie ze strony złośliwego oprogramowania – co jest akurat najnowszym trendem w rozwoju cyberszpiegostwa.

Przyjrzyjmy się historii Husaina Abdulli, amerykańskiego obywatela, dyrektora organizacji o nazwie Amerykanie za Demokracją i Prawami Człowieka w Bahrajnie[14]. W kwietniu 2012 roku szedł na spotkanie na Kapitolu, aby przedyskutować brutalną akcję przeciwko manifestującym w Bahrajnie demokratom. Po drodze kliknął na swoim smartfonie BlackBerry w e-mail od dziennikarza, zatytułowany „Powstanie nowego dialogu – Al-Wefaq & rząd", na temat wspierającej protestujących bahrajńskiej partii politycznej o nazwie Al-Wefaq. Husain próbował pobrać załącznik do e-maila, ale mu się nie udało. Nabrawszy podejrzeń, on i inni aktywiści z Bahrajnu, którzy otrzymali podobne załączniki, przekazali te e-maile nieustraszonemu reporterowi z „Bloomberg News", który z kolei namówił do przejrzenia tych plików specjalistów bezpieczeństwa cyfrowego.

Po miesiącach mrówczej pracy stwierdzili oni, że załączniki zawierają złośliwe oprogramowanie, które raz otwarte na urządzeniach działaczy, może zapisywać ich wszystkie uderzenia w klawiaturę, robić zrzuty z ekranu, uruchamiać ich kamery i mikrofony oraz podsłuchiwać rozmowy[15]. Okazało się też, że to oprogramowanie – stworzone przez

mieszczącą się w Wielkiej Brytanii Gamma Group – wysyłało wszystkie te informacje do komputerów w Bahrajnie. Firma Gamma odpowiedziała reporterowi „Bloomberga", że nie sprzedawała tego oprogramowania do Bahrajnu i że prawdopodobnie zostało ono skradzione[16].

Gamma jest liderem w szybko rozwijającym się świecie cyberszpiegostwa. Tego typu spółki tworzą programy, które obchodzą szyfrowanie. Ich narzędzia mogą włączyć mikrofon umieszczony w waszej kieszeni, a także wyłapać każde słowo, które będziecie wstukiwać na klawiaturze.

W październiku 2011 roku moja współpracowniczka Jennifer Valentino-DeVries pojechała ze mną do Waszyngtonu, gdzie odbywała się konferencja „ISS World", podczas której rządy z całego świata kupują od spółek typu Gamma urządzenia do cyberszpiegostwa. Czasami nazywa się ją „balem podsłuchiwaczy"[17].

Nie było zaskoczeniem, że nie mogłyśmy dostać się do środka. Jennifer udało się jednak zebrać ponad 200 ulotek reklamowych od 36 spółek, w tym Gammy. W broszurach zachwalano narzędzia do hakowania, umożliwiające rządom włamywanie się do komputerów i telefonów komórkowych oraz sprzęt do „masowego przechwytywania" całej internetowej komunikacji w danym kraju. Liczne fragmenty opublikowałyśmy w internecie w bazie danych o nazwie „Surveillance Catalog: Where governments get their tools"[18].

Broszura Gamma Group na temat FinSpy[19], narzędzia użytego do monitorowania aktywistów z Bahrajnu, promowała jego funkcjonalność umożliwiającą „monitorowanie zaszyfrowanej łączności"[20]. Twierdzono, że jest on używany w kafejkach internetowych do monitorowania komunikacji przez Skype'a, a nawet do fotografowania ludzi w trakcie korzystania z niego. „FinSpy jest sprawdzonym w boju rozwiązaniem do zdalnego monitorowania, które pozwala rządowi stawić czoło bieżącym wyzwaniom związanym z nadzorem nad mobilnymi, dobrze zabezpieczonymi celami, które regularnie zmieniają lokalizację, korzystają z szyfrowanych i anonimizujących kanałów łączności i mają siedziby w obcych krajach", przekonywano w folderze[21].

„Śledź sto tysięcy obiektów" – brzmiał nagłówek w broszurze włoskiej spółki o nazwie Hacking Team. „Zdalny system kontroli może śledzić od kilku do stu tysięcy obiektów jednocześnie". Jerry Lucas, organizator „balu podsłuchiwaczy", powiedział nam, że rynek urządzeń do inwigilacji

„dostępnych od ręki” urósł od „niemal zera” przed atakiem terrorystycznym 11 września 2001 do wartości około 5 mld dolarów rocznie[22].

– W gruncie rzeczy nie obchodzi nas pytanie: „Czy jest to w interesie publicznym?” – powiedział Lucas.

* * *

Miałam nadzieję, że nie muszę się martwić tym, czy na moim komputerze lub telefonie amerykański rząd zainstalował oprogramowanie śledzące.

W końcu wydaje się, że odpowiednie służby w Stanach Zjednoczonych potrzebują nakazu rewizji, by móc zainstalować na komputerze czy telefonie podejrzanego oprogramowanie szpiegujące. Na przykład w czerwcu 2007 roku Federalne Biuro Śledcze (FBI) otrzymało taki nakaz[23] – pozwolił on na przesłanie takiego programu na konto w portalu MySpace założone przez osobę, która wysyłała alarmy bombowe do liceum niedaleko Olympii w stanie Waszyngton. (W innej sprawie sędzia magistracki z Teksasu Stephen Smith[24], który odrzucił już wniosek o śledzenie lokalizacji telefonu komórkowego, oddalił także wniosek o nakaz rewizji w postaci instalacji oprogramowania szpiegującego, gdyż uznał, że byłoby to bliższe inwigilacji niż tradycyjnej rewizji. Podobnie jak w przypadku podsłuchu, także w sprawach o monitoring wideo, sądy mogą wymagać dodatkowego uzasadnienia).

Mimo to niepokoiłam się o moją szyfrowaną komunikację, która mogłaby trafiać do dragnetu Agencji Bezpieczeństwa Krajowego (NSA). Zamontowała ona przecież podsłuchy w krajowych spółkach telekomunikacyjnych, przez które, jak donosili moi koledzy Siobhan Gorman i Jennifer Valentino-DeVries, może przechodzić nawet 75 proc. amerykańskich połączeń internetowych[25].

Zgarniając te dane do swoje sieci, Agencja zapewne zupełnie zniszczy krajową komunikację. Przy tym wydaje się, że w wyjątkowy sposób traktuje komunikację szyfrowaną. W ujawnionej w roku 2009 przez Edwarda Snowdena notatce[26] NSA twierdziła, że przechowuje „całą komunikację, która jest zakodowana albo zachodzi uzasadnione podejrzenie, że zawiera tajne treści” – nawet jeśli jest w całości komunikacją krajową.

Oznacza to, że używając szyfrowania, prawdopodobnie wywieszam

czerwoną chorągiewkę, która wciąga mnie w sieci NSA.

Dostałam też ostrzeżenie. Jeszcze zanim Snowden ujawnił rządowe dokumenty, informator z NSA Bill Binney powiedział mi, że szyfrowanie, zwane *krypto*, jest na cenzurowanym. „Nie ufam żadnemu *krypto* w przestrzeni publicznej. Jeśli nie da się czegoś złamać, przeszukam cały internet, by to dorwać", mówił[27]. Binney twierdził, że nie koduje żadnych swoich e-maili, mając świadomość, że wszystko to jest monitorowane. „Prowadzę jawną korespondencję. Chcę, żeby wszystko wiedzieli", wyznał mi. „Nazywam ich gestapo i brunatne koszule z Białego Domu".

Pewnego wieczora spotkałam się na kolacji w barze w Bethesdzie z trzema informatorami z NSA: Binneyem, Kirkiem Wiebe'em i Thomasem Drake'em[28]. Wiebe poradził mi używanie krótkofalówek GMRS (General Mobile Radio Service). Binney zasugerował powrót do prawdziwych książek kodowych dystrybuowanych pocztą.

Drake powiedział mi, że odrobił tę lekcję wcześniej, kiedy nadzorował załogę samolotu przeznaczonego do przechwytywania i zakłócania wrogiej łączności. Podczas ćwiczeń w Nevadzie jego zespół zdołał umknąć myśliwcowi F-15, wykonując manewry, które zablokowały pulsacyjne radary dopplerowskie F-15, co pozwoliło im zejść na bardzo niską wysokość i stopić się z echem pochodzącym od ziemi.

„Oto jak pokonujesz wysoką technologię podstawową technologią", powiedział.

Mi jednak wciąż chodziło o rozwiązanie technologiczne. A tym, które stosowała większość znanych mi hakerów, był szyfrowany protokół komunikatora internetowego znany jako Off-the-Record Messaging.

Off-the-Record został stworzony w roku 2004 przez Nikitę Borysowa i Iana Goldberga[29], pracujących pod kierunkiem Erika Brewera, profesora informatyki na Uniwersytecie Kalifornijskim w Berkeley. To darmowy protokół szyfrujący, którego można używać wraz istniejącymi komunikatorami internetowymi.

Off-the-Record rozwiązuje problem użytkowników, którzy chcą strzec swoich kluczy poprzez automatyczne tworzenie nowych[30], często w trakcie danego czatu. Ktoś, kto ją inwigiluje, musi pozyskiwać te nowe klucze w trakcie toczącej się konwersacji.

Teoretycznie czyniło to Off-the-Record bezpieczniejszym od szyfrowanych e-maili. Niemniej wcale nie był on dużo łatwiejszy w użyciu.

Żeby skorzystać z Off-the-Record, musiałam ściągnąć trzy różne programy, a następnie skłonić je do współpracy. Najpierw do połączenia się z internetem użyłam anonimizującego programu Tor. Potem założyłam konto na komunikatorze internetowym Jabber. Następnie pobrałam zawierający protokół Off-the-Record program o nazwie Adium. Wreszcie skonfigurowałam Adium do pracy z Torem i Jabberem.

Byłam w stanie zrobić to wszystko tylko dlatego, że prowadził mnie specjalista bezpieczeństwa cyfrowego Jacob Appelbaum. Mówił, gdzie mam kliknąć i co wpisać w ustawieniach.

A przecież ta sklecona naprędce mieszanka darmowych programów była szczytem nowoczesności w dziedzinie szyfrowanej komunikacji. Zauważyłam, że wiele z moich wrażliwych źródeł informacji chce rozmawiać ze mną wyłącznie za pomocą kombinacji komunikatorowej Tora, Jabbera i Off-the-Record. W przypadku tych najważniejszych używałam czasami Tora, Jabbera i Off-the-Record na wyczyszczonym komputerze, który uruchamiałam przy użyciu USB zawierającego system operacyjny o nazwie Amnezyjny System Incognito Live (system operacyjny Tails)[31]. Tails jest darmowym, powszechnie dostępnym programem, który, gdy już zaprzyjaźniony haker zainstalował mi go na USB, był zaskakująco łatwy w użyciu. Kapitalne w Tails jest to, że jest on od początku zaprojektowany dla ochrony prywatności, a więc nie trzeba tam wprowadzać ustawień umożliwiających wycofanie danych czy chroniących przed ładowaniem niechcianych programów. Korzystanie z Tails było moją jedyną i najlepszą przelotną przygodą w tym alternatywnym świecie, w którym prywatność jest domyślnym wyborem.

W trakcie postępowania przed sądem wojskowym Bradley Manning, szeregowiec armii amerykańskiej, który wyniósł dokumenty do WikiLeaks, opisywał[32], jak połączył się z WikiLeaks używając do zaszyfrowanych czatów Tora i Jabbera. „Anonimowość zapewniana przez Tora i Jabbera oraz polityka organizacji WikiLeaks pozwoliły mi poczuć się sobą, wolnym od trosk związanych z tym, jak byłem postrzegany i etykietowany w realnym życiu”, powiedział Manning w swoim oświadczeniu przed sądem.

Szyfrowanie oczywiście ostatecznie nie ocaliło Manninga. Został zdradzony przez kolegę[33], hakera o nazwisku Adrian Lamo, który wydał go FBI. Rządowi śledczy znaleźli później w jego komputerze ślady korespondencji; na liście „liście kumpli” Manninga w Jabberze był Jullian

Assange[34].

A więc nawet ten niezgrabny, zaprojektowany do ukrywania się zestaw, może ujawniać zbyt wiele. To współpracujące trio programów jest też nadzwyczaj delikatne. Jakakolwiek zmiana w którymś z nich może wywołać efekt domina. Rok po tym, jak je zainstalowałam, Tor zmienił swoje ustawienia *proxy* i minęło kilka tygodni, zanim zrozumiałam, dlaczego przestał działać Jabber.

Nie mogłam obwiniać o to autorów oprogramowania. Tor jest jedynym, który ma jakiś opłacany zespół[35]. Jabber jest prowadzony przez wolontariuszy[36], którzy pracując na darowanych komputerach, walczą w jego obronie z nawracającymi atakami hakerskimi. Off-the-Record jest z kolei wolontariatem kierowanym[37] przez Iana Goldberga, obecnie profesora Uniwersytetu Waterloo.

Adium jest natomiast ogólnie dostępnym projektem prowadzonym przez Evana Schoenberga. Nie było wielu informacji o nim na stronie internetowej, więc zadzwoniłam do niego. Okazało się, że jest okulistą kończącym czwarty rok stażu w klinice[38]. Wystartował z Adium w college'u i starał się kontynuować projekt. „Gdy wybierałem się do szkoły medycznej, myślałem, że go komuś przekażę – oddam w cudze ręce", mówił mi Schoenberg (miał czas na rozmowę, ponieważ był to akurat spokojny dzień w szpitalu). „Ale nie mogłem znaleźć nikogo z doświadczeniem programistycznym, kto wydawałby się chętny do zaangażowania się w bieżące zarządzanie". I tak Adium podupadł. „Po prostu nie miałem na to czasu i większość zespołu poszła do normalnej, płatnej pracy", powiedział mi Schoenberg.

I na tym delikatnym fundamencie spoczęły moje najtrwalsze nadzieje związane z szyfrowaniem.

* * *

A przecież nie tak to miało wyglądać.

Gdy w roku 1991 antynuklearny aktywista Philip Zimmermann wprowadził pierwszy skierowany na masowy rynek program do kodowania o nazwie Pretty Good Privacy (PGP), wydawało się[39], że szyfrowanie w krótkim czasie wyswobodzi ludzkość z opresji.

PGP był pierwszym programem, który oferował zwykłym ludziom dostęp do kryptażu na poziomie wojskowym. Do tego czasu

wszechstronne komputerowe szyfrowanie było dostępne tylko dla rządu i wielkich korporacji, gotowych płacić drogie licencje. (Oprogramowanie GPG, którego używam do szyfrowania, to darmowa wersja PGP)[40].

Upowszechnienie solidnego kryptażu przyczyniło się do powstania ruchu zwanego Cypherpunks. 9 marca 1993 roku Eric Hughes opublikował „A Cypherpunk's Manifesto"[41]. „Prywatność jest władzą nad selektywnym odsłanianiem się przed światem", pisał Hughes. „Kiedy kupuję gazetę w sklepie i wręczam pieniądze kasjerowi, nie ma żadnej potrzeby, żeby wiedział, kim jestem... Jeśli moje dane identyfikacyjne są ujawniane poprzez ukryty mechanizm takiej transakcji, nie mam żadnej prywatności. Nie mogę tutaj odsłaniać się selektywnie; zawsze muszę ujawniać siebie w całości". Wzywał cyfrowe punki do stworzenia systemu, który pozwoli ludziom pozostać anonimowymi. „Musimy bronić własnej prywatności, jeśli chcemy w ogóle mieć jakąś", napisał. „Ludzie od wieków bronią swojej prywatności, wykorzystując do tego szepty, cień, koperty, zamknięte drzwi, sekretne uściski dłoni i posłańców. Technologie przeszłości nie pozwalały na silną prywatność, ale technologia elektroniczna – owszem".

Nie jest zaskoczeniem, że rząd Stanów Zjednoczonych nie był zbyt uszczęśliwiony powstaniem cyfrowych punków. Służby celne zaczęły sprawdzać, czy aby Zimmerman nie złamał prawa o handlu bronią[42], gdyż zgodnie z przepisami dotyczącymi eksportu wysoko skuteczne szyfrowanie było uważane za amunicję. Jednak w roku 1996 rząd zamknął śledztwo, nie stawiając mu zarzutów[43]. W 1999 roku Stany Zjednoczone zrezygnowały też z zakazu eksportu produktów szyfrowania[44].

NSA postanowiła inwigilować ruch w inny sposób. Stworzyła „Clipper chip" do szyfrowania transmisji głosowych[45]. Haczyk był następujący: kopie kluczy byłyby przechowywane przez rząd[46], co oznaczało, że rząd potencjalnie był w stanie wszystko odkodować.

W 1994 roku Matt Blaze z AT&T Bell Labs ujawnił podstawowy mankament „Clipper chipa", który przeoczyli mistrzowie szpiegowania – możliwe było wysłanie rządowi bezużytecznego klucza-żartu i kontynuowanie działalności przy pomocy szyfru. Zakłopotana Agencja wkrótce odsunęła projekt na bok, umożliwiając wielki sukces cyfrowych punków. Dumny ze zwycięstwa czołowy punk Bruce Schneier napisał w 1996 roku w swojej książce zatytułowanej *Applied Cryptography*: „Nie wystarczy bronić się prawem; musimy też bronić się matematyką"[47].

Okazało się jednak, że sama kryptografia nie potrafi dać rady prawu. Cyfrowi punkowcy stworzyli „remailers" – programy[48], które w czasach, kiedy konta e-mailowe nie były jeszcze tak proste do założenia jak teraz, pozwalały użytkownikom przesyłać zaszyfrowane, anonimowe wiadomości. Tymczasem w 1996 roku największy „remailer" z siedzibą w Finlandii wolał zakończyć działalność[49] niż zastosować się do sądowego nakazu ujawnienia danych użytkownika[50], który użył remailera do rozpowszechniania krytycznych materiałów o kościele scjentologicznym.

Kryptografia nie była także w stanie przezwyciężyć problemów związanych z błędami haseł, niezabezpieczonymi komputerami oraz niechlujnym programowaniem.

W 2000 roku Bruce Schneier zrewidował swój entuzjazm[51]. W książce zatytułowanej *Secrets & Lies* oświadczył, że nie miał racji, gdy kierował czytelników ku wierze, że „kryptografia jest rodzajem magicznej mgły bezpieczeństwa, którą mogą rozpylić nad swoim oprogramowaniem i uczynić je bezpiecznym". Schneier napisał, że doszedł do wniosku, że problemem nie jest kryptografia, ale ludzie ją stosujący. „Matematyka jest logiczna; a ludzie są nieobliczalni, kapryśni i trudno ich zrozumieć", skonkludował.

NSA od dawna eksploatuje ludzką kapryśność w celu obejścia kryptografii. W 2013 roku dokumenty ujawnione przez Edwarda Snowdena zarysowały podejmowane przez Agencję „agresywne, wielostronne działania zmierzające do złamania szeroko stosowanych w internecie technologii szyfrujących"[52] poprzez zmuszanie spółek technologicznych do umożliwienia Agencji dostępu do nich oraz przez wykorzystywanie złośliwego oprogramowania do ukierunkowanych ataków i używanie swoich wpływów do obniżania standardów kryptażu.

Jednak w tym larum nad atakami Agencji na szyfrowanie przeoczono fakt, że wykorzystywane przez nią techniki sugerują, iż wciąż jeszcze nie złamała matematycznych formuł leżących u podstaw kryptografii klucza publicznego.

Schneier, który przeglądał dla „Guardiana" dokumenty Snowdena, oświadczył: „Zaufajcie matematyce. Szyfrowanie jest waszym przyjacielem. Używajcie go dobrze i upewnijcie się, że nic mu nie grozi. Dzięki temu będziecie bezpieczni nawet w obliczu NSA"[53].

* * *

W jakimś sensie ruch cyfrowych punków odżywa.

Julian Assange, przez długi czas cyfrowy punk, odmienił relacje między dziennikarzami i ich źródłami informacji, tworząc w 2006 roku zaszyfrowany, tajny schowek WikiLeaks. Oferuje on pełną anonimowość ludziom, którzy chcą upublicznić jakieś informacje[54]. Inne cyfrowe punki skupiły się na budowaniu „technologii oswobodzenia", mających uwolnić ludzi od opresyjnych reżimów. Moxie Marlinspike stworzył w San Francisco szyfrujące aplikacje[55] – Redphone i TextSecure – do telefonów z Androidem. Nathan Freitas i Projekt Guardian[56] opracowali w Nowym Jorku aplikacje do prowadzenia z telefonów komórkowych zaszyfrowanych rozmów i korzystania z Tora.

Także rząd amerykański finansował kilka projektów[57] podobnych do Tora, w imię internetowej wolności. W tym samym jednak czasie Departament Sprawiedliwości inwigilował autora Tora Jacoba Appelbauma za jego zaangażowanie w WikiLeaks[58].

A Phil Zimmerman, założyciel Pretty Good Privacy, wszedł na drogę kapitalizmu. Sprzedał w 1997 roku PGP firmie Network Associates za 36 mln dolarów[59], zaś w 2012 roku włączył się wraz z kryptologiem Jonem Callasem i byłym członkiem formacji SEAL Mike'em Janke'em w budowanie płatnego serwisu kryptograficznego o nazwie Silent Circle. Sprzedawał on aplikacje do szyfrowania tekstów i rozmów telefonicznych[60].

* * *

Silent Circle był najprostszym programem, z jakiego kiedykolwiek korzystałam. Wszystko, co musiałam zrobić, to ściągnąć na mój iPhone dwie aplikacje, Silent Text i Silent Phone, i po chwili byłam już zaszyfrowana.

Ale potrzebowałam jeszcze kogoś do rozmowy. Serwis kosztował 9.95 dolarów miesięcznie, a ja miałam duże trudności ze znalezieniem kogoś pragnącego się przyłączyć.

W końcu przekonałam pewne wrażliwe źródło do pobrania Silent Text oraz Silent Phone. Usiedliśmy w barze i spędziliśmy godzinę

na instalowaniu aplikacji na naszych telefonach i upewnianiu się, że działają. Nazwałam się Ida, a moje źródło także użyło jakiegoś fikcyjnego nazwiska.

Kilkakrotnie udało nam się przesłać SMS-y, a nawet odbyliśmy rozmowę telefoniczną na Silent Phone. Była ona dość niewygodna – z trzysekundowym poślizgiem między wypowiedzią i transmisją, ale na ogół wszystko działało. Dyrektor i współzałożyciel Silent Circle Mike Janke powiedział mi[61], że opóźnienia spowodowane były korzystaniem z tego za pomocą sieci telefonii komórkowej zamiast WI-FI (wyłączyłam WI-FI, żeby uniknąć lokalizowania mnie przez sieci handlowe). Zwrócił też uwagę, że moje źródło i ja nie wcisnęliśmy na początku rozmowy telefonicznej przycisku „sprawdź", które to przeoczenie także mogło wpłynąć na zakłócenia w trakcie rozmowy.

Ale kiedy próbowałam umówić się na spotkanie z moim źródłem, nagle przestałam otrzymywać odpowiedzi na Silent Texty. Widziałam tylko wiadomość o treści: „tworzenie klucza".

Kiedy później spytałam Silent Circle o ten przypadek, technolog Jon Callas wyjaśnił mi, że przy każdym tekście Silent Text wymienia zestaw kluczy na nowy. A to oznacza przekazanie najważniejszych informacji w tę i z powrotem przynajmniej trzy razy, zanim jeszcze zacznie się przesyłanie SMS-a[62]. Pozwala to Silent Circle pozbywać się mojego klucza po każdej sesji w podobny sposób jak robił to Off-the-Record.

Jednak dla sprawnej wymiany klucza obie strony muszą być w tym samym czasie na linii. Zwróciłam uwagę, że jeśli ja albo mój partner z Silent Text bylibyśmy w windzie albo poza zasięgiem, to wymiana kluczy mogłaby się nie dokonać.

W naszym przypadku jedno z nas – moje źródło albo ja – „przerwało" generowanie klucza w trakcie komunikacji. W rezultacie nasze SMS-y nie przechodziły. Mieliśmy spotkać się wieczorem, ale nie mieliśmy jeszcze ustalonego miejsca i czasu.

Dzień upływał, a ja coraz wpadałam w coraz większą rozpacz. Wysłałam do mojego źródła SMS-a z pytaniem, gdzie i kiedy mamy się spotkać, ale nie dostałam odpowiedzi. Do popołudnia zaczęłam się już niepokoić.

O godzinie 15.13 napisałam: „Możesz bez problemu zadzwonić albo napisać mi miejsce spotkania. Mam nadzieję, że się uda!". Ciągle brak reakcji. Zaczęłam się martwić, że moje źródło stchórzyło.

O godzinie 17.07 spróbowałam raz jeszcze: „Hmm – mam potwierdzenie

odbioru SMS-a, ale żadnej wiadomości zwrotnej". Wciąż bez echa.

Wreszcie o 18.24 moje źródło zadzwoniło do mnie na telefon komórkowy, żeby się zameldować. I tyle było szyfrowania. Jesteśmy z powrotem w sieci.

To jest właśnie zagwozdka związana z wykorzystywaniem w dzisiejszym świecie szyfrów. Gdy działają, mamy do czynienia z magią. Gdy zawodzą, stanowią najgorszy rodzaj fałszywej obietnicy – potrafią zdradzić najdelikatniejsze relacje.

* * *

Kontynuowałam korzystanie z Silent Circle. Pomimo wszystkich swoich wad był on dużo mniej niewygodny niż inne programy do szyfrowania, których używałam.

Namówiłam do tego kilka osób: bliską przyjaciółkę mieszkającą w Paryżu, mojego współpracownika przy pisaniu książek, który żył w Japonii i kolegę z branży. I nauczyłam się żyć z „przerwanymi" kluczami. Moja przyjaciółka z Paryża – która na Silent Circle nazwała się na Hedy Lamarr – i ja „przerywałyśmy" klucze tak często, że w trakcie naszych cotygodniowych rozmów telefonicznych stale musiałyśmy naciskać „reset", by te ostatecznie się wyzerowały.

W końcu obie zaczęłyśmy postrzegać Silent Text jako coś bliższego komunikatorowi internetowemu niż SMS-om. Obie musiałyśmy być w tym samym czasie w sieci. Jeśli jedna z nas była poza siecią, generowanie kluczy zostawało wstrzymane, a nasze wiadomości znikały w eterze.

Silent Text wyzwolił także u Hedy wewnętrznego piromaniaka. Zakochała się w możliwości „podpalania" wiadomości. Mogły rozpłynąć się na moich oczach 24 godziny po tym, jak je otrzymałam. Czasami jej wiadomości rozpadały się w proch, zanim nawet zdążyłam je przeczytać. Skarżyłam się, że potrzebuję dokumentacji naszej korespondencji, by wykorzystać ją w książce, ale to tylko rozochociło ją do większego „podpalania".

W trakcie jednej ze swoich wizyt w Nowym Jorku Hedy powiedziała mi, że w końcu zaczęła mieć wątpliwości co do „palenia" wszystkich SMS-ów. „Przeczytałam jedną z twoich wiadomości i miałaś bardzo śmieszną odpowiedź", powiedziała mi. „Ale już spaliłam swoją wiadomość, więc nie

mogłam sobie przypomnieć, na co tak śmiesznie odpowiedziałaś".

I szybko postanowiła nie „palić" więcej wiadomości. Po jakimś czasie jednak zdecydowała, że dalej będzie wrzucać nasze dane do wirtualnego ognia.

– To takie słodko-gorzkie – powiedziała. – Ale takie jest życie.

14

WALKA ZE STRACHEM

Moim obowiązkiem jest pilnowanie moich dzieci. To zajęcie, któremu człowiek oddaje się w sposób ciągły. W każdej minucie życia, na jawie i we śnie, powinnam wiedzieć, gdzie są, co robią oraz czy są bezpieczne.

Każdy rodzic wie, że to męczące. Ganianie za małymi dziećmi jest wyczerpujące fizycznie, a świadomość, że jesteś odpowiedzialny za wszystko, co się stanie – z twojej bądź nie z twojej winy – jest obciążająca psychicznie. Gdyby okazało się, że wpatrywałam się w telefon komórkowy, kiedy jedno z moich dzieci wybiegło na jezdnię i zostało potrącone przez samochód (uchowaj Boże), nie tylko sama uznałabym się za winną, ale też każdy człowiek na świecie przypisałby mi odpowiedzialność za to zdarzenie.

Jest to ten rodzaj presji, który może doprowadzać ludzi do stosowania ekstremalnych środków: trzymania dzieci na smyczy, sekretnego monitorowania ich przy użyciu programu szpiegowskiego albo też zakładania kamer do podglądania opiekunek.

I rzeczywiście, wiele porad ekspertów na temat ochrony prywatności najmłodszych sprowadza się do zasady: „inwigiluj swoje dzieci”:

- Amerykańska Akademia Pediatryczna (AAP) zaleca[1] rodzicom nadzór nad ich pociechami zawsze, gdy te używają komputera, korzystanie z oprogramowania do śledzenia stron internetowych odwiedzanych przez dzieci oraz rozważenie zakupu programu blokującego dostęp do niewłaściwych stron.
- Federalne Biur Śledcze (FBI) zaleca[2] rodzicom stosowanie

oprogramowania do kontroli rodzicielskiej oraz „posiadanie stałego dostępu do kont internetowych ich dzieci, a także okazjonalne sprawdzanie ich skrzynek pocztowych”.

- Departament Bezpieczeństwa Krajowego (DHS) zaleca[3] wykorzystywanie oprogramowania do śledzenia stron internetowych, które odwiedzają dzieci. „Narzędzia monitorujące mogą być używane za wiedzą dziecka bądź bez niej”.

Mogę zrozumieć, dlaczego wielu rodziców stosuje się do tych rad. W końcu pochodzą one od państwowych instytucji. A rodzice boją się tego strasznego świata i mają nadzieję, że śledzenie dzieci pomoże im zapobiec katastrofie.

Wyobrażam sobie, że takie same rodzicielskie uczucia motywują urzędników z NSA. Ich zadaniem jest ochrona społeczeństwa i wiedzą, że to ich będzie się obwiniać, jeśli dojdzie do aktu terroru. Zatem decydują się oni monitorować wszystko – tak na wszelki wypadek.

Mimo to nie potrafiłam usprawiedliwić tworzenia dragnetów do wychwytywania wszystkich ruchów moich pociech w internecie, skoro sama starałam się unikać nadzoru. Żeby to pochwalać, musiałabym być hipokrytką.

* * *

Ale właściwie dlaczego by temu nie ulec? Dlaczego nie wsadzić procesorka z GPS-em do plecaka mojego dziecka? Dlaczego nie zainstalować programu szpiegowskiego na komputerach dzieci, monitorującego każde kliknięcie myszką? Czy byłyby wtedy bezpieczniejsze?

Być może. Warto jednak pamiętać, że już teraz są całkiem bezpieczne. Przestępczość w Stanach Zjednoczonych w ostatnich dwudziestu latach mocno spadła[4]. Liczba rozbojów w latach 1999–2009 obniżyła się o około 40 procent. Przestępstwa przeciwko własności spadły o niemal 40 procent. Kradzieże samochodów – o ponad 50 procent.

Dane z Nowego Jorku, w którym mieszkam, napawają jeszcze większym optymizmem. Od 1993 roku liczba zabójstw spadła o 83 proc.[5], włamań też o 83 proc., a kradzieży o 78 procent. Miasto ma drugi najniższy w kraju współczynnik zabójstw – w roku 2012 było to 5,05 na 100 tys.

mieszkańców. Wśród miast o liczbie mieszkańców większej niż 1 mln, wskaźnik ten jest niższy tylko w San Diego – wynosi 3,51 na 100 tys. ludzi[6].

Liczba przestępstw przeciwko dzieciom również została ograniczona. Z przeglądu badań na ten temat, przygotowanego przez Centrum Badań nad Przestępstwami Przeciwko Dzieciom (Crimes Against Children Research Center, CCRC), w latach 1992–2000 w Stanach Zjednoczonych gwałtownie spadła liczba przypadków wykorzystania dzieci na tle seksualnym[7]. Inne badania pokazują, że spada także liczba przypadków znęcania się nad dziećmi, choć współczynnik ten jest wciąż większy, niż być powinien[8]. Liczba samobójstw nastolatków[9] oraz nastoletnich ciąż [10] także zmniejszyła się w ciągu ostatnich 20 lat. A przy tym badania nieustannie wskazują, że przestępstwa przeciwko dzieciom popełniają najczęściej osoby dobrze im znane.

Skąd w takim razie przeświadczenie, że nasz cyfrowy świat jest do tego stopnia niebezpieczny, że trzeba monitorować dzieci? David Finkelhor, dyrektor CCRC, nazywa tę paranoję na punkcie dzieci i internetu „juwenoją”[11]. Juwenoja, jak przypuszcza, u współczesnych rodziców bierze się z przekonania, że stanowią oni tarczę, która chroni ich dzieci przed wpływami kultury masowej. Dawniej rodziny żyły w mniejszych społecznościach i plemionach, w których wyznawano wspólne wartości. Dzisiaj nowocześni rodzice często czują, że muszą powstrzymywać oddziaływanie kultury popularnej na dzieci – z jej afirmacją seksualności, śmieciowego jedzenia, przemocy i konsumeryzmu. „Ironią losu jest, że rodzice z najbardziej elitarnych środowisk Ameryki, tak samo rozpaczliwie jak wszyscy inni, pragną uchronić swoje dzieci przed przemożnym wpływem kultury głównego nurtu”, pisze Finkelhor.

A więc to nie tylko przestępstw boją się rodzice, lecz także zepsucia, które oddziałuje na ich dzieci spoza domu. Czy to wystarczający powód, by je śledzić?

Za szczególnie bolesną kwestię uważam dzisiaj psychologiczne efekty inwigilacji. Badania pokazują, że ukryta inwigilacja może powodować u dorosłych lęk i poczucie przytłoczenia. U dzieci wydaje się natomiast prowadzić do czegoś szczególnie przygnębiającego: studzi ich zapał do nauki.

Z przełomowego badania z roku 1975 wynika[12], że monitorowanie dzieci przez dorosłych wywołuje efekt „przekształcania gry w pracę”,

studząc u dzieci entuzjazm do zabawy z ciekawą układanką. Podczas doświadczenia zostawiono dzieci same w pokoju z kamerą i powiedziano im, że w trakcie zabawy, dorośli będą je przez nią obserwować. Gdy następnie usadzono dzieci w klasie i dano im puzzle, wykazywały dużo mniejsze zainteresowanie zabawą niż grupa kontrolna. „Świadomość bycia obserwowanym w trakcie wykonywania jakiegoś zadania i bycia ocenianym przez kogoś... wydaje się być wystarczającym powodem spadku zainteresowania tym zadaniem w późniejszym czasie", podsumowali autorzy badania Mark L. Lepper i David Greene.

Entuzjazm dzieci do zabawy spadał jeszcze bardziej, gdy dostawały za nią określoną nagrodę. Dzieciom pokazano kuszące zabawki i powiedziano im, że będą się mogły nimi pobawić, o ile będą się grzecznie zachowywać przy układaniu puzzli. Gdy później usadzono je w klasie i po raz kolejny dano im układankę, ich zainteresowanie nią było praktycznie żadne. Lepper i Greene stwierdzili, że najlepszym sposobem angażowania dzieci w aktywność jest „zastosowanie minimalnej presji, wystarczającej tylko do wywołania albo podtrzymania pożądanego zachowania".

* * *

Jeszcze zanim zainteresowałam się ochroną prywatności, uznałam, że umieszczanie zdjęć moich dzieci w internecie to kiepski pomysł. Sądziłam, że tworzenie jakiegokolwiek ich cyfrowego śladu, z którym musiałyby sobie później radzić, byłoby niewłaściwe.

Od czasu narodzin naszych dzieci, mój mąż i ja zawsze chętnie pokazywaliśmy ich zdjęcia rodzinie i znajomym. Na początku używaliśmy nieistniejącej już strony internetowej Kodak Gallery do przesyłania bliskim linków aktywujących pokazy slajdów. Dziadkom regularnie drukowaliśmy i wysyłaliśmy zdjęcia. Zaprzestaliśmy jednak korzystania z Kodak Gallery, kiedy ta zaczęła zachęcać nas do częstszego drukowania fotografii pod rygorem usunięcia naszych zdjęć z systemu[13].

Po opuszczeniu Kodak Gallery, krótko korzystaliśmy z serwisu Shutterfly do udostępniania zdjęć. Ale w końcu zorientowaliśmy się, że właściwie wcale nie chcemy się nimi aż tak „dzielić". Tylko kilka osób naprawdę chciało je bez końca oglądać. Zaczęliśmy więc wysyłać fotografie do dziadków i paru innych bliskich krewnych e-mailem.

Jednak nawet wtedy zdarzyło nam się kilka przygód, w wyniku których zdjęcia wydostały się do przestrzeni publicznej. Kiedy w 2008 roku urodził się mój syn, byłam tak wyczerpana, a przy tym chciałam powiadomić o tym tyle osób, że umieściłam jego zdjęcie na Facebooku. To zdjęcie wciąż się tam znajduje – i to mnie niepokoi. Usunęłam je, ale było wciąż wśród danych, które pobrałam z Facebooka, czyszcząc profil.

Mój mąż przesłał kiedyś przez pomyłkę zdjęcia rodzinne na Google+, bo myślał, że loguje się na koncie Gmail. Udało mu się je usunąć, niemniej zajęło trochę czasu, zanim zniknęły z wyszukiwarki.

Innym razem moja matka bez pytania umieściła na blogu fotografię mojej córki i mnie w piżamach (!). Córka zauważyła to i poprosiła babcię, żeby zdjęła ze strony zdjęcie. Babcia zrobiła to, ale znów minęło trochę czasu, zanim zniknęło ono z wyszukiwarki. Ale teraz już go nie ma.

Nadzór nad cyfrowymi obrazami moich dzieci nie jest łatwy. Organizatorzy letnich obozów i zajęć pozaszkolnych proszą o zgodę na robienie zdjęć moim dzieciom i wykorzystywanie ich do wszelkich możliwych celów. Odmawiam, ale nie satysfakcjonuje mnie rola irytującego rodzica, który tylko stwarza problemy.

Wiem, że ta walka jest z góry przegrana. Tak jak sama nie potrafię ustrzec się od publicznego fotografowania mnie, tak nie jestem w stanie uchronić moich dzieci od życia w świecie, który jest nafaszerowany kamerami.

Niemniej wydaje się niesprawiedliwe, że nie mam praw do wizerunków swoich dzieci. Gdyby ktoś nagrał film z udziałem moich dzieci, gdy znajdują się w przestrzeni publicznej i umieścił go w sieci, nie miałabym żadnego prawa do jego usunięcia.

Ale gdyby ten filmik zawierał chronioną prawami autorskimi muzykę, ich właściciel mógłby go zdjąć w mgnieniu oka. Właściwie dla żartu zadałam szybkie pytanie kilkorgu prawników: „Czy mogłabym zastrzec prawa autorskie do wizerunku swoich dzieci?". Odpowiedzieli, że nie.

A więc trzymam ich wizerunki z dala od sieci, wiedząc, że ostatecznie i tak przegram.

* * *

Są dwie ustawy, które mają chronić prywatność dzieci: ustawa o ochronie prywatności dzieci w internecie (Children's Online Privacy Protection Act)

oraz ustawa o prywatności i edukacyjnych prawach rodziny (Family Educational Rights and Privacy Act). Żadna z nich nie jest jednak szczególnie skuteczna.

Właściwie zanim jeszcze zaczęłam swoje eksperymenty z prywatnością, zdążyłam złamać ustawę z 1998 roku o ochronie prywatności dzieci w internecie. Prawo to nakłada na strony internetowe obowiązek uzyskania zgody rodziców przed zbieraniem danych osobowych dzieci poniżej 13. roku życia[14]. W roku 2013 przepisy te zostały znowelizowane[15] – rozszerzono ich zasięg na innego rodzaju dane, na śledzenie aktywności w internecie, zdjęcia, filmy i lokalizowanie.

Celem ustawy jest uniemożliwienie stronom internetowym wykorzystywania dzieci. Niestety prawo to zarazem zniechęca firmy do tworzenia witryn dedykowanych dzieciom poniżej 13. roku życia. Gdy bowiem tylko posiądą „faktyczną wiedzę", że z ich stron korzystają dzieci, muszą znaleźć sposób na zdobycie zgody ich rodziców.

W rezultacie ustawa ta zachęca do oszustw. Założyłam mojej córce konto Gmail, gdy miała siedem lat – choć Gmail wymaga, by użytkownicy mieli co najmniej trzynaście lat. Chcieliśmy, żeby mogła wysyłać e-maile do swoich dziadków, którzy mieszkają w Indiach.

Na swoją obronę dodam, że nie jestem jedynym rodzicem, który kłamie w internecie na temat swoich dzieci. W 2011 roku zespół badaczy, którym kierowała Danah Boyd z Microsoftu[16], przepytali ponad tysiąc rodziców dzieci w wieku od dziesięciu do czternastu lat i stwierdzili, że jedna trzecia z nich przyznała, że ich pociechy miały konto na Facebooku zanim ukończyły 13. rok życia, przy czym dwie trzecie tych rodziców pomogło im nawet je założyć. Naukowcy wysnuli wniosek, że prawne ograniczenia dotyczące wieku nie są „ani rozwiązaniem w trosce o prywatność i bezpieczeństwo w sieci, ani sposobem na przekazanie większych uprawnień rodzicom"[17].

Ustawa z roku 1974 o prywatności i edukacyjnych prawach rodziny została napisania, by wyposażyć rodziców w prawo dostępu do rejestrów dotyczących edukacji ich dzieci. Wprowadzała też wymóg uzyskania ich zgody przed przekazaniem tych zapisów podmiotom trzecim[18]. Ustawa ta jest jednak pełna luk. Szkoły mogą bez zgody rodziców przekazywać te dane „urzędnikom szkolnym" albo „organizacjom prowadzącym badania w imieniu szkoły". A dane takie jak nazwisko, adres, adres e-mail, telefon, waga i wzrost oraz zdjęcie ucznia uznawane za „informacje rejestrowe"

i także mogą być ujawniane bez zgody rodziców.

W Nowym Jorku szkoły publiczne wysyłają dane uczniów do zewnętrznego ośrodka gromadzenia danych o nazwie inBloom[19], który twierdzi, że pomaga szkołom rozwijać technologię wspierającą „spersonalizowane uczenie się". Podobno takie uczenie pozwoli „nauczycielom przyjąć rolę trenerów, uczniom uczyć się w swoim tempie, a technologii śledzić postępy uczniów; szkoły będą oceniane za wyniki, jakie osiągają"[20]. Za tę wizję Nowy Jork zaczął w roku 2015 płacić inBloom od 2 do 5 dolarów za dziecko[21].

Wolałabym raczej wydać te pieniądze na pensje i podręczniki, niż na przekazywanie danych moich dzieci do bazy danych o charakterze korytarza luster, w dodatku o wątpliwej, niesprawdzonej reputacji. Nie mogę jednak usunąć z niej danych o moich dzieciach. Ustawa nie przewiduje możliwości wycofania zgody na przetwarzanie danych, w przypadku, gdy szkoła dzieli się nimi z „organizacjami prowadzącymi badania"[22]. Jednak okręgi szkolne mogą, gdy mają taką chęć, ustanowić własne przepisy. InBloom, która jest organizacją *non-profit*, twierdzi, że nie przegląda, nie wykorzystuje, nie analizuje ani nie sprzedaje danych dzieci[23].

Z przykrością muszę więc podsumować, że żadna z dwóch ustaw dotyczących ochrony prywatności dzieci mnie akurat zbyt dobrze nie służy.

* * *

Uważa się powszechnie, że dzieci nie troszczą się o prywatność. Dorośli stale mi mówią, że prywatność jest kwestią pokoleniową i że dzieci są szczęśliwe, żyjąc w pełni publicznym życiem.

I jest też prawdą, że dzieci popełniają przerażające błędy, umieszczając głupstwa w internecie – co czasem ma poważne konsekwencje.

Jednym z najbardziej drastycznych przykładów jest przypadek osiemnastoletniego Justina Cartera z Teksasu[24], który został aresztowany za pisanie sarkastycznych komentarzy na swojej tablicy na Facebooku. Carter sprzeczał się z przyjacielem na temat internetowej gry „League of Legends", gdy ten nazwał go wariatem. Carter odpisał: „Jasne, myślę właśnie, że wystrzelam w powietrze przedszkole i będę patrzył na deszcz krwi niewiniątek, a potem zjem bijące serce jednego z nich". Został

aresztowany i oskarżony o stwarzanie zagrożenia terrorystycznego[25]. Carter spędził w areszcie okres od lutego do lipca 2013 roku. Kaucję w wysokości 500 tys. dolarów, na którą jego rodziny nie było stać, wpłacił anonimowy darczyńca[26].

Warto jednak pamiętać, że dorośli piszą w sieci tyle samo głupstw, w rezultacie czego również popadają w kłopoty. Przyjrzyjmy się tym dwóm historiom:

- W styczniu 2012 roku dwaj brytyjscy turyści zostali zatrzymani na dwanaście godzin[27] oraz odmówiono im prawa wjazdu do Stanów Zjednoczonych po tym, jak jeden z nich napisał tweeta o nadchodzącej podróży: „Wolne w tym tygodniu, małe pogaduchy/przygotowanka, zanim pojadę i rozwalę Amerykę". Miał na myśli „imprezowanie" w Stanach Zjednoczonych.
- 9 września 2009 roku Joe Lipari miał przykrą sytuację w sklepie Apple w Nowym Jorku[28]. Gdy wrócił do domu, sparafrazował na swojej tablicy na Facebooku cytat z filmu „Fight Club". Brzmiał on: „Joe Lipari mógłby wejść do sklepu Apple przy Piątej Alei z półautomatycznym karabinkiem na gaz Armalite AR-10 i wypruwać magazynek za magazynkiem do jednego z tych zadowolonych z siebie małych cieciów". Nie minęły dwie godziny, jak pod jego drzwiami byli już nowojorscy policjanci. Przeszukali mu dom na okoliczność posiadania materiałów wybuchowych[29], aresztowali i oskarżyli o stwarzanie zagrożenia terrorystycznego. Walczył z tymi oskarżeniami przez rok, odmawiając zawarcia ugody, aż w końcu zarzuty wycofano.

Tymczasem badania pokazują, że dzieci dbają o swoją prywatność. W roku 2012 ankieta przeprowadzona wśród nastolatków[30], którzy korzystali z aplikacji na telefonach komórkowych, wykazała, że 46 proc. z nich wyłączało możliwość śledzenia ich lokalizacji przez telefon, a 26 proc. odinstalowało tę aplikację w trosce o prywatność. Z badania wynikało także, że 70 proc. nastolatków szukało podpowiedzi, jak poradzić sobie z prywatnością w internecie[31].

Nawet dzieci, które nie wydają się specjalnie dbać o swoją prywatność,

często stosują różne triki, aby ochronić się w sieciach społecznościowych, jak wskazują ankiety przeprowadzone ze 163 nastolatkami, przeanalizowane przez badaczki z Microsoftu: Danah Boyd i Alice Marwick[32]. Opisują one sztuczkę zastosowaną przez siedemnastoletnią Carmen, która usiłowała skomunikować się ze swoimi znajomymi na Facebooku, wśród których znajdowała się także jej matka.

Carmen była smutna z powodu rozstania z chłopakiem, więc umieściła na Facebooku słowa piosenki „Always Look on the Bright Side of Life”[*18]. Matka Carmen wzięła je dosłownie i skomentowała, że powodzi się jej chyba całkiem dobrze. Ale inni znajomi zrozumieli ukrytą ironię. Piosenka pojawia się bowiem w filmie Monty Pythona pt. „Żywot Briana”, gdy główny bohater doświadcza ukrzyżowania.

Ten ukryty przekaz Carmen przemówił do mnie. Kiedyś, w moich latach licealnych nie mieliśmy Facebooka. Naszą „tablicą” był rocznik szkolny. Pod koniec roku każdy uczeń starszej klasy musiał ozdobić stronę rocznika. Moja strona – i wiele innych – była mieszanką żartów i tekstów, znanych tylko naszej grupie znajomych, wymyślonych po to, aby coś ukryć. Odnalazłam moją stronę rocznika i przejrzałam swoje wiadomości. Większości nie potrafiłam odszyfrować. Dlaczego wykrzyczałam „korektor” do swojej koleżanki Heidi? I co miałam na myśli, mówiąc do mojej przyjaciółki Suzy, żeby „wyluzowała”? Co stało się „15 sierpnia”, że chciałam się koniecznie skontaktować z moją przyjaciółką Sheryl? Wszystko zatarł czas.

W tamtym okresie jednak ukryte przekazy były skuteczne. Moi przyjaciele wiedzieli, o co mi chodzi, za to rodzice byli prawdopodobnie tak samo zdezorientowani, jak ja teraz.

W rzeczywistości zawsze dbałam o prywatność, nawet jako nastolatka. Gdy byłam dzieckiem, niepokoił mnie nadzór ze strony rodziców, teraz martwi mnie inwigilacja w wykonaniu korporacji i rządu.

Z czasem zmienił się więc tylko mój model zagrożenia.

* * *

Gdy zaczynałam swoje eksperymenty z ochroną prywatności, moje dzieci postrzegały to jako wyzwanie, które trzeba podjąć.

Przezwałam swoją córkę Harriet „szpiegiem”, gdyż była świetna w szpiegowaniu mnie. Kiedyś pracowałam w domu, a ona nie poszła

do szkoły z powodu zapalenia spojówek. Rozmawiałam w swoim pokoju z koleżanką narzekając, że nie potrafię zmusić laptopa firmy Apple do współpracy z monitorem Hewlett-Packard, gdy ten oto e-mail wpadł do mojej skrzynki pocztowej:

> *Słyszałam każde słowo, jakie powiedziałaś o tym, jak twój Mac nie współpracuje z twoim HP. Usłyszałam ponad 10 brzydkich słów i większość z nich była na „p".*

Otworzyłam drzwi sypialni i dostrzegłam moją córkę, trzymającą iPada i chichoczącą z triumfem po udanej próbie podsłuchu. Uwielbiała także podkradać się do mnie, gdy pisałam hasła.

Moje dzieci myślały, że jestem podła, bo nie pozwalam im umieszczać filmików na YouTube. Córka ma dziewięć lat, a syn pięć. Uwielbiają internet, szczególnie YouTube. Dzięki oglądaniu filmików muzycznych moja córka nauczyła się grać na pianinie. Syn natomiast zakochał się w muzyce Woody'ego Guthrie, którą tam znalazł. (Chce, żebym nazywała go w tej książce Woody, więc będę tak robić).

Harriet i Woody marzą o umieszczaniu własnych filmików na YouTubie. W końcu w świecie YouTube'a w ten właśnie sposób się rozmawia. Jedna osoba umieszcza filmik, a potem kolejna umieszcza swój, który jest doklejony do pierwszego albo odpowiada na niego. Moje dzieci mają rację, tak bowiem rozwija się sztuka, dzięki artystom dzielącym się swoją pracą. YouTube jest paryską kawiarnią naszych czasów. I czuję się okropnie, odmawiając im przyjemności tak kreatywnej zabawy.

Ale nie mogę im obiecać, że te filmiki – albo jakaś inna aktywność w sieci – nie powrócą kiedyś, żeby je prześladować. Mogą być wykorzystane przy odmowie im pracy lub paszportu, albo po prostu pozbawić je prawa do kształtowania sposobu, w jaki postrzegają je inni ludzie.

Kiedy myślę o swoim dzieciństwie, z rozmarzeniem stwierdzam, że było tak słabo udokumentowane. Nie pozostawiwszy po sobie cyfrowych śladów, byłam w stanie wymyślić siebie zupełnie na nowo, gdy tylko chciałam. W gimnazjum na przykład ubierałam się wyłącznie na różowo i turkusowo. Ale kiedy przeniosłam się na drugi koniec miasta do liceum, całkowicie zmieniłam swoją garderobę – nosiłam wyłącznie ubrania

w stylu *preppy* i eleganckie pantofle. Nikt nie dowiedział się o mojej przemianie, ponieważ po moim dawnym stylu nie było żadnego śladu, oprócz kilku zakurzonych fotografii w pudełku po butach w szafie u rodziców.

Chciałam, żeby moje dzieci miały tę samą swobodę ponownego tworzenia samych siebie. Ale miałam też świadomość, że mówienie cały czas „nie" wywoływało u nich nienawiść do prywatności i skutkowało próbami oszukania mnie.

* * *

Zdecydowałam, że podejdę do tego inaczej. Wzorując się na badaniu na temat przekształcania „zabawy w pracę", spróbowałam zamienić prywatność w zabawę.

Postanowiłam traktować narzędzia ochrony prywatności jak atrakcyjne zabawki, którymi moje dzieci miałyby okazję się pobawić, bez żadnych jawnych nagród czy śledzenia ich zachowań.

Dobrym początkiem było zarabianie na hasłach. Moja córka uwielbiała pieniądze, które uzyskiwała, rzucając kostką i sprzedając silne hasła. I była zachwycona, że ta działalność się rozwijała. Dorośli byli pod wrażeniem, kiedy mówiła im o tym hasłowym biznesie, i byli jej najważniejszymi klientami.

Dodatkową korzyścią z biznesu, jaki wymyśliła sobie Harriet, było to, że przestała podglądać mnie, gdy wpisuję hasła. Wiedziała, że albo były one przechowywane w programie 1Password, albo stanowiły „zasoloną" wersję tych, które sama dla mnie wymyśliła. Dla niej gra zmieniła swój charakter: teraz nie chodziło już o odgadnięcie mojego hasła, ale o stworzenie lepszego.

Harriet wkrótce zainteresowała się innymi moimi eksperymentami z prywatnością. Uwielbiała moją fikcyjną tożsamość – Idę Tarbell. Postanowiła, że także będzie używała fałszywego imienia do kontaktów w internecie. Żadne dziecko nie jest dość dorosłe, by posiadać profil w mediach społecznościowych, Harriet zmieniła więc na fikcyjne wyłącznie dane w adresie e-mailowym. W końcu jej rodzina i przyjaciele i tak będą wiedzieć, że to ona.

Był to taki niewinny okruch społecznościowej steganografii. Uświadomiłam sobie jednak, że nie było żadnego powodu, by nie

wprowadzać Harriet w szyfrowanie. Założyłam jej więc na iPadzie konto Silent Circle i wkrótce Harriet i Ida wymieniały zaszyfrowane SMS-y i odbywały takież rozmowy telefoniczne.

Harriet zaciekawiły również moje próby blokowania śledzenia aktywności internetowej. Stała przy moim komputerze i śmiała się, gdy próbowałam przeglądać sieć przy pomocy nieporęcznego NoScripta, utrudniającego stronom prawidłowe otwieranie się. Cieszyła się jednak, kiedy przeniosłam się do Ghostery i już mniej stron się nie ładowało. Szczególnie podobało jej się logo – sympatyczny niebieski duszek, który widnieje w prawym górnym rogu przeglądarki. Wkrótce i ona chciała mieć Ghostery.

Zainstalowałam go więc na jej komputerze, starym netbooku, który dostaliśmy za darmo, kiedy zakładaliśmy szybkie łącze internetowe. Zaczęła patrzeć na Ghostery jak na grę wideo, a celem było znalezienie stron internetowych z największą liczbą tropicieli. „Mamo, znalazłam taką z 41 elementami śledzącymi!", powiedziała kiedyś, wpadając do mojego pokoju ze swoim komputerem.

Harriet polubiła też DuckDuckGo ze śmieszną kaczką w muszce. Ustawiłam to jako jej domyślną wyszukiwarkę, a ona cieszyła się, popisując się kaczką przed przyjaciółmi.

Narzekała jednak, że aplikacja Ghostery[33] – która korzysta z wyszukiwarki DuckDuckGo – działa na iPadzie zbyt wolno. Po miesiącu jej narzekań w końcu wyciągnęłam stoper i zmierzyłyśmy to. Szukanie „nagród Grammy" na aplikacji Ghostery zajęło 6,7 sekundy. Na wyszukiwarce Apple Safari Web – 1,7 sekundy. Miała rację. Aplikacja Ghostery była na iPadzie zbyt wolna.

Zrezygnowałyśmy więc z Ghostery na iPadzie i wspólnie zainstalowałyśmy Disconnect Kids, aplikację na iPada autorstwa technika z Google, Briana Kennisha, który wystartował z nią w roku 2010[34]. Pod względem technicznym była ona w zasadzie tym samym, czego użyłam, gdy pozwoliłam Ashkanowi Soltaniemu kierować mój ruch w internecie przez jego komputery, by wyszukać elementy śledzące. Disconnect Kids także wyłapywało cały ruch wychodzący z iPada i blokowało wszelką łączność z listą znanych mechanizmów mobilnego śledzenia.

Myślałam, że to całkiem sensowne, ale Harriet była rozczarowana, że nie miało cech gry wideo. Nie mogła zobaczyć, jak wiele elementów śledzących jest blokowanych, ponieważ działanie Disconnect Kids było

niewidzialne.

Po pewnym czasie, gdy okazało się, że usługa nie blokowała działania żadnej z jej aplikacji, ja także postanowiłam zainstalować na moim iPhonie Disconnect Kids. Przecież usiłowałam znaleźć sposób na zablokowanie ogłoszeń w telefonie – a to było najlepsze rozwiązanie, jakie dotąd widziałam.

Teraz, kiedy spoglądam na tańczącego w moim telefonie zielonego robota Disconnect Kids, przypominam sobie, że moje dzieci i ja stoimy przed tymi samymi wyzwaniami związanymi z ochroną przed zasięgiem dragnetów. Ponieważ nasze dane są przez nie przemiatane w równym stopniu, naprawdę nie ma potrzeby dzielić programów na te strzegące prywatności „dzieci" i te chroniące „dorosłych".

15

DOKTRYNA NIESPRAWIEDLIWOŚCI

Po niemal roku starań, by uciec spod nadzoru, nieoczekiwanie stałam się pełna nadziei.

Z jednej strony moje wysiłki zmierzające do zniknięcia z zasięgu dragnetów nie były zbyt udane. Nie znalazłam sposobu telefonowania – także z pre-paida jednorazowego użytku – który chroniłby moją lokalizację i zwyczaje dotyczące korzystania z telefonu. Jedynym rozwiązaniem zdawało się pozostawianie urządzenia w domu albo umieszczanie w metalowej skrzynce, co jednak czyniło je bezużytecznym. Nie uwolniłam się całkowicie z uścisku Google'a i Facebooka. Moje nazwisko i adres wciąż figurowały w bazach ponad stu spółek handlujących danymi, które nie umożliwiły mi ich usunięcia. I nie zanosiło się na to, bym była w stanie uniknąć kamer rozpoznających twarze.

Jednak w innym wymiarze moje oczekiwania się spełniły i to z nawiązką.

Uwolniłam się od ogromnej większości ogłoszeń internetowych. Moje hasła – stworzone przez córkę, oparte na rzutach kostką i odnajdywaniu słów w słowniku – były całkiem silne. Fikcyjna tożsamość, Ida Tarbell, pozwoliła mi na odcięcie prawdziwej mnie od zakupów, w trakcie których traci się wrażliwe dane, niektórych rozmów telefonicznych i spotkań. I udało mi się przekonać część moich przyjaciół i informatorów do korzystania z zaszyfrowanych SMS-ów, e-maili i wiadomości w komunikatorach.

Niespodziewane moim największym sukcesem okazały się własne dzieci. Zaczynały od myślenia, że prywatność to tylko jakieś słowo oznaczające „nie". Jednak z czasem zaczęły przyswajać techniki ochrony prywatności, od blokowania śledzenia aktywności internetowej

do szyfrowania treści. Zastanawiałam się nawet, czy aby nie zapędziłam się za daleko, kiedy moja córka udzieliła mi reprymendy za wpisanie do szkolnego formularza jej numeru ubezpieczenia społecznego.

Oczywiście moje sukcesy były tymczasowe. Nowe technologie ułatwią złamanie mojego nowego, dwudziestoznakowego hasła. Im częściej moje dzieci i ja będziemy używać fikcyjnych tożsamości, tym łatwiej będzie je z powrotem z nami powiązać. Moje zaszyfrowane rozmowy są prawdopodobnie przechowywane przez Agencję Bezpieczeństwa Krajowego (NSA), w celu zabezpieczenia możliwości prowadzenia późniejszych analiz. A internetowi podglądacze już rozwijają nowe technologie obchodzenia zabezpieczeń.

Zdałam sobie jednak sprawę, że wartość tkwi w samym podejmowaniu prób. Wycofywanie zgody na przetwarzanie informacji o mnie w różnych serwisach podważa argumenty firm działających w branży baz danych, że tylko nielicznym rzeczywiście zależy na prawie do ich usunięcia. Korzystanie przeze mnie z szyfrowania i programów do anonimizacji danych dało sygnał NSA i spółkom internetowym, że nie chcę, aby czytały one moje wiadomości. Zachęciło także niektórych moich przyjaciół i współpracowników do stosowania razem ze mną kryptografii. Posługiwanie się fikcyjnymi tożsamościami skłoniło moje dzieci do rozwijania własnych strategii tworzenia pseudonimów, co, jak mamy nadzieję, zaprocentuje, gdy będą nastolatkami.

Krótko mówiąc, wierzę, że moje działania okazały się skuteczniejsze raczej w kwestii zmiany sposobu myślenia o ochronie prywatności niż przeciwdziałania inwigilacji. Przypominały mi „okupowanie barów" w latach 60. przez ciemnoskórych studentów z Greensboro w Karolinie Północnej. Siadali oni przy barze „tylko dla białych" w sklepie F.W. Woolwortha, aby zaprotestować przeciwko praktykowanej w tej spółce polityce segregacji rasowej[1]. Te protesty nie zlikwidowały rasizmu, ale doprowadziły do narodowej debaty, która ostatecznie go zmiotła.

Mam nadzieję, że jeśli wystarczająco dużo ludzi dołączy do mnie w sprzeciwie wobec masowej inwigilacji, wywołamy debatę, która także doprowadzi do istotnej zmiany.

* * *

Mimo to nie byłam zadowolona ze szkód, jakie metody przeciwdziałania

inwigilacji wyrządziły mojej psychice. Im więcej dowiadywała się o tym, kto mnie obserwuje, tym większą miałam paranoję. Gdy mój eksperyment dobiegał końca, nie zgadzałam się już nawet na rozmowy z przyjaciółmi przez internet, jeśli nie były one szyfrowane. Zaczęłam posługiwać się nieprawdziwym imieniem przy przeprowadzaniu nawet najzwyklejszych transakcji w sieci. Przyjaciółka, która zapisała się ze mną na lekcje jogi, była w szoku, że zgłosiłam się na nie jako Ida Tarbell.

Nie chciałam żyć w świecie, który budowałam – świecie podstępu, dezinformacji i ukrytych działań. To był świat oparty na strachu, pozbawiony zaufania. Nie było to miejsce, które chciałabym zostawić dzieciom.

Pamiętam moich rodziców wyrażających te same obawy wobec dwóch wielkich zagrożeń ich pokolenia – skażenia środowiska naturalnego i rozprzestrzeniania się broni masowego rażenia. Nie chcieli zostawiać dzieciom świata, który mógłby zostać przez nie zniszczony. Oczywiście nie rozwiązaliśmy całkowicie żadnego z tych problemów, niemniej zagrożenie bronią jądrową opanowaliśmy dzięki traktatom międzynarodowym, a zanieczyszczenie środowiska zmniejszyliśmy na drodze prawa i presji społecznej.

Wnioski płynące z dziedziny ochrony środowiska dla kwestii ochrony prywatności są szczególnie istotne. Oczywiście na tym polu wciąż wiele jest do zrobienia, warto jednak pamiętać, jak bardzo, jeszcze niedawno, zanieczyszczone były Stany Zjednoczone. W 1969 roku na rzece Cuyahoga w Ohio stanęła w ogniu czekoladowa plama ropy naftowej[2]. I nie był to pierwszy raz, gdy w tej silnie zanieczyszczonej na wysokości miejskich stalowni rzece zapaliły się ścieki. Nie był to także największy pożar[3]. Okładka magazynu „Time” z ogniem na wodzie z 1969 roku (uzupełniona dramatycznym i zwodniczym zdjęciem z dużo gorszego pożaru w 1952 roku) stała się jednak dla społeczeństwa sygnałem alarmowym. Przez kolejne dekady rozmawialiśmy o tym, że to niesprawiedliwe obarczać podatników kosztami usuwania skutków zanieczyszczeń środowiska, wywołanych działalnością firm z sektora przemysłowego.

Zrównoważenie produkcji pod względem ekologicznym okazało się sukcesem w każdym aspekcie. Powietrze jest bardziej świeże[4]. Woda jest czystsza[5]. Zagrożone gatunki zostały ocalone[6]. W rzece Cuyahoga w końcu lat 60. nie było ryb. Obecnie jest ich tam ponad 40 gatunków[7], a nawet kilka gatunków małży[8], co jest oznaką wciąż poprawiającej się

jakości wody. (Oczywiście przeoczyliśmy pewien duży problem środowiskowy – gromadzenie się w atmosferze dwutlenku węgla i innych gazów cieplarnianych, a w konsekwencji wzrost temperatur na Ziemi; miejmy nadzieję, że wkrótce i z tym się uporamy).

Ochrona prywatności i środowiska to podobne problemy. Szkody dotyczące każdego z tych aktywów są z pozoru niewidzialne i szybko się rozprzestrzeniają. Są skutkiem nadużywania zasobów – ziemi, wody czy informacji. Trudno odpowiedzialność za nie przypisać czemuś konkretnemu. Nie jest łatwo zidentyfikować pojedynczego truciciela albo pojedynczą informację, która wywołała szkodę. Jest ona raczej wynikiem skumulowanych działań trucicieli albo nagromadzenia danych. A przecież szkody wynikające zarówno z zanieczyszczenia środowiska, jak i naruszenia prywatności dotykają całych zbiorowości. Zanieczyszczenie nie obciąża pojedynczych ludzi – cała społeczność cierpi, kiedy powietrze jest skażone, a woda niezdatna do picia. Podobnie wszyscy cierpimy, gdy żyjemy w strachu, że nasze dane zostaną wykorzystane przeciwko nam przez próbujące nas eksploatować firmy albo przez inwigilujące nas służby.

Aby zrozumieć związek między ochroną prywatności a ochroną środowiska naturalnego, zgłosiłam się do Dennisa Hirscha, profesora prawa ochrony środowiska[9] w Capital University Law School w Ohio, który od dekady bada obie kwestie. Hirsch porównał instytucje, które pozyskują dane osobowe do ranczerów zbyt intensywnie wypasających bydło na wspólnych pastwiskach. Zjawisko to zostało zobrazowane w zamieszczonym w magazynie „Science" brzemiennym w skutki eseju[10] Garretta Hardina z 1968 roku pt. „Tragedy of the Commons"[*19]. Hardin opisywał, jak ranczerzy dążą do zwiększenia zysków poprzez zwiększanie liczebności stad bydła, choć wiedzą, że zbyt duża liczba zwierząt spustoszy i całkowicie zniszczy pastwisko. „Całkowita dowolność postępowania ze wspólnymi zasobami, prowadzi do zniszczenia wszystkiego", pisał Hardin.

Hirsch określił eksplorację danych na wielką skalę jako tragedię podobną dylematowi wspólnych zasobów. Mówił, że podobnie jak pasterze bydła, spółki pozyskujące dane mają bodziec do wykorzystywana coraz większej ich ilości. Dążą bowiem do osiągnięcia przewagi konkurencyjnej. Ale za każdym razem, kiedy tak robią, podkopują wiarę ludzi w to, że mogą o nie dbać i odpowiednio je chronić. Aż w końcu, stwierdził, ludzie stracą zaufanie do firm i przestaną ujawniać informacje

o sobie. „W tym przypadku ryzyko polega na tym, że ostatecznie i tak dojdzie do nadużycia naszego zaufania, że wycofamy się z internetu”[11], powiedział mi.

To był z pewnością dobry opis mojego własnego zachowania. Podczas śledztwa poświęconego dragnetom, straciłam zaufanie do wielu instytucji, które przechowywały dane o mnie. Stałam się *surwiwalistką* w kwestii danych. Zaczęłam ściągać je z sieci i gromadzić w domu. Stałam się także specjalistką do spraw dezinformacji – przezwyciężywszy moje obawy przed rozpowszechnianiem nieprawdziwych informacji o moich zwyczajach i o mnie samej.

Walcząc o ochronę danych, zanieczyszczałam przestrzeń publiczną i siałam nieufność. Pomyślałam, że musi istnieć lepszy sposób przeciwstawiania się niesprawiedliwym dragnetom.

* * *

Pewnym sposobem wyrównania szans byłoby wejście wszystkich do biznesu inwigilacyjnego.

Jest to argument wysuwany przez niektórych specjalistów ds. technologii, w tym Davida Brina[12], autora książki *The Transparent Society*. Opisał on w niej nieuchronne upowszechnienie się inwigilacji. Brin dowodzi, że jedyną rzeczą, która ostudzi rozrost państwa nadzoru jest rozwój tego, co nazywa „sousveillance”[*20]. Zjawisko to polega na tym, że obywatele oddolnie monitorują rząd tak agresywnie, jak ten śledzi ich z góry[13].

Z pewnością fakt, że każdy obywatel nosi teraz w telefonie komórkowym kamerę, uczynił policję bardziej ostrożną w swoich działaniach. Na przykład funkcjonariusz, który użył gazu pieprzowego[14] w spreju wobec nieagresywnych studentów protestujących na Uniwersytecie Kalifornijskim w Davis w 2011 roku, został zwolniony z pracy po tym, jak film z tej akcji został upubliczniony.

„Sousveillance” stało się również działalnością antywojenną. W 2010 roku aktor George Clooney i działacz na rzecz praw człowieka John Prendergast rozpoczęli program satelitarnego śledzenia wojny domowej w Sudanie[15]. W maju 2013 roku ich Sentinel Satellite Project ujawnił dowody na to, że ani Sudan, ani Sudan Południowy nie realizują zobowiązania wycofania wojsk z wytyczonej wzdłuż granicy strefy

zdemilitaryzowanej[16].

Niestety wielu działań rządu nie da się nadzorować kamerami czy satelitami. Moglibyśmy się nigdy nie dowiedzieć o dragnetach NSA, zarzuconych na niewinnych Amerykanów, gdyby nie wyciągnął tego na światło dzienne Edward Snowden. Bez tego, co ujawnił na temat „czarnego budżetu" agencji wywiadowczych, prawdopodobnie nie wiedzielibyśmy także, ile pieniędzy podatników wydawano na ich finansowanie[17].

Moglibyśmy nie zobaczyć mrożących krew w żyłach filmów, przedstawiających żołnierzy amerykańskich strzelających w Bagdadzie ze swoich samolotów do niewinnych dziennikarzy i dzieci, gdyby nie udostępnił ich szeregowiec Bradley Manning. Zapewne nie poznalibyśmy też dokładnej liczby cywilów zabitych podczas wojen w Iraku[18] i Afganistanie[19], gdyby Manning nie ujawnił setek tysięcy dokumentów wojennych.

Informacje Snowdena i Manninga miały olbrzymią siłę rażenia. Obaj mieli skarbonki z dokumentami, które składały się na obraz pełniejszy, niż mógłby odmalować jakikolwiek samodzielny dowód. W pewnym sensie prowadzili „sousveillance" rządu, wykorzystując do tego swoje własne informacyjne dragnety.

Okazuje się jednak, że rządowi co najmniej tak samo jak mnie nie podoba się możliwość bycia złapanym w sieć. Administracja Obamy obrzuciła błotem zarówno Manninga, jak i Snowdena, oskarżając ich o całą gamę przestępstw, w tym szpiegostwo. W 2013 roku Manning został skazany na trzydzieści pięć lat więzienia[20], Snowden zaś otrzymał tymczasowy azyl polityczny w Rosji[21].

Nie tylko zresztą wysiłki Snowdena i Manninga, zmierzające do zdemaskowania działań rządu, skutkowały prześladowaniami. Zwykli dziennikarze – którzy znajdują się na pierwszej linii frontu, patrząc rządowi na ręce – coraz częściej stają się celem śledztw. W 2013 roku Departament Sprawiedliwości poinformował agencję informacyjną Associated Press (AP) – już po fakcie – że otrzymał pochodzące z okresu dwóch miesięcy zapisy rozmów telefonicznych wielu dziennikarzy AP. Doszło do tego w związku ze śledztwem dotyczącym wycieku informacji o tajnej operacji CIA w Jemenie[22]. Gary Pruitt, prezes i dyrektor generalny AP, zaprotestował przeciwko tym naruszeniom, mówiąc: „Uważamy te działania Departamentu Sprawiedliwości za poważną ingerencję

w konstytucyjne prawa AP do zbierania i przekazywania informacji”[23].

Tymczasem Departament Sprawiedliwości wciąż naciska na reportera „New York Timesa” Jamesa Risena[24], żeby ujawnił swoje źródła informacji, które wykorzystał w książce ukazującej spartaczoną przez CIA operację dostarczenia irańskim naukowcom planów urządzeń nuklearnych. Risen powiedział, że prędzej pójdzie do więzienia, niż zezna coś o swoich źródłach[25].

Wzajemna inwigilacja chyba raczej nie wyrówna szans, jeśli rząd będzie używać władzy do prześladowania tych, którzy starają się go pociągnąć do odpowiedzialności za jego działania.

* * *

Kolejnym możliwym sposobem obarczenia tych, którzy zarzucają dragnety, odpowiedzialnością za ich działania jest nakazanie im płacenia za dostęp do danych osobowych. Ten pomysł uwodzi swoją prostotą. Wolę odebrać swoje dane, schować je w wirtualnej szafie i sprzedać niektóre na otwartym rynku – niż pozwolić, by mi je „zabrano”. Pojawiło się już kilka start-upów, liczących na prywatyzację rynku danych osobowych[26]. A Światowe Forum Ekonomiczne ogłosiło w 2011 roku, że dane te wyłaniają się jako „nowa klasa aktywów”[27].

Ale jak dotąd dane osobowe są aktywem w praktyce rozczarowującym. Powody są proste: popyt i podaż. Nie jestem posiadaczką jedynego rejestru z moimi danymi, skoro nie istnieją przepisy, które zobowiązywałyby podmioty rynku baz danych do zwrócenia mi go. Zatem nikt nie będzie chciał mi dużo zapłacić za wykorzystanie mojej kopii, jeśli gdzie indziej będzie mógł ją dostać taniej.

Analiza „Financial Times” wykazała[28], że wszechobecność danych osobowych obniżyła ich ceny tak bardzo, że informacje o wieku, płci czy lokalizacji przeciętej osoby są warte ułamek centa. A sumę wszystkich danych o większości z ludzi sprzedaje się za mniej niż dolara. Wprowadziłam informacje o mnie do kalkulatora danych „Financial Times” i zobaczyłam, że ich wartość to tylko 28 centów.

Prawo, które przyznaje ludziom własność – lub częściową własność – ich danych, może przyczynić się do podniesienia ceny. Ale też bardzo szybko się to skomplikuje. Bo w jaki sposób będę dzielić własność danych o moich połączeniach telefonicznych ze spółką AT&T? I jak uchronię się

przed przejęciem przez służby od AT&T tych częściowo tylko moich informacji?

Nie jestem wcale pewna, czy efektem handlu danymi będzie ograniczenie skutków inwigilacji. Zanim jako społeczeństwo dorobiliśmy się minimalnego wynagrodzenia i ograniczenia czasu pracy, ludzie byli gotowi „sprzedawać" swoją wielogodzinną pracę po nadzwyczaj niskich cenach.

Profesor Alessandro Acquisti z Carnegie Mellon, który prowadzi badania nad ekonomią prywatności, zauważył, że ludzie mają mniejszą skłonność do płacenia za ochronę prywatności, gdy już ją stracili. W ramach jednego z doświadczeń Acquisti i jego współpracownicy oferowali grupie ludzi kartę podarunkową Visa o wartości 10 dolarów, twierdząc że korzystanie z niej będzie anonimowe[29]. Innej grupie przekazali kartę o wartości 12 dolarów, mówiąc, że każda płatność zostanie zarejestrowana. Następnie umożliwili członkom grup wymianę kart między sobą. Spośród posiadaczy kart dziesięciodolarowych 52 proc. postanowiło je zachować – godząc się poświęcić 2 dolary w imię prywatności. Tymczasem ponad 90 proc. posiadaczy karty dwunastodolarowej odmówiło wymiany – co oznacza, że nie byli gotowi zapłacić 2 dolarów za ochronę prywatności. „To pokazuje, że ludzie wyżej cenią pewne rzeczy, kiedy je mają, niż gdy ich nie mają", powiedział mi Acquisti[30].

W istocie, gdy nie macie prywatności, odczuwacie mniejszą przykrość z powodu jej utraty. Za to doznajecie negatywnych emocji, gdy musicie ją „wykupić". Ta niezdolność do nadania odpowiedniej wartości naszym danym osobowym jest jednym z powodów, dla których większość produktów oferujących ochronę prywatności nie cieszy się sukcesem. Jest to także jeden z powodów, dla których wymiana danych osobowych na pieniądze – bez wprowadzenia przepisów uznających je za dobro rzadkie, a przez to cenniejsze – może tylko ułatwić i sankcjonować wszechobecną inwigilację.

* * *

Tak więc wracam, choć niechętnie, do prawa ograniczającego funkcjonowanie dragnetów. Moja postawa wobec nich wynika z faktu, że tak niewiele osiągnęliśmy w Stanach Zjednoczonych w dziedzinie ochrony prywatności. W odróżnieniu od innych krajów Zachodu, w USA

nie istnieją ogólne standardy obowiązujące wszystkich tych, którzy gromadzą dane osobowe. Zamiast tego są przepisy regulujące tę kwestię w poszczególnych sektorach – zdrowia[31], finansów[32], dzieci[33] i archiwów rządowych[34]. W większości nakładają one na tych, którzy gromadzą dane, obowiązek informowania o tej praktyce i uzyskiwania zgody ludzi na ich przetwarzanie. Brzmi nieźle. Jednak w praktyce obowiązek ten łatwo daje się obejść.

Dobrym przykładem jest ustawa o ochronie prywatności dzieci w internecie (Children Online Privacy Protection Act)[35]. Firmy wolą pozostawać w nieświadomości co do tego, że jakieś dzieci wchodzą na ich strony, niż uzyskiwać zgody rodziców na gromadzenie ich adresów e-mailowych.

Zwróćmy uwagę na ustawę z 1996 roku o przenoszeniu ubezpieczeń zdrowotnych i odpowiedzialności za nie (Health Insurance Portability and Accountability Act)[36], która ma umożliwiać ludziom dostęp do ich dokumentacji medycznej i przenoszenie jej do kolejnego usługodawcy. Zabrania ona sprzedaży[37] dla celów marketingowych danych zdrowotnych, pozwalających na identyfikację danej osoby, niemniej dane, które nie pozwalają na identyfikację na ogół nie podlegają ochronie. W rezultacie wiele aptek robi świetny biznes na sprzedawaniu wielkim krajowym bazom danych informacji o wykupie recept, nie pozwalających na identyfikację osób (stan Vermont próbował zakazać sprzedaży danych aptecznych, ale Sąd Najwyższy zmiażdżył jego ustawę, orzekając, że ograniczenia prowadzenia działalności marketingowej przez producentów farmaceutycznych naruszają Pierwszą Poprawkę do Konstytucji[38]).

Albo przyjrzyjmy się federalnej ustawie o prywatności (Privacy Act)[39], która zobowiązuje instytucje rządowe do pozyskiwania zgody zainteresowanych przed podzieleniem się informacjami o nich z urzędami dla celów niezwiązanych z pierwotnym celem gromadzenia danych. Okazuje się, że zamiast szukać kompromisu[40], instytucje opisują międzyresortowe dzielenie się danymi jako „rutynowy użytek”, który jest wyłączony z zakresu obowiązywania ustawy. W efekcie ustawa o prywatności nie zapobiegła przejęciu przez Krajowe Centrum ds. Antyterroryzmu (National Counterterrorism Center, NCC) od innych agencji rządowych całych baz danych obywateli, celem poszukiwania

śladów działalności terrorystycznej[41]. Prawo do prywatności oparte o pojęcie zgody wydaje się nieuchronnie skutkować tworzeniem zgód sfabrykowanych.

Przepisy przyznające ludziom prawo wglądu do tych informacji o nich, które mogą być wykorzystane przeciwko nim, wydaje się jednak dobrym pomysłem.

Zastanówmy się nad niesprawiedliwością listy obserwacyjnej potencjalnych terrorystów. W 2009 roku Gulet Mohamed, amerykański obywatel urodzony w Somalii[42], który w wieku trzech lat wyemigrował do Stanów Zjednoczonych, wyjechał na kilka miesięcy odwiedzić krewnych w ojczyźnie. Następnie przeniósł się do Kuwejtu, gdzie mieszkał u swego wuja i studiował język arabski.

20 grudnia 2010 roku Mohamed pojechał na lotnisko w Kuwejcie, żeby odnowić swoją wizę, tak jak to robił co trzy miesiące od czasu przyjazdu. Gdy przebywał na lotnisku, podeszło do niego dwóch mężczyzn, zakuło w kajdanki, zawiązało oczy i zawiozło do miejsca o nieokreślonej lokalizacji. Mohamed, który miał w tym czasie osiemnaście lat, mówi, że przez ponad tydzień był torturowany, bity kijami i zmuszany do wielogodzinnego stania w miejscu; pewnego razu, gdy przywiązano mu ręce do belki na suficie, zemdlał. Wypytywano go o dowódcę wojsk, Anwara al-Awlakiego.

28 grudnia został przetransportowany do ośrodka deportacyjnego, gdzie odwiedzili go agenci FBI. Odmówił odpowiedzi na ich pytania. Wreszcie 16 stycznia 2011 roku kuwejccy urzędnicy zabrali go na lotnisko i wręczyli bilet do Stanów Zjednoczonych, który zakupiła mu jego rodzina. Jednak Mohamed nie został wpuszczony do samolotu, ponieważ znajdował się na liście osób z zakazem latania. Ostatecznie 21 stycznia zezwolono mu na wylot do domu. Ale od tej pory nie wolno mu podróżować tą drogą.

Za gehennę Mohameda przypuszczalnie odpowiedzialne są jego dane osobowe. Nie pozwolono mu jednak w nie wejrzeć. Rząd twierdzi, że powinien dochodzić odszkodowania na drodze skargi do Programu Odszkodowań Pasażerskich (TRIP) Departamentu Bezpieczeństwa Wewnętrznego[43]. Pasażerowie, którym odmówiono wstępu na pokład samolotu[44], mogą przedłożyć informację resortowi, a ten sprawdzi, czy nie doszło do pomyłki, np. ze względu na fakt posiadania nazwiska brzmiącego identycznie z nazwiskiem umieszczonym na liście obserwacyjnej. Jednak resort nie jest zobligowany do rozpatrywania

sprzeciwów od osób, które znalazły się na liście i wniosków o wycofanie z niej nazwiska[45]. W rzeczywistości Departament nigdy nie potwierdza ani nie zaprzecza czyjejś obecności na niej. Mohamed twierdzi, że przez odmówienie mu „zgodnego z konstytucją mechanizmu prawnego" zakwestionowania jego obecności na liście osób z zakazem latania, pozbawiono go konstytucyjnego prawa do właściwej procedury prawnej[46].

To najgorszy rodzaj nadużycia danych osobowych: Mohamed był torturowany i z nieznanych mu przyczyn do dzisiaj nie może wejść na pokład samolotu, a przy tym mówi mu się, że nie może odpowiedzieć na to, co mu się zarzuca, w sądzie. Nie wszystkie nadużycia danych osobowych są tak przerażające w skutkach, jak w przypadku Mohameda, ale jego sytuacja przypomina, jak ważne jest istnienie mechanizmów pozwalających ludziom na wgląd w te dane o nich, które mogą być wykorzystywane przeciwko nim.

Coraz bardziej widoczne są działania mające uczynić firmy odpowiedzialnymi za dane ich klientów. Unia Europejska wymaga, by różne podmioty umożliwiały obywatelom wgląd do przechowywanych informacji o nich[47]. W 2011 roku senatorowie John McCain i John Kerry zaproponowali przepisy[48] o ochronie prywatności w handlu, na podstawie których podmioty gromadzące dane o konsumentach musiałyby umożliwiać im dostęp do nich, ci z kolei mieliby prawo do ich usunięcia lub wycofania zgody na ich przetwarzanie przez podmioty trzecie. Jednak projektowi temu sprzeciwili się zarówno obrońcy prywatności[49], jak i brokerzy sprzedaży danych[50]. Prace nad nim zostały więc wstrzymane[51]. W 2012 roku administracja Obamy oświadczyła[52], że nie będzie czekać na zmiany w ustawie o prywatności zapowiadane przez Kongres. Zainicjowała starania zmierzające do tego, by branża brokerów danych samodzielnie wypracowała zasady zgodności z przepisami o prawie do prywatności, a także zaproponowała zasady dostępu konsumentów do danych o nich.

Jedną z najskuteczniejszych metod[53] przypisywania odpowiedzialności spółkom prowadzącym bazy danych, jest ustawa o rzetelnej informacji kredytowej (Fair Credit Reporting Act), która umożliwia ludziom dostęp, korektę i kwestionowanie informacji o nich, wykorzystywanych do ich oceny dla celów decyzji finansowych. Mimo więc, że mój raport historii kredytowej zawierał nieścisłości, łatwo mi było je sprostować. Każdy, kto

wykorzysta raport o mnie jako uzasadnienie odmowy zatrudnienia, kredytu czy ubezpieczenia, musi poinformować mnie o przyczynach leżących u podstaw tej decyzji i dać mi możliwości odwołania się.

Oczywiście prawo regulujące kwestie rzetelnej informacji kredytowej ma luki. Prostowanie danych zawarte w moim raporcie może okazać się trudne. Przepisy obejmują bowiem tylko pewnego rodzaju decyzje finansowe. Zbyt łatwo jest wielkim brokerom sprzedaży danych, którzy dysponują ogromnym *dossier* na temat ludzi, utrzymywać, że posiadane przez nich informacje nie podlegają ochronie. Instytucja ratingowa eBureau, która skategoryzowała mnie jako osobę bez matury, przekonuje, że jej oceny są wykorzystywane do „szacowania" ludzi dla celów marketingowych[54], a nie na potrzeby decyzji kredytowych i pożyczkowych, czy ustalania cen ubezpieczeń – co może sugerować, że jej oceny nie podlegają wspomnianym przepisom.

Federalna komisarz handlu Julie Brill walczyła o to, by rozszerzyć ochronę[55] na znacznie większy zakres danych – szczególnie jeśli chodzi o informacje, które wykorzystuje się do oceny tego, czy „cechuje nas zbyt duże ryzyko, by można było prowadzić z nami interesy" albo czy „pasujemy do konkretnych klubów, serwisów randkowych, szkół lub innych programów"[56]. Poprosiła brokerów danych o to, by dobrowolnie umożliwili ludziom dostęp do posiadanych informacji o nich, do ich sprostowania i wycofania zgody na przetwarzanie w celach marketingowych. Ale ponieważ Federalna Komisja Handlu nie ma mandatu, by szybko tworzyć przepisy – w odróżnieniu od Agencji Ochrony Środowiska – Brill może jedynie zachęcać branżę handlu danymi do samoregulacji; no chyba, że podmioty te w swych działaniach przekroczą pewne granice i naruszą ogólne przepisy zakazujące „dyskryminacji i wprowadzania w błąd".

W gospodarce informacyjnej przydałaby nam się Agencja Ochrony Informacji, która sprawowałaby nad nią nadzór, pilnując transparentności i odpowiedzialności procesów przechowywania i przetwarzania danych.

* * *

Jednak utworzenie Agencji Ochrony Informacji nie wystarczy do kontroli rządowej inwigilacji. Nie będzie też lekarstwem na problemy ludzi takich jak Gulet Mohamed.

Jeśli chodzi o monitoring rządowy[57], to gdy wynikają z niego korzyści dla społeczeństwa, mamy tendencję do usprawiedliwiania natarczywości dragnetów. Tolerujemy niespodziewane wizyty państwowych inspektorów w miejscach pracy. Zezwalamy policji na tworzenie blokad na drogach w poszukiwaniu pijanych kierowców. Czasem godzimy się na testy na obecność narkotyków w pracy.

Nie akceptujemy jednak dragnetów, które są zbyt inwazyjne jak na cele, którym służą. Nie zgadzamy się lotniskowe skanery, obnażające zarysy nagiego ludzkiego ciała[58]. Nie umieszczamy śledzących mikroczipów w skórze naszych dzieci[59], choć robimy to zwierzętom domowym. Nie umieszczamy kamer monitoringu w toaletach.

Domagamy się, aby rządowe sieci nie opierały się na dyskryminacji rasowej. W 2013 roku sędzia Shira Scheindlin z Federalnego Sądu Dystryktowego orzekła[60], że policja nowojorska naruszyła konstytucję, zarzucając dragnet rutynowych kontroli na młodych Afroamerykanów i Latynosów, którzy nie byli o nic podejrzewani. „Nikt nie powinien żyć w strachu przed tym, że zostanie zatrzymany, gdy wyjdzie z domu, by zajmować się swoimi sprawami", napisała.

Oczywiście, zdarza się, że w gorączce wojennej pozwalamy rządowym dragnetom pójść za daleko. W 1944 roku Sąd Najwyższy orzekł, że internowanie ponad 100 tys. Amerykanów japońskiego pochodzenia podczas II wojny światowej, było zgodne z prawem, ponieważ „niemożliwe było natychmiastowe rozróżnienie pomiędzy lojalnymi i nielojalnymi obywatelami"[61]. W płomiennym zdaniu odrębnym sędzia Frank Murphy napisał, że orzeczenie „wychodzi poza najdalszą krawędź konstytucyjnej władzy i wpada w obrzydliwą otchłań rasizmu".

Mimo to, pośród oczywistych pomyłek, w ostatnich latach sądom udało się ustanowić interesujący zestaw pytań, które należy zadać przy ocenianiu słuszności istnienia dragnetów:

- Czy inwazyjność dragnetu jest dopasowana do celu, jakiemu służy?
- Czy przynosi on korzyści społeczeństwu?
- Czy wpada on w obrzydliwą otchłań rasizmu (lub innego rodzaju uprzedzeń)?

Te w oczywisty sposób niejasne kryteria przypomniały mi o teście publicznym, którym posłużyłam się, próbując usprawiedliwić używanie fikcyjnej tożsamości. W tamtej sytuacji uznałam, że racjonalna jednostka znajdzie uzasadnienie dla moich kłamstw, jako że miały one ograniczony zakres, ich celem nie było szkodzenie innym i stanowiły próbę przywrócenia równowagi pewnej relacji. Teraz, na samym początku afery Edwarda Snowdena, opinia publiczna decydowała o tym, czy test przeszły dragnety Agencji Bezpieczeństwa Krajowego. Przypomina on o jednej z najskuteczniejszych taktyk ruchu ochrony środowiska. Każdego roku Agencja Ochrony Środowiska publikuje w swoim Spisie Toksycznych Emisji listę spółek odpowiedzialnych za najbardziej toksyczne zanieczyszczenia[62]. Jawność tej listy spowodowała, że firmy zaczęły konkurować o to, która przechowuje najmniej toksycznych zasobów. Rezultatem tego jest ograniczenie rozlewów, np. olejowych. „Nikt nie chce być wysoko na tej liście", mówi Lisa Heinzerling, profesor ochrony środowiska z Uniwersytetu Georgetown[63]. „To wielki sukces".

Zastanawiałam się, czy podobne naciski na zachowanie przejrzystości nie byłyby dobrym rozwiązaniem problemu rządowych dragnetów. Uważa tak Christopher Slobogin, profesor prawa z Uniwersytetu Vanderbilt[64], który szczegółowo badał państwowe sieci monitoringu. Wskazuje on, że sądy powinny delegalizować te dragnety, które nie mają umocowania w ustawach. „Przy jednoczesnym pozostawieniu sądom kontroli nad stosowaniem prawa dotyczącego rewizji i zajęć w indywidualnych przypadkach, umacnia to demokratyczne wartości... gdy chodzi o rewizję czy zajęcie aktywów grupy ludzi", napisał. Dodatkowo proponuje on, by sądy mogły ograniczać działanie dragnetów, gdy stają się zbyt inwazyjne alb dyskryminują pewne grupy.

Krótko mówiąc, twierdzi on, że rządowe dragnety nie mogą być tajne. Muszą pozostawać pod nadzorem albo ciała ustawodawczego, albo sądu.

* * *

Dragnety są co do zasady niesprawiedliwe. Z samej ich definicji wynika, że przechwytują one dane o wszystkich: zarówno o podejrzanych jak i niewinnych. W ten sposób budują kulturę strachu – w której ludzie tacy jak Sharon Gill i Bilal Ahmed boją się w internecie rozmawiać o swoich problemach emocjonalnych, a Yasir Afifi zrywa z kolegą wypisującym

głupoty.

No tak, ale życie w ogóle jest niesprawiedliwe. Rodzi się więc pytanie: jakiego rodzaju niesprawiedliwość jest akceptowalna? Tolerujemy brak sprawiedliwości społecznej. Niektórzy ludzie są bogaci; inni biedni. Niektóre dzieci chodzą do dobrych szkół publicznych; inne chodzą do okropnych szkół publicznych. Niektórzy ludzie mieszkają blisko parków i zieleni; inni żyją w miejscach oddalonych od zielonych przestrzeni. Istnieje jednak niesprawiedliwość, na którą nie wyrażamy zgody. Nie tolerujemy ludzi, którzy kradną i którym uchodzi to na sucho. Nie tolerujemy łapownictwa. Nie tolerujemy firm, które sprzedają produkty krzywdzące ludzi.

Nasze poczucie sprawiedliwości ewoluowało latami. Kiedyś myśleliśmy, że sprawiedliwe jest, by dzieci pracowały całe dnie przy liniach montażowych. Później zmieniliśmy zdanie. Uważaliśmy, że usprawiedliwione jest zanieczyszczanie rzek i powietrza przez fabryki. Ale także w tej sprawie mamy już inny pogląd. Sądziliśmy, że dozwolone jest pozostawianie kupy naszego psa na chodniku. To już przeszłość. Doszliśmy do takich rozstrzygnięć jako członkowie społeczeństwa obywatelskiego.

Co do dragnetów, zauważyliśmy już, że w przypadku informacji kredytowej skuteczne są przejrzystość i odpowiedzialność. Przyjrzeliśmy się kryteriom, jakie stosują sędziowie do oceny zasadności dragnetów. Nawiązując do testu publicznego, moglibyśmy stworzyć zestawienie sześciu pytań, które powinny zostać zadane przy projektowaniu każdej sieci monitoringu:

- Czy dragnet daje ludziom prawo dostępu, sprostowania i wycofania ich danych?
- Czy twórcy dragnetu mogą być pociągnięci do odpowiedzialności za sposób, w jaki wykorzystują dane?
- Czy dragnet nie jest zbyt inwazyjny względem celu, któremu służy?
- Czy przynosi społeczeństwu korzyści?
- Czy jego założenia są rasistowskie (lub służą innym uprzedzeniom)?
- Czy obroni się, gdy zostanie poddany wnikliwej analizie?

Przez zadawanie tych pytań w odniesieniu do każdego dragnetu będzie

można, mam nadzieję, odróżnić masowy monitoring, który jest nie do przyjęcia od tego, na który możemy się zgodzić. Pewne istniejące współcześnie dragnety, wykorzystujące zaawansowane technologie, z pewnością nie przeszłyby tego testu. Zwróćcie uwagę na śledzenie w internecie i sieciach handlowych. Rejestrowanie każdego naszego kliknięcia myszką i śledzenie telefonów klientów podczas zakupów w sklepie to metody zbyt inwazyjne względem stosunkowo błahego celu, jakim jest ułatwienie prowadzenia działań promocyjnych. Dragnety te nie pozwalają na zgłaszanie reklamacji czy uzyskiwanie rekompensaty.

A dragnety Agencji Bezpieczeństwa Krajowego (NSA)? Agencja musi dostarczać przekonywających dowodów, że na inwigilowaniu niewinnych Amerykanów społeczeństwo skorzystało wystarczająco dużo, by uzasadniało to jej natarczywość. Poszczególne osoby nie mają dostępu do swoich danych, a o legalności dragnetów decyduje tajny sąd.

Albo zastanówcie się nad infiltracją meczetów i muzułmańskiej społeczności prowadzoną przez policję nowojorską. To ewidentne, że ów dragnet wpadł w odrażającą otchłań rasizmu.

Są jednak sieci, które mogłyby przejść nasz test. Wykorzystywanie przez policję kamer monitoringu i fotografowanie tablic rejestracyjnych może przynieść społeczeństwu wystarczająco dużo korzyści, by usprawiedliwić ich natarczywość. Podejrzani mają zresztą możliwość zakwestionowania nagrania w sądzie. Brokerzy sprzedaży danych, którzy ponoszą odpowiedzialność za sposób ich przechowywania i przetwarzania – podobnie jak biura informacji kredytowej – także mogliby przejść test.

Nawet freestylowcom, takim jak Google czy Facebook, udałoby się go zdać, gdyby ograniczyli inwazyjność śledzenia, umożliwili użytkownikom prawdziwy dostęp do informacji o nich oraz wzięli odpowiedzialność za dane, którymi dzielą się z innymi.

Moja lista niesprawiedliwości jest z całą pewnością niedoskonała. Ale to tylko próba wytyczenia drogi pomiędzy tymi, którzy proszą, byśmy przekazali im wszystkie nasze dane i „natychmiast o tym zapomnieli", a tymi którzy przekonują, że w ten sposób rzucamy się na szyny tuż przed rozpędzony pociąg (gospodarkę opartą na danych). Ludzie, także ja, nie chcą pozbawiać się korzyści, jakie niesie ze sobą gospodarka informacyjna – jej map, faktów dostępnych za dotknięciem palców, zdolności do natychmiastowego łączenia się z drugą osobą, przebywającą gdzieś w świecie. Ale też nikt z nas nie powinien ot tak rezygnować z ochrony swoich danych, nie mając pewności, że nie wrócą kiedyś do nas, uderzając

w nas rykoszetem.

Nie musieliśmy porzucić gospodarki przemysłowej, żeby ograniczyć zanieczyszczenie środowiska. Po prostu poprosiliśmy trucicieli, żeby byli bardziej odpowiedzialni za swoje działania. Ustanowiliśmy prawo, powołaliśmy nową agencję rządową i wymusiliśmy na nich przejrzystość działania. Podobnie nie musimy kończyć z gospodarką informacyjną. Powinniśmy jednak skłonić tych, którzy gromadzą dane o nas, by umożliwili nam wgląd w te informacje, i żądać, by ponosili odpowiedzialność za każdą szkodę będącą wynikiem ich nadużycia.

Jeśli uda się nam odnaleźć złoty środek, możemy żyć w nowym, jasnym świecie, w którym prywatność nie będzie już celem samym w sobie. Możemy uznać, że prywatność była jedynie tarczą, którą trzymaliśmy, by chronić się przed szkodami. Jeśli będziemy w stanie ograniczyć straty, będziemy mogli odsunąć tarczę na tyle, by moje dzieci mogły umieszczać swoje filmiki na YouTube, Sharon i Bilal mogli z powrotem rozmawiać na forum medycznym PatientsLikeMe, a Yasir i Chalid – odzyskać swoją przyjaźń z dzieciństwa. To byłby świat, który chciałabym zostawić swoim dzieciom.

PODZIĘKOWANIA

Książki z dziedziny literatury faktu to projekty, które promuje się zwykle jako wynik pracy jednostki. Jednak ta publikacja zawdzięcza swe istnienie całej grupie ludzi, można nawet powiedzieć, że współkonspiratorów.

Naturalnie, należą do niej przede wszystkim członkowie mojej rodziny. Mąż i dzieci byli łaskawi brać udział w doświadczeniach z prywatnością i cierpliwie znosili moją niekończącą się pracę nad tym projektem. Moi rodzice, brat oraz jego narzeczona dostarczyli mi najważniejszego wsparcia w kluczowych momentach procesu pisania.

Teściowie dali mi niekończącą się miłość i wsparcie.

Moja definicja rodziny obejmuje także kobiety, które prowadziły mnie za rękę na każdym etapie tej podróży i bez których z pewnością bym się zgubiła. Chciałyby, aby znano je jako Hedy Lamarr, Hildy Johnson oraz George Eliot. Niech Bóg błogosławi mojej rodzinie i niech będzie otoczona miłością.

Miałam także oparcie w grupie współkonspiratorów z redakcji „Wall Street Journal" – tych dawnych i tych obecnych, którzy dołączyli do mnie w tej długiej, nieprawdopodobnej podróży – której niniejsza książka stanowi zaledwie fragment. Nic by się nie udało, gdyby nie Jennifer Valentino-DeVries, Ashkan Soltani, Emily Steel, Jesse Pesta, Jeremy Singer-Vine oraz Scott Thurm. Od samego początku moją wizję podsycali Kevin Delaney, Rebecca Blumenstein, Mike Williams, oraz Alix Freedman, którym także przesyłam specjalne podziękowania.

Jedną z najprzyjemniejszych niespodzianek w tej podróży było poznanie otwartej, ciepłej społeczności badaczy, którzy od lat pracowali nad poruszaniem się w tym wyłaniającym się dopiero cyfrowym krajobrazie i którzy chętnie dzielili się ze mną swoimi odkryciami. Dużo zawdzięczam ich zbiorowej pracy. W szczególności chciałabym wyrazić wdzięczność Ryanowi Calo, Danielle Citron oraz Danielowi Weitznerowi, którzy byli

pierwszymi czytelnikami tej książki i którzy dostarczyli niezbędnych uwag do jej szkicu. Jestem także dłużniczką Julie Brill, Paula Ohma, Alessandra Acquisti, Susan Freiwald, Katherine Strandburg, Chrisa Hoofnagle'a, Rachel Levinson-Waldman, Christophera Slobogina, Gary'ego Bruce'e oraz Lisy Sotto, których wsparcie i rada miały szczególny wpływ na mój sposób myślenia.

Ciepło powitała mnie także rozsiana po świecie społeczność hakerska. Bez dorobku tych ludzi nie wiedzielibyśmy, dokąd trafiają nasze dane i nie mielibyśmy narzędzi, by móc ich strzec. Do tych, którzy prowadzili mnie w mojej pracy i w moim myśleniu należą: Ashkan Soltani, Dave Campbell, Jacob Appelbaum, Brian Kennish, Jon Callas, Michael Tiffany, Mike Perry, Christopher Soghoian, Dan Kaminsky oraz Jonathan Mayer.

Szczególne podziękowania pragnę przekazać Johnowi Gilmore'owi, który był moim pierwszym oknem do tego świata już tyle lat temu, i którego historię wciąż mam nadzieję opowiedzieć w pełni, tak jak na to zasługuje.

Miałam szczęście, że moja ekipa wydawnicza miała doskonałych liderów. Mój agent, Todd Shuster, okazał się wybawcą na wielu frontach – przede wszystkim zachęcając mnie, by uczynić książkę bardziej osobistą. Zespół wydawnictwa Henry Holt & Company, czyli Stephen Rubin, Paul Golob, Emi Ikkanda, Patricia Eisemann, Maggie Richards oraz Leslie Brandon – nie szczędzili mi słów zachęty i swych cennych uwag. Nie mogę nachwalić się pracy moich analityków Lauren Kirchner, Courtney Schley, Neeny Lall oraz Bena Kalina, który weryfikował dla mnie fakty. Zarwali przy tym projekcie wiele nocy, podzielając moją obsesję na punkcie szczegółu.

I wreszcie, chciałabym podziękować każdemu, kto opowiedział mi swoją osobistą historię – w szczególności Bilalowi Ahmedowi, Sharon Gill, Yasirowi Afifiem oraz Billowi Binneyowi. To nie lada sprawa powierzyć swoją narrację komuś innemu. Mam nadzieję, że sprostałam zadaniu odmalowania ich historii w sposób uczciwy i odpowiednio wrażliwy.

Przypisy tłumacza

[*1] Bazy danych dragnet to elektroniczne bazy danych dozoru amerykańskich obywateli, generowane w oparciu o technologię rozwijaną w ramach projektu Dragnet, o którym po raz pierwszy poinformowano w 2005 roku, a więcej informacji o nim ujawnił dopiero w 2013 roku Edward Snowden – przyp. Kurhaus.
[*2] Edward Snowden – były współpracownik NSA, jeden z najsłynniejszych „sygnalistów", obecnie uciekinier przebywający prawdopodobnie w Rosji. Pracując w Centrum Operacji Bezpieczeństwa Regionalnego NSA na Hawajach miał dostęp do poufnych informacji agencji. W 2013 roku ujawnił mediom nadużycia amerykańskich i brytyjskich służb bezpieczeństwa, polegające na masowym inwigilowaniu polityków i zwykłych obywateli – przyp. Kurhaus.
[*3] Więcej: https://en.wikipedia.org/wiki/No_Fly_List
[*4] Counter Intelligence Program – czyli Program Kontrwywiadowczy – miał na celu infiltrację i zakłócenia funkcjonowania amerykańskich organizacji politycznych, takich jak Socjalistyczna Partia Robotników (Socialist Workers Party), Czarne Pantery, Ku Klux Klan czy Konferencja Przywódców Chrześcijan z Południa (Southern Chrisian Leadership Conference) Martina Luthera Kinga. Właściwie rozpoczęto go pod koniec lat 50. – przyp. Kurhaus.
[*5] Ciekawie na ten temat pisał w 2014 roku Will Pavia z dziennika „The Times". Polski przekład: http://www.polskatimes.pl/artykul/3657254, zabij-sie-bydlaku-fbi-szantazowala-martina-luthera-kinga-chciala-sklonic-go-do-samobojstwa, id, t.html – przyp. Kurhaus.
[*6] Lowe's to sieć hipermarketów specjalizująca się w sprzedaży narzędzi, materiałów budowlanych itd., podobnie jak jej konkurent, firma Home Depot, którą autorka także wspomina – przyp. Kurhaus.
[*7] Chodzi prawdopodobnie o wybory w 2008 roku, w których Bentsen ubiegał się o fotel wiceprezydenta jako kandydat Partii Demokratycznej, u boku kandydata na prezydenta – Michaela Dukakisa – przyp. Kurhaus.

[*8] M. Foucault (1993, wyd. pol), s. 242
[*9] Patriot Act to uchwalona w 2001 roku po zamachach 11 września ustawa, umożliwiająca organom ścigania przetrzymywanie przez nieokreślony czas (bez konieczności uzyskania zgody sądu) obywateli nieamerykańskich, podejrzewanych o to, że mogą stanowić zagrożenie dla bezpieczeństwa narodowego – przyp. Kurhaus.
[*10] Stosowane w oryginale *computer security* jest po polsku określane zamiennie jako cyberbezpieczeństwo, bezpieczeństwo cyfrowe, rzadziej komputerowe – przyp. tłum.
[*11] Angwin J., *Stealing MySpace: The Battle to Control the Most Popular Website in America*, Random House, 2009 – przyp. Kurhaus.
[*12] Gra podobna do hokeja na trawie z użyciem rakiet zamiast kijów – przyp. tłum.
[*13] Po polsku oznacza to: ZbiórHistoriiDyplomacji-od_1966-Do-DzisiejszegoDnia# – przyp. tłum.
[*14] Amerykański zespół rockowy – przyp. tłum.
[*15] Tytuł utworu zespołu U2 – przyp. tłum.
[*16] *Wardriving* to wyszukiwanie sieci bezprzewodowych w danej okolicy – przyp. Kurhaus.
[*17] Tzw. *red cups* to symbol amerykańskich „domówek", czyli imprez suto zakrapianych alkoholem – przyp. Kurhaus.
[*18] W wolnym tłumaczeniu oznacza to: „Dostrzegaj zawsze pozytywne strony życia" – przyp. Kurhaus.
[*19] Po polsku: „Tragedia wspólnego pastwiska" – przyp. Kurhaus.
[*20] Gra słów. Angielskie słowo „surveillance", czyli „inwigilacja", pochodzi z języka francuskiego, w którym jest pisane tak samo i to samo oznacza. Nieistniejące słowo „sousveillance" wykorzystuje obecną w języku francuskim opozycję między przyimkami „sur", czyli „na", i „sous", czyli „pod" (przyp. tłum).

Przypisy

ROZDZIAŁ 1: ZHAKOWANI

[1] Sharon Gill w rozmowie z autorką, 12 lipca 2013.
[2] Bilal Ahmed w rozmowie z autorką, 27 stycznia 2013.
[3] Sharon Gill w rozmowie z autorką, 12 lipca 2013.
[4] J. Angwin, S. Stecklow, „*Scrapers* Dig Deep for Data on Web", „Wall Street Journal", 12 października 2010. Dostępny w internecie: http://online.wsj.com/article/SB10001424052748703358504575544381288117
[5] B. Heywood, „Transparency, Openness and Privacy", blog: *The Value of Openness*, 20 maja 2010, http://blog.patientslikeme.com/2010/05/20/bentransparencymessage/.
[6] Angwin, Stecklow, „*Scrapers* Dig Deep".
[7] K. Zetter, „Prosecutors Drop Plans to Appeal Lori Drew Case", blog: *Threat Level*, Wired.com, 20 listopada 2009, http://www.wired.com/threatlevel/2009/11/lori-drew-appeal/.
[8] Merriam-Webster Online, http://www.merriam-webster.com/dictionary/privacy.
[9] Szersze spojrzenie na lukę pomiędzy śledzeniem akceptowalnym i nieakceptowalnym społecznie, zob. H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law School, Stanford 2010.
[10] Więcej uwag na temat problemów, które stwarza masowe śledzenie, zob. S. Freiwald, „First Principles of Communications Privacy", „Stanford Technology Law Review" 2007, nr 3. Dostępny w internecie: http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf. Także: Ch. Slobogin, „Government Dragnets" (praca naukowa nr 10-25), Vanderbilt Law School, http://ssrn.com/abstract=1640108.
[11] „Moore's Law at 40: Happy Birthday", „Economist", 23 marca 2005. Dostępny w internecie: http://www.economist.com/node/3798505.
[12] J. Angwin, J. Valentino-DeVries, „New Tracking Frontier: Your License Plates", „Wall Street Journal", 29 września 2012. Dostępny w internecie:

http://online.wsj.com/article/SB10000872396390443995604578004723603
[13] „NSA Inspector General Report on Email and Internet Data Collection Under Stellar Wind – Full Document", „Guardian", 27 czerwca 2013. Dostępny w internecie: http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.
[14] „Which Governments Are in the Market", blog: *The Surveillance Catalog*, WSJ.com, 7 lutego 2012, http://projects.wsj.com/surveillance-catalog/attendees/.
[15] J. Valentino-Devries, J. Angwin, S. Stecklow, „Document Trove Exposes Surveillance Methods", „Wall Street Journal", 19 listopada 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203611404577044192607407
[16] A. Pasztor, J. Emshwiller, „Drone Use Takes Off on the Home Front", „Wall Street Journal", 21 kwietnia 2012. Dostępny w internecie: http://online.wsj.com/article/SB10001424052702304331204577354331959335
[17] J. Angwin, S. Thurm, „Judges Weigh Phone Tracking", „Wall Street Journal", 9 listopada 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203733504577024092345458
[18] Angwin, Valentino-DeVries, „New Tracking Frontier: Your License Plates".
[19] M. Dano, „The Sale of (Anonymous) Wireless Users' Location and Behavior Is Already Big Business", internetowy newsletter: „FierceWireless", 22 maja 2013, www.fiercewireless.com/story/sale-anonymous-wireless-users-location-and-behavior-already-big-business/2013-05-23.
[20] Euclid Analytics, „Euclid Analytics – How It Works", http://euclidanalytics.com/product/how oraz S. Clifford, Q Hardy, „Attention, Shoppers: Store Is Tracking Your Cell", „New York Times", 14 lipca 2013. Dostępny w internecie: http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?hp.
[21] P. Dixon, „Privacy Implications of the New Digital Signage Networks", World Privacy Forum, 27 stycznia 2010. Dostępny w internecie: http://www.ftc.gov/os/comments/privacyroundtable/544506-00112.pdf.
[22] J. Valentino-DeVries, J. Singer-Vine, „They Know What You're Shopping For", „Wall Street Journal", 7 grudnia 2012. Dostępny

w internecie:
http://online.wsj.com/article/SB10001424127887324784404578143144132736214
[23] J. Angwin, „The Web's New Gold Mine: Your Secrets", „Wall Street Journal", 30 lipca 2010. Dostępny w internecie:
http://online.wsj.com/article/SB10001424052748703940904575395073512989
[24] E. Steel, J. Angwin, „Device Raises Fear of Facial Profiling", „Wall Street Journal", 13. lipca 2011. Dostępny w internecie:
http://online.wsj.com/article/SB10001424052702303678704576440253307984
[25] K. Barry, „Insurance Company Telematics Trade Perks for Privacy", „Wired", 19 sierpnia 2011. Dostępny w internecie:
http://www.wired.com/autopia/2011/08/insurance-company-telematics-trade-perks-for-privacy/.
[26] J. Marston, J. Hart, „Should Consumers Participate in Their Utility's Smart-Meter Program?", „Wall Street Journal", 12 kwietnia 2013. Dostępny w internecie:
http://online.wsj.com/article/SB10001424127887323415304578368683701371
[27] „Glass", Google Inc., http://www.google.com/glass/start/.
[28] „Protecting Your Answers", Biuro Spisów Ludności Stanów Zjednoczonych, 2010,
https://www.census.gov/2010census/about/protect.php.
[29] W. Seltzer, M. Anderson, „Government Statistics and Individual Safety: Revisiting the Historical Record of Disclosure, Harm, and Risk", praca przygotowana jako prezentacja na warsztaty pt. „Access to Research Data: Assessing Risks and Opportunities" zorganizowane przez Panel on Confidential Data Access for Research Purposes, Committee on National Statistics (CNSTAT), National Academies, Waszyngton, 16-17 października 2003. Dostępny w internecie:
https://pantherfile.uwm.edu/margo/www/govstat/WS-MAcnstat.pdf
[30] J.R. Minkel, „Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II", „Scientific American", 30 marca 2007,
https://www.scientificamerican.com/article.cfm? id=confi rmed-the-us-census-b&sc=I100322.
[31] L. Clemetson, „Homeland Security Given Data on Arab-Americans", „New York Times", 30 lipca 2004. Dostępny w internecie:
http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.
[32] R.C. Bonner, Komisarz Urzędu Celnego i Ochrony Granic Stanów Zjednoczonych, „Policy for Requesting Information of a Sensitive Nature

from the Census Bureau" (notatka), 9 sierpnia 2004, https://epic.org/privacy/census/foia/policy.pdf.
[33] W. Seltzer, „On the Use of Population Data Systems to Target Vulnerable Population Subgroups for Human Rights Abuses", „Coyuntura Social" 2005, nr 32 (lipiec), s. 3–44. Dostępny w internecie: https://pantherfile.uwm.edu/margo/www/govstat/CoyunturaSocialpaper2(
[34] E.P. Kraly, J. McQuilton, „The ‚Protection' of Aborigines in Colonial and Early Federation Australia: The Role of Population Data Systems", „Population, Space and Place" 2005, nr 11 s. 225–50, Dostępny w internecie: http://ro.uow.edu.au/era/172/.
[35] A.J. Christopher, „‚To Define the Indefinable': Population Classification and the Census in South Africa" 2002, nr 4, s. 401–8.
[36] Sprawa Prokuratura kontra Jean-Paul Akayesu, sygn. ICTR-96-4, orzeczenie z dnia 2 września 1998, http://www.humanrights.is/the-human-rights-project/humanrightscasesandmaterials/cases/internationalcases/tribunalfor
[37] W. Seltzer, „Population Statistics, the Holocaust, and the Nuremberg Trials", „Population and Development Review" 1998, nr 3 (wrzesień), s. 511–52. Dostępny w internecie: https://pantherfile.uwm.edu/margo/www/govstat/seltzer.pdf.
[38] „Dr. Martin Luther King, Jr., Case Study" (raport końcowy) Select Committee to Study Governmental Operations with Respect to Intelligence Activities United States Senate, 23 kwietnia 1976, http://www.aarclibrary.org/publib/church/reports/book3/pdf/ChurchB32M
[39] RSA, „Anatomy of an Attack", blog: *Speaking of Security: The Official RSA Blog and Podcast*, 1 kwietnia 2011, http://blogs.rsa.com/anatomy-of-an-attack/.
[40] Sprawa Helen Remsburg, zarządca spadku po Amy Lynn Boyer kontra Docusearch, Inc., sygn. CV-00-211-B, Sąd Dystryktowy dla Dystryktu New Hampshire, 2002, http://www.courts.state.nh.us/supreme/opinions/2003/remsb017.htm.
[41] H. Ramer, „Mother of Slain Woman Settles Lawsuit Against Info-Broker", „USA Today", 10 marca 2004. Dostępny w internecie: http://usatoday30.usatoday.com/tech/news/internetprivacy/2004-03-10-boyer-suit-settledx.htm? POE=TECISVA.
[42] Strona internetowa Docusearch, docusearch.com.
[43] Sprawa Rembsburg (Boyer) kontra Docusearch, Inc.
[44] Intelius.com.

[45] W 2010 roku: A. Furillo, „Wife of Slain Offi cer Satisfied with Murder Verdict Against Vue", blog: *Sacto 911*, Sacbee.com, 29 września 2010, http://blogs.sacbee.com/crime/archives/2010/09/chu-vue-found-g.html.
[46] K. Minugh, „Former Deputy Sought Data on Slain Man, Trial Is Told", „Sacramento Bee, 17 sierpnia 2010.
[47] Tamże.
[48] A. Furillo, „Cell Phone Calls Place Vues near Slaying Victim", „Sacramento Bee", 24 sierpnia 2010.
[49] A. Furillo, „Ex-Deputy Gets Life for Arranging Correctional Offi cer's Murder", „Sacramento Bee, 29 listopada 2010. Dostępny w internecie: http://blogs.sacbee.com/crime/archives/2010/11/ex-deputy-gets.html.
[50] Departament Sprawiedliwości Stanów Zjednoczonych, „Former Department of Commerce Agent Indicted for Making a False Statement and Exceeding Authorized Access to a Government Database" (komunikat prasowy), 19 września 2007, http://www.justice.gov/criminal/cybercrime/press-releases/2007/robinsonIndict.htm.
[51] Srawa Stany Zjednoczone konta Benjamin Robinson, nr CR-07-00596 (N.D. Cal., 2001), http://ia600500.us.archive.org/11/items/gov.uscourts.cand.195976/gov.uscourts.cand.195976.1.0.pdf.
[52] Tamże.
[53] „The U.S. Electronic Passport Frequently Asked Questions", Travel.State.Gov, Biuro Spraw Konsularnych Departamentu Stanów Zjednoczonych, http://travel.state.gov/passport/passport 2788.html.
[54] „FAQ on RFID and RFID Privacy", RSA Laboratories, http://www.emc.com/emc-plus/rsa-labs/research-areas/faq-on-rfid-and-rfid-privacy.htm#4 [link niedostępny; ostatni dostęp: 8.09.2013].
[55] Sprawa Steve Hernandez kontra Northside Independent School District, sygn. SA-12-Ca-1113-OG, Sąd Dystryktowy Stanów Zjednoczonych dla Zachodniego Dystryktu Teksasu, 2013, https://www.rutherford.org/files_images/general/01-08-2013HernandezRuling.pdf.
[56] M. Del Barco, „California Law Outlaws RFID Implant Mandate", National Public Radio, 1 stycznia 2008, http://www.npr.org/templates/transcript/transcript.php?storyId=17762244.

[57] Angwin, Thurm, „Judges Weigh Phone Tracking".
[58] S. Thurm, J. Scheck, „Police Respond to WSJ Survey", „Wall Street Journal", 8 listopada 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203733504577024283882878
[59] Angwin, Thurm, „Judges Weigh Phone Tracking".
[60] A. Troianovski, „Phone Firms Sell Data on Customers", „Wall Street Journal", 21 maja 2013. Dostępny w internecie: http://online.wsj.com/article/SB10001424127887323463704578497153556847
[61] W. Bender, „Webcam Uproar Figure Decries ‚Unjust' Rumors", „Philadelphia Inquirer", 25 lutego 2010, http://articles.philly.com/2010-02-25/news/24956421webcam-blake-robbins-laptops.
[62] M.T. Moore, „Pa. School District's Webcam Surveillance Focus of Suit", „USA Today", 5 maja 2010, http://usatoday30.usatoday.com/tech/news/surveillance/2010-05-02-school-spyN.htm? loc=interstitialskip.
[63] W. Richey, „Did School Use Laptops to Spy on Students? Feds Won't Press Charges", „Christian Science Monitor", 17 sierpnia 2010, http://www.csmonitor.com/USA/Justice/2010/0817/Did-school-use-laptops-to-spy-on-students-Feds-won-t-press-charges.
[64] J.P. Martin, „Lower Merion Schools Hit with New Webcam Spying Suit", „Philadelphia Inquirer", 9 czerwca 2011, http://articles.philly.com/2011-06-09/news/29638824 1blake-robbins-jalil-hasan-new-webcam.
[65] Tamże.
[66] Sprawa Levin kontra Lower Merion School District, sygn. 11:3642, Sąd Dystryktowy Stanów Zjednoczonych dla Wschodniego Dystryktu Pensylwanii, 2011.
[67] J.P. Martin, „Lower Merion Settles Another Webcam Lawsuit", „Philadelphia Inquirer, 28 grudnia 2011, http://articles.philly.com/2011-12-28/news/30565544 1blake-robbins-lower-merion-school-district-school-issued-laptop.
[68] Notatki z: Lower Merion School Board Business Meeting, 16 sierpnia 2010, http://www.lmsd.org/data/files/gallery/BoardMeetingMinutes/BOSD Minutes100816.pdf.
[69] „Who's Watching: Video Camera Surveillance in New York City and the Need for Public Oversight", New York Civil Liberties Union, jesień 2006, http://www.nyclu.org/pdfs/surveillancecamsreport121306.pdf.

[70] B. Palmer, „Big Apple Is Watching You", „Slate", 3 maja 2010, http://www.slate.com/articles/newsandpolitics/explainer/2010/05/bigapple
[71] CHS X-Files, „Capitol Hill Drone Pilot Spotted, Glowing Orbs, Phone Thief on Wheels, „blog: *Capitol Hill Seattle*, 8 maja 2013. Dostępny w internecie: http://www.capitolhillseattle.com/2013/05/chs-x-files-capitol-hill-drone-pilot-spotted-glowing-orbs-phone-thief-on-wheels/.
[72] N. Anderson, „Meet the Men Who Spy on Women Through Their Webcams", blog: *Ars Technica*, 10 marca 2013, http://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/.
[73] Federalne Biuro Śledcze, „Orange County Man Who Admitted Hacking into Personal Computers Sentenced to Six Years in Federal Prison for ‚Sextortion' of Women and Teenage Girls" (komunikat prasowy), 1 września 2011, https://www.fbi.gov/losangeles/press-releases/2011/orange-county-man-who-admitted-hacking-into-personal-computers-sentenced-to-six-years-in-federal-prison-for-sextortion-of-women-and-teenage-girls.
[74] N. Bilton, „At Google Conference, Cameras Even in the Bathroom", blog: *Bits*, NYTimes.com, 17 maja 2013, http://bits.blogs.nytimes.com/2013/05/17/at-google-conference-even-cameras-in-the-bathroom/.
[75] R. Scoble, „My Two-Week Review of Google Glass", post na Google+, 27 kwietnia 2013, https://plus.google.com/+Scobleizer/posts/ZLV9GdmkRzS.
[76] G.A. Fowler, „When the Most Personal Secrets Get Outed on Facebook", „Wall Street Journal", 13 października 2012. Dostępny w internecie: http://online.wsj.com/article/SB10000872396390444165804578008740578
[77] S. Shane, S.G. Stolberg, „A Brilliant Career with a Meteoric Rise and an Abrupt Fall", „New York Times", 10 listopada 2012. Dostępny w internecie: https://www.nytimes.com/2012/11/11/us/david-petraeus-seen-as-an-invincible-cia-director-self-destructs.html?ref=davidhpetraeus&r=0.
[78] Sprawa Stany Zjednoczone kontra John Kiriakou, sygn. 1:12-CR-127, Sąd Dystryktowy Stanów Zjednoczonych dla Wschodniego Dystryktu Wirginii, 2012, https://www.fas.org/sgp/jud/kiriakou/indict.pdf.
[79] Sprawa Stany Zjednoczone kontra John Kiriakou, https://www.fas.org/sgp/jud/kiriakou/012513-judgment.pdf.

[80] „Copyright Trolls", Electronic Frontier Foundation, https://www.eff.org/issues/copyright-trolls.
[81] M. Zimmerman, „Fifth Circuit Upholds Sanctions Against Copyright Troll Attorney", blog: *Deeplinks*, Electronic Frontier Foundation, 12 lipca 2012, https://www.eff.org/deeplinks/2012/07/fifth-circuit-upholds-sanctions-award-against-copyright-troll-attorney.
[82] Sprawa Mick Haig Productions kontra 670 użytkowników konta Evan Stone, sygn. 11-10977.
[83] M. Stoltz, „Prenda Law Is the Tip of the Iceberg", blog: *Deeplinks*, Electronic Frontier Foundation, 7 maja 2013, https://www.eff.org/deeplinks/2013/05/prenda-law-tip-iceberg.
[84] J. Suell, „Identity Theft 911" (podcast), http://www.idt911.com/KnowledgeCenter/VideoAndAudio/VideoAndAudia={498D6632-1D69-4FAA-8060-3BD63105D8E2}.
[85] J. Angwin, „The Fallacy of Identity Theft", blog: *Decoder*, WSJ.com, 13 października 2009, http://online.wsj.com/article/SB125537784669480983.html.
[86] Child and Family Services Improvement and Innovation Act, 2011, http://www.gpo.gov/fdsys/pkg/PLAW-112publ34/pdf/PLAW-112publ34.pdf.
[87] Federalna Komisja Handlu, „Consumer Sentinel Network Data Book", luty 2013.
[88] Steve Toporoff w rozmowie z autorką, 18 marca 2013.
[89] Biuro Prokutatora Generalnego Stanów Zjednoczonych dla Południowego Dystryktu Florydy, „South Florida Women Sentenced in Identity Theft Tax Refund Fraud Scheme Involving the Filing of Approximately 2,000 Fraudulent Tax Returns Seeking $11 Million Dollars in Refunds" (komunikat prasowy), 25 kwietnia 2013, http://www.justice.gov/usao/fls/PressReleases/130425-01.html.
[90] M. Masihy, „Hospital Identity Theft Found at Some South Florida Hospitals", NBC 6 South Florida, 14 marca 2013, http://www.nbcmiami.com/investigations/Hospital-Identity-TheftGrowing-Amid-South-Florida-Hospitals-197866811.html.
[91] „Data Loss Statistics", DataLoss DB, Open Security Foundation, 24 czerwca 2013, http://datalossdb.org/statistics.
[92] Federalna Komisja Handlu, „FTC Files Complaint Against Wyndham Hotels for Failure to Protect Consumers' Personal Information" (komunikat prasowy), 6 czerwca 2012,

http://www.ftc.gov/opa/2012/06/wyndham.shtm.
[93] Federalna Komisja Handlu kontra Wyndham, nr CV 12-1365-PHX-PGR (2012), http://ftc.gov/os/caselist/1023142/120809wyndhamcmpt.pdf.
[94] B. Kendall, „FTC Fires Back in Cybersecurity Case", blog: *Law Blog*, WSJ.com, 24 maja 2013, http://blogs.wsj.com/law/2013/05/24/ftc-fires-back-in-cybersecurity-case/.
[95] Aktywista Eli Pariser nazywa to zjawisko bańką filtrującą [ang. *filter bubble*]. E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Press, Nowy Jork 2011.
[96] L. Sweeney, „Discrimination in Online Ad Delivery" (dokument roboczy), Uniwersytet Harvarda, Cambridge, Massachusetts, 28 stycznia 2013, https://papers.ssrn.com/sol3/papers.cfm?abstractid=2208240.
[97] J. Angwin, „On Google, a Political Mystery That's All Numbers", „Wall Street Journal", 4 listopada 2012. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203347104578099122530085
[98] M. Abrams, „Guest Headnote: Boxing and Concepts of Harm", „Privacy and Data Security Law Journal", wrzesień 2009, nr 674, http://theprivacyprojects.org/wp-content/uploads/2009/08/PDSLJ-article.pdf.
[99] R. Calo, „Digital Market Manipulation" (badanie nr 2013-27), Szkoła Prawa Uniwersytetu Waszyngtonu, 15 sierpnia 2013, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309703.
[100] E. Steel, J. Angwin, „On the Web's Cutting Edge, Anonymity in Name Only", „Wall Street Journal", 3 sierpnia 2010. Dostępny w internecie: http://online.wsj.com/article/SB10001424052748703294904575385532109190
[101] J. Valentino-DeVries, J. Singer-Vine, A. Soltani, „Websites Vary Prices, Deals Based on Users' Information", „Wall Street Journal", 24 grudnia 2012. Dostępny w internecie: http://online.wsj.com/article/SB10001424127887323777204578189391813881
[102] K. Blumenthal, „How Banks, Marketers Aid Scams", „Wall Street Journal", 15 lipca 2009. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970204556804574260062522
[103] Federalna Komisja Handlu, „FTC Settlements Require Equifax to Forfeit Money Made by Allegedly Improperly Selling Information About Millions of Consumers Who Were Late on Their Mortgages" (komunikat prasowy), 10 października 2012, http://www.ftc.gov/opa/2012/10/equifaxdirect.shtm.

[104] Sprawa Stany Zjednoczone kontra Direct Lending Source, http://www.ftc.gov/os/caselist/1023000/121010directlendingcmpt.pdf.
[105] CV-2441DMS BLM oraz Kalifornijski Departament Sprawiedliwości, Biuro Prokutatora Generalnego i Ministra Sprawiedliwości, „Four Arrested, Five Wanted for Fleecing Hundreds of Homeowners Seeking Foreclosure Relief" (komunikat prasowy), 20 maja 2010, http://oag.ca.gov/news/press-releases/four-arrested-five-wanted-fleecing-hundreds-homeowners-seeking-foreclosure.
[106] Stowarzyszenie Marketingu Bezpośredniego, „Guidelines for Ethical Business Practices", wydanie poprawione, maj 2011, http://www.dmaresponsibility.org/Guidelines/.
[107] John Gass w rozmowie z autorką, 18 lutego 2013.
[108] Tamże
[109] Sprawa John H. Gass kontra Registrar of Motor Vehicles, Sąd Apelacyjncy stanu Massachusetts.
[110] John Gass w rozmowie z autorką, 18 lutego 2013.

ROZDZIAŁ 2: KRÓTKA HISTORIA ŚLEDZENIA

[1] William Binney w rozmowie z autorką, 24 maja 2012.
[2] „World Trade Center Fires Out", ABCNews.com, 19 grudnia 2001, http://abcnews.go.com/US/story? id=92066& page=1.
[3] „The Anthrax Attacks Remain Unsolved", „Wall Street Journal", 24 stycznia 2010. Dostępny w internecie: http://online.wsj.com/article/SB10001424052748704541004575011421223515
[4] T. Shorrock, „Obama's Crackdown on Whistleblowers", „Nation", 26 marca 2013. Dostępny w internecie: http://www.thenation.com/article/173521/obamas-crackdown-whistleblowers? page=0,1.
[5] William Binney w rozmowie za autorką, 24 maja 2012.
[6] Sprawa Jewel, Hepting, Hicks Knutzen i Walton kontra Agencja Bezpieczeństwa Krajowego, sygn. CV-08-04373-JSW, Sąd Dystryktowy Stanów Zjednoczonych dla Północnego Dystryktu Kalifornii, 2012, zeznania Williama Binneya, 28 września 2012.
[7] „Companies Won, Investors Lost", „Wall Street Journal", The Intelligent Investor, 10 marca 2010, http://online.wsj.com/article/SB10001424052748704145904575111952082691
[8] Christopher Slobogin, „Government Dragnets" (praca naukowa nr 10–

37), Public Law & Legal Theory, Vanderbilt University Law School, Nashville, Tennessee, 2010.
[9] J. Otis, „Against Writs of Assistance", transkrypcja przemówienia, Boston, 24 lutego 1761. Dostępny w internecie: http://www.constitution.org/bor/otisagainstwrits.htm.
[10] Konstytucja Stanów Zjednoczonych, Czwarta Poprawka.
[11] Sprawa Floryda (stan) kontra Riley, sygn. 488 U.S. 445, 1989, http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=488&page=445.
[12] Sprawa Stany Zjednoczone kontra Miller, sygn. 425 U.S. 435, 1976 oraz sprawa Smith kontra Maryland (stan), sygn. 442 U.S. 735, 1979.
[13] J. Valentino-DeVries, „How Technology Is Testing the Fourth Amendment", blog: *Digits*, WSJ.com, 21 września 2011, http://blogs.wsj.com/digits/2011/09/21/how-technology-is-testing-the-fourth-amendment/.
[14] „A Guardian Guide to Your Metadata", „Guardian", 12 czerwca 2013, http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance #meta=0000000.
[15] E. Perez, S. Gorman, „Phones Leave a Telltale Trail", „Wall Street Journal", 15 czerwca 2013, http://online.wsj.com/article/SB10001424127887324049504578545352803220
[16] S. Stellin, „The Border Is a Back Door for U.S. Device Searches", „New York Times", 9 września 2013, http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html? pagewanted=1&r=2&hp.
[17] Dekret prezydencki nr 12,333,3 C.F.R., 1981, http://www.archives.gov/federal-register/codification/executive-order/12333.html.
[18] „NSA Inspector General Report on Email and Internet Data Collection Under Stellar Wind – Full Document", „Guardian", 27 czerwca 2013, http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection; Albo: ST-09-0002 (dokument roboczy), Biuro Inspektora Generalnego, Agencja Bezpieczeństwa Krajowego, 19 marca 2009.
[19] J. Risen, E. Lichtblau, „Bush Lets U.S. Spy on Callers Without Courts", „New York Times", 16 grudnia 2005. Dostępny w internecie: http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.

[20] „Whistle-Blower Outs NSA Spy Room", „Wired", 7 kwietnia 2006. Dostępny w internecie: http://www.wired.com/science/discoveries/news/2006/04/70619
[21] M. Klein, „Whistle-Blower's Evidence, Uncut", „Wired", 22 maja 2006. Dostępny w internecie: http://www.wired.com/science/discoveries/news/2006/05/70944.
[22] L. Cauley, „NSA Has Massive Database of Americans' Phone Calls", „USA Today", 11 maja 2006. Dostępny w internecie: http://usatoday30.usatoday.com/news/washington/2006-05-10-nsax.htm? csp=34.
[23] E. Lichtblau, „Deal Reached in Congress to Rewrite Rules on Wiretapping", „New York Times", 20 czerwca 2008. Dostępny w internecie: http://www.nytimes.com/2008/06/20/washington/20fisacnd.html? r=0.
[24] „NSA Slides Explain the PRISM Data-Collection Program", „Washington Post", 6 czerwca 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [ostatnia aktualizacja: 10.07.2013].
[25] K. Zetter, „Yahoo Supplied Data to PRISM Only After Losing Scrappy FISA Fight", blog: *Threat Level*, Wired.com, 14 czerwca 2013, http://www.wired.com/threatlevel/2013/06/yahoo-failed-fisa-fight/.
[26] R.S. Litt, „Privacy, Technology and National Security: An Overview of Intelligence Collection", Remarks at Brookings Institution, Waszyngton, 19 lipca 2013, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.
[27] „Verizon Forced to Hand over Telephone Data – Full Court Ruling", „Guardian", 5 czerwca 2013, http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[28] E. O'Keefe, „Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program", blog: *Post Politics*, WashingtonPost.com, 6 czerwca 2013, http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/.
[29] K.L. Wainstein, „Memorandum for the Attorney General", 20 listopada 2007, http://s3. documentcloud.org/documents/717974/nsa-

memo.pdf.
[30] G. Greenwald, S. Ackerman, „How the NSA Is Still Harvesting Your Online Data", „Guardian", 27 czerwca 2013, http://www.guardian.co.uk/world/2013/jun/27/nsa-online-metadata-collection.
[31] Intelligence Budget Data, Związek Naukowców Amerykańskich, https://www.fas.org/irp/budget/index.html.
[32] Budget-in-Brief, Departamentu Bezpieczeństwa Krajowego, rok budżetowy 2012.
[33] Homeland Security Grant Program, Departamentu Bezpieczeństwa Krajowego, rok budżetowy 2012, http://www.fema.gov/fy-2012-homeland-security-grant-program.
[34] J. Angwin, J. Valentino-DeVries, „New Tracking Frontier: Your License Plates", „Wall Street Journal", 29 września 2012, http://online.wsj.com/article/SB10000872396390443995604578004723603
[35] „Federal Support for and Involvement in State and Local Fusion Centers", Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations, 3 października 2012, http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers.
[36] J. Angwin, S. Thurm, „Judges Weigh Phone Tracking", „Wall Street Journal", 9 listopada 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203733504577024092345458
[37] „The Attorney General's Guidelines for Domestic FBI Operations", 28 września 2008, http://www.justice.gov/ag/readingroom/guidelines.pdf.
[38] J. Angwin, „U.S. Terrorism Agency to Tap a Vast Database of Citizens", „Wall Street Journal". Dostępny w internecie: http://online.wsj.com/article/SB10001424127887324478304578171623040640
[39] S. Hamm, „The Education of Marc Andreessen", „BusinessWeek", 2 kwietnia 1998, http://www.businessweek.com/1998/15/topstory.htm; L.A. Lorek, „Investors Not Just Browsing: Netscape Navigator Stock Goes Public in One of Wall Street's Most Impressive Debuts", „Fort Lauderdale Sun-Sentinel", 10 sierpnia1995; oraz: K.M. Kristof, „Why Individual Investors Lose on IPOs", „Los Angeles Times", 10 sierpnia 1995, http://articles. latimes.com/1995-08-10/business/fi-336171_individual-investors.

[40] „The Golden Geeks", „Time", 19 lutego 1996. Dostępny w internecie: http://www.time.com/time/covers/0,16641,19960219,00.html.
[41] Sprawa Departament Sprawiedliwości Stanów Zjednoczonych kontra Microsoft, sygn. 253 F.3d 34, Sąd Apelacyjny USA dla Okręgu Dystryktu Kolumbii, 2001, https://law. justia.com/cases/federal/appellate-courts/F3/253/34/576095/.
[42] Microsoft Consent Decree Compliance Advisory, 1 sierpnia 2003, http://www.justice.gov/atr/cases/f201200/201205a.htm.
[43] M. Calore, „Internet Explorer Leaves Netscape in Its Wake", blog: *This Day in Tech Wired*, Wired.com, 28 września 1998, http://www.wired.com/thisdayintech/2009/09/0928ie-beats-netscape.
[44] T. Drapeau, „End of Support for Netscape Web Browsers", blog: *Netscape*, 28 grudnia 2007, http://blog. netscape.com/2007/12/28/end-of-support-for-netscape-web-browsers/.
[45] J. Tessler, „Tech Sector Mirrors Downfall of Silicon Valley General Economy", „San Jose Mercury News", 16 kwietnia 2001.
[46] V. O'Connell, „The Best Way to... Advertise", „Wall Street Journal", 21 listopada 2001.
[47] W. Taylor, „Online Ads Need to Get a Clue", ZDWire Small Business Advisor, 19 września 2001.
[48] „In re DoubleClick Inc. Privacy Litigation", Sąd Dystryktowy dla Południowego Dystryktu Nowego Jorku, 2001. Dostępny w internecie: https://cyber. harvard. edu/is02/readings/doubleclick.html.
[49] M. McIntire, „Clinton Backer's Ties to Powerful Cut Both Ways", „New York Times", 14 lipca 2007, http://www.nytimes.com/2007/07/14/us/politics/14gupta.html.
[50] Vinod Gupta w rozmowie ze Scottem Pelleyem, „60 Minutes II", CBS, 30 kwietnia 2003.
[51] R. Evatt, „Large Corporation Begins with Small-Town Staff", Associated Press Newswires, 18 sierpnia 2002.
[52] R. O'Harrow Jr., „Are Data Firms Getting Too Personal?", „Washington Post", 8 marca 1998, http://www.washingtonpost.com/wp-srv/frompost/march98/privacy8.htm.
[53] Bruce Biegel (członek kadry zarządzającej w Winterberry Group) i Jonathan Margulies (dyrektor zarządzający w Winterberry Group) w rozmowie z autorką, 17 kwietnia 2013.
[54] M. George, „State Made $62 Million by Selling Florida Drivers' License Information", ABC Action News, 21 czerwca 2011,

http://www.abcactionnews.com/dpp/news/localnews/investigations/i-team%3A-state-made-$62-million-by-selling-florida-drivers%27-license-information.
[55] Rzecznik prasowy Urzędu Regulacji Poczty USA w rozmowie z analityczką Lauren Kirchner, 30 kwietnia 2013.
[56] Bruce i Jonathan Margulies w rozmowie z autorką, 17 kwietnia 2013.
[57] K. Kaye, „Tacoda Buy Could Bolster AOL's Relevance in Web Ad Arena", „Clickz Marketing News", 24 lipca 2007, http://www.clickz.com/clickz/news/1712324/tacoda-buy-could-bolster-aols-relevance-web-ad-arena.
[58] P.R. La Monica, „Google to Buy DoubleClick for $3.1 Billion", CNNMoney.com, 13 kwietnia 2007, http://money.cnn.com/2007/04/13/technology/googledoubleclick/index.htr
[59] Ch. Isidore, „Microsoft Buys aQuantive for $6 Billion", CNNMoney.com, 18 maja 2007, http://money. cnn.com/2007/05/18/technology/microsoft aquantive/.
[60] K.J. Delaney, E. Steel, „Firm Mines Offl ine Data to Target Online Ads", „Wall Street Journal", 17 października 2007. Dostępny w internecie: http://online.wsj.com/article/SB119258320189661423.html.
[61] E.M. Rusli, „Buy Signal: Facebook Widens Data Targeting", „Wall Street Journal", 9 kwietnia 2013. Dostępny w internecie: http://online.wsj.com/article/SB10001424127887324504704578412960951909
[62] J. Angwin, „The Web's New Gold Mine: Your Secrets", „Wall Street Journal", 30 lipiec 2010. Dostępny w internecie: http://online.wsj.com/article/SB10001424052748703940904575395073512989
[63] „Internet Advertising Revenue Report", Związek Pracodawców Branży Internetowej, kwiecień 2013, https://www.iab. net/media/file/IABInternetAdvertisingRevenueReportFY2012POSTED.pdf.
[64] R. Rothenberg, „Has Mozilla Lost Its Values?", IABlog Związku Pracodawców Branży Internetowej, 16 lipca 2013, https://www.iab. net/iablog/2013/07/has-mozilla-lost-its-values.html.
[65] M. Kunewa, „Round Table on Online Data Collection, Targeting and Profiling" (wystąpienie publiczne), Bruksela, 31 marca 2009, http://europa. eu/rapid/press-releaseSPEECH-09-156en.htm.
[66] „Voter Privacy in the Digital Age", California Voter Foundation, 2002, http://www.calvote.org/issue/votprivacy/pub/0504voterprivacy.pdf.

[67] Tamże.
[68] „Political Date: Learn More", Aristotle, 11 września 2013, http://www.aristotle.com/political-data/political-data-learn-more/.
[69] „Premium Enhancement for Your Political Data", Aristotle, 13 września 2013, http://www.aristotle.com/political-data/premium-enhancements/.
[70] „About Us", Aristotle, 13 września 2013, http://www.aristotle.com/about-us/.
[71] M.C. Oppenheim, „The Dark Data Cycle: How the U.S. Government Has Gone Rogue in Trading Personal Data from an Unsuspecting Public", Uniwersytet Harvarda, marzec 2012.
[72] „Premium Enhancement for Your Political Data".
[73] Oppenheim, „The Dark Data Cycle".
[74] „Prime Award Service Data: Search Term: LEXIS-NEXIS; Department: Homeland Security", USAspending.gov, http://www.usaspending.gov/search? formfields={%22search term%22%3A%22LEXIS-NEXIS%22%2C%22dept%22%3A [%227000%22]}&sortby=dollars&perpage=25 [strona niedostępna].
[75] „CoreLogic Reports 55,000 Completed Foreclosures in June", CoreLogic.com, 30 lipca 2013, http://www.corelogic.com/about-us/news/corelogic-reports-55,000-completed-foreclosures-in-june.aspx.
[76] „Our Company", CoreLogic, 15 września 2013, http://www.corelogic.com/about-us/news/assetuploadfile85622101.pdf.
[77] William Binney w rozmowie z autorką, 24 maja 2012.
[78] J. Mayer, „The Secret Sharer", „New Yorker", 23 maja 2011, http://www.newyorker.com/reporting/2011/05/23/110523fafactmayer.
[79] S. Gorman, „Scuttled NSA Program Had Privacy Safeguards", „Baltimore Sun", 18 maja 2006. Dostępny w internecie: http://articles. sun-sentinel.com/2006-05-18/news/06051715281 warrantless-surveillance-nsa-communications-data.
[80] William Binney, Kirk Wiebe i Thomas Drake w rozmowie z autorką, 18 maja 2012.
[81] Inspektor Generalny, „Audit of the Requirements for the TRAILBLAZER and THINTHREAD Systems" (notatka), 15 grudnia 2004, https://www.fas.org/irp/agency/dod/ig-thinthread.pdf.
[82] S. Gorman, „NSA Rejected System That Sifted Phone Data Legally", „Baltimore Sun", 18 maja 2006, http://articles. baltimoresun.com/2006-05-18/news/06051800941surveillance-national-secu rity-agency-well-

informed.
[83] William Binney w rozmowie z autorką, 24 maja 2012.
[84] L. Poitras, „Surveillance Teach-In", 20 kwietnia 2012, http://whitney.org/WatchAndListen/Exhibitions? play id=722.
[85] William Binney, Kirk Wiebe i Thomas Drake w rozmowie z autorką, 24 maja 2012.
[86] Thomas Drake w rozmowie z autorką, 24 maja 2012.
[87] Sprawa Stany Zjednoczone kontra Thomas Andrews Drake, sygn. 10-cr-0181-RDB, Sąd Dystryktowy USA dla Dystryktu Maryland, 2010.
[88] Thomas Drake w rozmowie z autorką, 24 maja 2012.
[89] Sprawa Stany Zjednczonone kontra Drake, orzeczenie, 15 lipca 2011.
[90] D. Wise, „Leaks and the Law: The Story of Thomas Drake", „Smithsonian Magazine", lipiec-sierpień 2011, http://www.smithsonianmag.com/history-archaeology/Leaks-and-the-Law-The-Story-of-Thomas-Drake.html.
[91] Sprawa Stany Zjednoczone kontra Drake, orzeczenie, 15 lipca 2011.
[92] Binney w rozmowie z autorką, 18 marca 2012.
[93] Binney w rozmowie z autorką, 24 maja 2012.

ROZDZIAŁ 3: STAN NADZORU

[1] G. Bruce, *The Firm: The Inside Story of the Stasi*, Oxford University Press, Nowy Jork 2010, s. 10.
[2] Tamże.
[3] Statistiches Jahrbuch der Deutschen Demokratischen Republik, 1998 (w tłumaczeniu Gary'ego Bruce'a przesłanym do autorki w e-mailu z 27 lutego 2013).
[4] Bruce, *The Firm*, s. 10.
[5] Günter Bormann w rozmowie z autorką, 19 września 2011.
[6] Gary Bruce w rozmowie z autorką, 6 lutego 2013.
[7] Gary Bruce, tłumaczenie przesłane autorce 6 lutego 2013.
[8] Bruce, *The Firm*, s. 4.
[9] Bruce, tłumaczenie dla autorki.
[10] Bruce, *The Firm*, 111.
[11] Bruce, tłumaczenie dla autorki.
[12] David Burnett, tłumaczenie przesłane autorce 10 marca 2013.
[13] Tamże.
[14] Gary Bruce w rozmowie z autorką, 6 lutego 2013.

[15] Bruce, *The Firm*, s. 156.
[16] B. Bauer, *Kontrolle und Repression: individuelle Erfahrungen in der DDR (1971–1989)*, opisana w książce Bruce'a *The Firm*, s. 158. Oryginał: http://nypl.
bibliocommons.com/item/show/16455058052907kontrolleundrepression.
[17] J. Bentham, *The Panopticon Writings*, Verso, Nowy Jork 2010.
[18] M. Foucault, *Discipline and Punish: Th e Birth of the Prison*, Vintage, Nowy Jork 1995.
[19] Oulasvirta i in., „Long-Term Effects of Ubiquitous Surveillance in the Home", Helsinki Institute for Information Technology, Helsinki 2012.
[20] „Study Exposes the Negative Effects of Increasing Computerized Surveillance" (press release), Aalto University, 10 kwietnia 2012, http://www.aalto. fi/en/current/news/view/2012-10-04/.
[21] D. Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?*, Perseus Books, Cambridge, Massachusetts 1998.
[22] Ch. A. Preble, „Who Ever Believed in the ‚Missile Gap'? John F. Kennedy and the Politics of National Security", „Presidential Studies Quarterly", grudzień 2003, nr 33, s. 805–6.
[23] Corona Fact Sheet, Narodowe Biuro Rozpoznania. Dostępny w internecie: http://www.nro.gov/history/csnr/corona/factsheet.html [dostęp: 19.07.2013].
[24] D.A. Day, „Of Myths and Missiles: The Truth About John F. Kennedy and the Missile Gap" „Space Review", 3 stycznia 2006. Dostępny w internecie: http://www.thespacereview.com/article/523/1.
[25] J.T. Correll, „Airpower and the Cuban Missile Crisis", „Air Force Magazine", sierpień 2005, nr 88. Dostępny w internecie: http://www.airforcemag.com/MagazineArchive/Pages/2005/August%2020(
[26] Traktat o ograniczeniu rozwoju, testowania i rozmieszczenia systemów antybalistycznych (ABM), podpisany między Stanami Zjednoczonymi a Związkiem Radzieckim 26 maja 1972. Dostępny w internecie: https://www.fas.org/nuke/control/abmt/text/abm2.htm.
[27] J. Carter, „Remarks at the Congressional Space Medal of Honor Awards Ceremony", Kennedy Space Center, Floryda, 1 października 1978. Dostępny w internecie: http://www.gwu.
edu/~nsarchiv/NSAEBB/NSAEBB231/doc32.pdf.
[28] R. Calo, „The Boundaries of Privacy Harm", Consumer Privacy

Project, Center for Internet and Society, Szkoła Prawa Uniwersytetu Stanforda, 2010.
[29] M. Ernest-Jones, D. Nettle, M. Bateson, „Effects of Eye Images on Everyday Cooperative Behavior: A Field Experiment", „Evolution and Human Behavior" 2011, nr 32, s. 172–78, http://www.staff.ncl.ac.uk/daniel.nettle/ernestjonesnettlebateson.pdf.
[30] A. Cameron, E. Kolodinski, H. May, N. Williams, „Measuring the Effects of Video Surveillance on Crime" (raport), California Research Bureau, 5 maja 2008. Dostępny w internecie: http://www.library.ca.gov/crb/08/08-007.pdf.
[31] N.G. La Vigne, S.S. Lowry, J.A. Markman, A.M. Dwyer, „Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention", Urban Institute, wrzesień 2011. Dostępny w internecie: http://www.urban.org/publications/412403.html.
[32] L. Hempel, E. Töpfer, „On the Threshold to Urban Panopticon?: Analysing the Employment of CCTV in European Cities and Assessing Its Social and Political Implications" (dokument roboczy nr 1) [w]: „Inception Report", Urban Eye, styczeń 2002, http://www.urbaneye.net/results/uewp1.pdf.
[33] N.G. La Vigne, S.S. Lowry, „Evaluation of Camera Use to Prevent Crime in Commuter Parking Facilities: A Randomized Controlled Trial", Urban Institute, wrzesień 2011, http://www.urban.org/publications/412451.html.
[34] B.C. Welsh, D. Farrington, „Surveillance for Crime Prevention in Public Space: Results and Policy Changes", „Criminology and Public Policy", lipiec 2004, nr 3.
[35] La Vigne, Lowry, „Evaluation of Camera Use".
[36] Ch. Cooper, „Reid's Shoe Bomb Was Sophisticated, Like an Explosive Used by Palestinians", „Wall Street Journal", 9 stycznia 2002. Dostępny w internecie: http://online.wsj.com/article/SB10105336618080030000.html.
[37] B. Whitaker, „Immigration Unit Almost Deported Airport Gunman in 1996", „New York Times", 7 lipca 2002. Dostępny w internecie: http://www.nytimes.com/2002/07/07/us/immigration-unit-almost-deported-airport-gunman-in-1996.html.
[38] „Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood", Texas, 5 listopda 2009. Dostępny w internecie:

https://www.fbi.gov/news/pressrel/press-releases/final-report-of-the-william-h.-webster-commission.
[39] „White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack", Biały Dom, 7 stycznia 2010, http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack.
[40] A. Elliott, „Militant's Path from Pakistan to Times Square", „New York Times", 22 czerwca 2010, http://www.nytimes.com/2010/06/23/world/23terror.html?pagewanted=all.
[41] M. Arsenault, „Dead Suspect Broke Angrily with Muslim Speakers", „Boston Globe", 21 kwietnia 2013, http://www.boston.com/news/nation/2013/04/21/bombing-suspect-tamerlan-tsarnaev-had-broken-angrily-with-muslim-speakers-mosque/XCBPdDswOKxaa4AJ0mkuVL/singlepage.html.
[42] Gen. K. Alexander, „Remarks at the AFCEA International Cyber Symposium", Baltimore, Maryland, 27 czerwca 2013.
[43] Sprawa Stany Zjednoczone kontra Najibullah Zazi, sygn. 10–60, Sąd Dystryktowy dla Wschodniego Dystryktu Nowego Jorku, 2011. Dostępny w internecie: http://www.justice.gov/opa/documents/zazi-indictment.pdf.
[44] Gen. K. Alexander, „Remarks at the AFCEA International Cyber Symposium".
[45] „House Permanent Select Committee on Intelligence Holds a Hearing on Surveillance Programs", Waszyngton, 18 czerwca 2013.
[46] „Inside the Zazi Takedown", „Newsweek" dla Daily Beast, 25 września 2009, http://www.thedailybeast.com/newsweek/2009/09/26/inside-the-zazi-takedown.html.
[47] Sprawa Stany Zjednoczone kontra Najibullah Zazi, sygn. 09 CR 663, Sąd Dystryktowy dla Wschodniego Dystryktu Nowego Jorku, 2010.
[48] Zeznania gen. Keitha Alexandra przed Zespołem Stałym Komisji ds. Wywiadu, 18 czerwca 2013.
[49] Prezydent Barack Obama w rozmowie Charlie'm Rose'em, 16 czerwca 2013, http://www.charlierose.com/watch/60230424.
[50] M. Apuzzo, A. Goldman, *Enemies Within: Inside the NYPD's Secret Spying Unit and Bin Laden's Final Plot Against America*, Simon and Schuster, Nowy Jork 2013, s. 89.

[51] E. Lipton, S. Shane, „Questions on Why Suspect Wasn't Stopped", „New York Times", 27 grudnia 2009. Dostępny w internecie: https://www.nytimes.com/2009/12/28/us/28terror.html.
[52] „White House Review Summary Regarding 12/25/2009 Attempted Terrorist Attack", Biały Dom, 7 stycznia 2010. Dostępny w internecie: http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack.
[53] „Final Report of the William H. Webster Commission".
[54] G. Miller, S. Horwitz, „Boston Bombing Suspect Put on Terrorist Watch List at CIA Request", „Washington Post", 25 kwietnia 2013, http://articles. washingtonpost.com/2013-04-24/national/387815881dagestan-u-s-embassy-paul-bresson.
[55] J. Jonas, J. Harper, „Effective Counterterrorism and the Limited Role of Predictive Data Mining" (analiza nr 584), Cato Institute, 11 grudnia 2006. Dostępny w internecie: http://www.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf.
[56] Siddhartha Bhattacharyya w rozmowie z autorką, 11 czerwca 2013.
[57] Jonas, Harper, „Effective Counterterrorism".
[58] „Protecting Individual Privacy in the Struggle Against Terrorists", Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, Narodowa Rada ds. Badań, Waszyngton, National Academies Press, 2008.
[59] M. Olsen (dyrektor Krajowego Ośrodka Zwalczania Terroryzmu, NCC), „The National Counterterrorism Center's Role in Counterterrorism" (przemówienie), Aspen Institute, Waszyngton, 26 lipca 2012, http://www.aspeninstitute.org/video/national-counterterrorism-center-s-role-counterterrorism.
[60] M. Naughton, „Davis: Feds Didn't Tell Boston Police About Tamerlan Tsarnaev", Metro. us, 13 maja 2013, http://www.metro. us/boston/news/local/2013/05/09/davis-feds-didnt-tell-boston-police-about-tamerlan-tsarnaev/.
[61] R. Popplewell, „The Stasi and the East German Revolution of 1989", „Contemporary Europe an History" marzec 1992, nr 1, s. 37–63.

ROZDZIAŁ 4: WOLNOŚĆ STOWARZYSZANIA SIĘ

[1] Yasir Afifi w rozmowie z autorką, 17 stycznia 2013.
[2] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.

[3] Yasir Afifi w rozmowie z autorką, 17 stycznia 2013.
[4] Yasir Afifi i Angelina Asfour w rozmowie z autorką, 8 czerwca 2013.
[5] F. Fassihi, „Iranian Crackdown Goes Global", „Wall Street Journal", 3 grudnia 2009. Dostępny w internecie: http://online.wsj.com/article/SB12597864 9644673331.html.
[6] J.W. Hsu, E. Dou, „Chinese Dissident Skirts Talk of NYU", „Wall Street Journal", 23 czerwca 2013. Dostępny w internecie: http://online.wsj.com/article/SB10001424127887323998604578565310545277
[7] Artykuł 17, Powszechna Deklaracja Praw Człowieka przyjęta 10 grudnia 1948, https://www.un.org/en/documents/udhr/index.shtml#atop.
[8] Sprawa Krajowe Stowarzyszenie Postępu Ludzi Kolorowych kontra Patterson, sygn. 357 U.S. 449, 1958.
[9] Fitbit Inc., http://www.fitbit.com.
[10] G.A. Fine, Inspektor Generaly, Departament Sprawiedliwości Stanów Zjednoczonych, oświadczenie złożone przed House Committee on the Judiciary Subcommittee on the Constitution, Civil Rights and Civil Liberties, w związku z raportem „Report by the Office of the Inspector General on the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records", 14 kwietnia 2010. Dostępny w internecie: http://www.justice.gov/oig/testimony/t1004.pdf.
[11] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Nowy Jork 2013, s. 175–82.
[12] E. Schmidt, *The New Digital Age: Reshaping the Future of People, Nations and Busines*, Alfred A. Knopf, Nowy Jork 2013, s. 55.
[13] Tamże, s. 77.
[14] Tamże, s. 62.
[15] Opis wydarzeń przedstawionych na kolejnych stronach pochodzi z zarzutów sformułowanych w procesie wytoczonym później przez Afifiego; sprawa Yasir Afifi kontra Eric Holder i in., nr 1:11cv460 (D.C., 2012). W październiku 2013 roku sprawa wciąż pozostawała nierozpatrzona.
[16] JayClay: *So if My Deodorant Could Be a Bomb, Why Are You Just Chucking It in the Bin?*, Reddit, 24 czerwca 2010, zrzut z ekranu 28 stycznia 2013, http://www.reddit.com/r/AskReddit/comments/ciiag/soifmydeodorant_cou

limit=500.
[17] khaledthegypsy, komentarz na portalu Reddit, 24 czerwca 2010, http://www.reddit.com/r/AskReddit/comments/ciiag/soifmy_deodorantcou
[18] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[19] Chalid Ibrahim w rozmowie z autorką, 16 sierpnia 2012.
[20] Yasir Affi w rozmowie z autorką, 15 sierpnia 2012.
[21] Yasir Afifi, korespondencja e-mailowa z autorką, 2 lutego 2013.
[22] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[23] khaledthegypsy: *Does This Mean the FBI Is After Us?*, Reddit, 3 października 2010, zrzut z ekranu 28 stycznia 2013, http://www.reddit.com/comments/dmh5s/doesthismeanthefbiisafterus/
[24] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[25] Sprawa Afifi kontra Holder.
[26] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[27] Sprawa Afifi kontra Holder.
[28] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[29] Sprawa Afifi kontra Holder.
[30] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[31] Yasir Afifi, korespondencja e-mailowa z autorką, 2 lutego 2013.
[32] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[33] Sprawa Afifi kontra Holder.
[34] Tamże.
[35] Sprawa Afifi kontra Holder.
[36] Sprawa Afifi kontra Holder.
[37] Sprawa Stany Zjednoczonych kontra Jones, 2012. Dostępny w internecie: http://www.law. cornell. edu/supremecourt/text/10-1259.
[38] Sprawa Afifi kontra Holder.
[39] Konstytucja Stanów Zjednoczonych, Pierwsza Poprawka.
[40] Lee Bollinger w rozmowie z autorką, 19 czerwca 2013.
[41] Sprawa „New York Times" kontra Sullivan, sygn. 376 U.S. 254, 1964.
[42] Sprawa Boy Scouts of America kontra Dale, sygn. 530 U.S. 640, 2000.
[43] Sprawa Laird kontra Tatum, sygn. 408 U.S. 1, 1972.
[44] Sprawa Clapper kontra Amnesty International USA, 2013. Dostępny w internecie: http://www.law. cornell. edu/supremecourt/text/11-1025.
[45] Chalid Ibrahim w rozmowie z autorką, 16 sierpnia 2012.
[46] khaledthegypsy, komentarz w portalu Reddit, 9 kwietnia 2011, http://www.reddit.com/r/AskReddit/comments/gmcw5/heyredditwhathap

[47] Chalid Ibrahim w rozmowie z autorką, 16 sierpnia 2012.
[48] T. Aaronson, „The Informants", „Mother Jones", wrzesień – październik 2011 http://www.motherjones.com/politics/2011/08/fbi-terrorist-informants?
[49] T. Aaronson, seria pytań i odpowiedzi, Szkoła Prawa Uniwersytetu Columbia, Nowy Jork, 31 stycznia 2013.
[50] „AP's Probe into NYPD Intelligence Operations", Associated Press, http://www.ap.org/Index/AP-In-The-News/NYPD.
[51] Chris Hawley, „NYPD Monitored Muslim Students All over Northeast", Associated Press, 18 lutego 2012, http://www.ap.org/Content/AP-In-The-News/2012/NYPD-monitored-Muslim-students-all-over-Northeast.
[52] A. Dandia, „My Life Under NYPD Surveillance: A Brooklyn Student and Charity Leader on Fear and Mistrust", blog: *Blog of Rights*, American Civil Liberty Union, 18 czerwca 2013, http://www.aclu.org/blog/national-security-religion-belief-criminal-law-reform-technology-and-liberty/my-life-under-nypd.
[53] A. Goldman, M. Apuzzo, „Informant: NYPD Paid Me to ‚Bait' Muslims", Associated Press, 23 października 2012, http://www.ap.org/Content/AP-In-The-News/2012/Informant-NYPD-paid-me-to-bait-Muslims.
[54] Dandia, „My Life".
[55] Sprawa Raza kontra miasto Nowy Jork, sygn. CV 13-2448, Sąd Dystryktowy dla Wschodniego Dystryktu Nowego Jorku, 2013.
[56] Yasir Afifi w rozmowie z autorką, 17 stycznia 2013.
[57] Yasir Afifi w rozmowie z autorką, 15 sierpnia 2012.
[58] Afifi, odwiedziny autorki, 8 czerwca 2013.

ROZDZIAŁ 5: MODELE ZAGROŻEŃ

[1] L. Osterman, „Threat Modeling Again, Threat Modeling Rules of Thumb", weblog Larry'ego Ostermana, 21 września 2007. Dostępny w internecie: http://blogs.msdn.com/b/larryosterman/archive/2007/09/21/threat-modeling-again-threat-modeling-rules-of-thumb.aspx.
[2] B. Schneier, *Schneier on Security*, Wiley Publishing, Indianapolis 2008, s. viii.
[3] Jeff Stein, „Draft Dodgers", „Foreign Policy", 14 listopada 2012.

Dostępny w internecie:
http://www.foreignpolicy.com/articles/2012/11/14/draftdodgers.
[4] K. Zetter, „Email Location Data Led FBI to Uncover Top Spy's Affair", „Wired", 12 listopada 2012. Dostępny w internecie:
http://www.wired.com/threatlevel/2012/11/gmail-location-data-petraeus/.
[5] N. Perlroth, „Trying to Keep Your E-Mails Secret When the C.I.A. Chief Couldn't", „New York Times", 16 listopada 2012. Dostępny w internecie: http://www.nytimes.com/2012/11/17/technology/trying-to-keep-your-e-mails-secret-when-the-cia-chief-couldnt.html.
[6] R.D. McFadden, „Prisoner of Rage", „New York Times", 26 maja 1996. Dostępny w internecie:
http://www.nytimes.com/1996/05/26/us/prisoner-of-rage-a-special-report-from-a-child-of-promise-to-the-unabom-suspect.html.
[7] D. Johnston, „17-year Search, an Emotional Discovery and Terror Ends", „New York Times", 5 maja 1998. Dostępny w internecie:
http://www.nytimes.com/1998/05/05/us/17-year-search-an-emotional-discovery-and-terror-end.html.
[8] D. Politi, „Obama Has Charged More Under Espionage Act Than All Other Presidents Combined, „Slate.com, 22 czerwca 2013,
http://www.slate.com/blogs/theslatest/2013/06/22/edwardsnowdeniseightl
[9] D. Carr, „Blurred Line Between Espionage and Truth", „New York Times", 26 lutego 2012,
http://www.nytimes.com/2012/02/27/business/media/white-house-uses-espionage-act-to-pursue-leak-cases-media-equation.html.
[10] J. Angwin, „The Mess We're In" (Brownstone Diary), „Wall Street Journal", 19 lutego 2010, Dostępny w internecie:
http://online.wsj.com/article/SB10001424052748704041504575045241309357
[11] Ulysses, „Revive: The West 123rd Street Brownstone", blog: *Harlem + Bespoke*, 17 lutego 2010, http://harlembespoke.
blogspot.com/2010/02/revive-west-123rd-street-brownstone.html.
[12] J.J. Luna, *How to Be Invisible: Protect Your Home, Your Children, Your Assets, and Your Life*, Thomas Dunne Books, Nowy Jork 2004.
[13] K.W. Royce, *One Nation, Under Surveillance*, Javelin Press, Gillette (Wyoming) 2009.
[14] N.Y. VAT. Law § 402: NY Code – Section 402: Distinctive Number; Form of Number Plates; Trailers, http://codes. lp.
findlaw.com/nycode/VAT/IV/14/402.
[15] Mark Eckenwiler w rozmowie z autorką, 6 marca 2013.

[16] 18 USC § 1028 – Fraud and Related Activity in Connection with Identifi cation Documents, Authentication Features, and Information, http://www.law. cornell. edu/uscode/text/18/1028.
[17] Sprawa Flores-Figueroa kontra Stany Zjednoczone, sygn. 08-108, 274 Fed. Appx. 501, http://www.law. cornell. edu/supct/html/08-108. ZO.html.
[18] 18 USC § 1343 – Fraud by Wire, Radio, or Television, http://www.law. cornell. edu/uscode/text/18/1343.
[19] John Strauchs w rozmowie z autorką, 5 marca 2013.
[20] M. Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals*, Penguin Books, Nowy Jork 2006, s. 392.
[21] The Surveillance Self-Defense Project: „Wiretapping Law Protections", Electronic Frontier Foundation, https://ssd. eff.org/wire/govt/wiretapping-protections [dostęp: 26.07.2013].
[22] „Transparency Report: User Data Requests", Google, Inc., https://www.google.com/transparencyreport/userdatarequests/.
[23] J. Valentino-Devries, „‚Stingray' Phone Tracker Fuels Constitutional Clash", „Wall Street Journal", 22 września 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424053111904194604576583112723197
[24] E. Holder, „Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended", 28 lipca 2004.
[25] Mike Perry w rozmowie z autorką, 5 czerwca 2013.
[26] John Strauchs w rozmowie z autorką, 5 marca 2013.

ROZDZIAŁ 6: AUDYT

[1] Michael Sussmann w rozmowie z autorką, 24 październik 2012.
[2] The Data Liberation Front, http://www.dataliberation.org/.
[3] Rob Shilkin, e-mail do autorki, 30 lipca 2013.
[4] N. Lundeen, K. Skrying, „Student Group Challenges Facebook on Privacy", blog: *Tech Europe*, WSJ.com, 2 lutego 2012, http://blogs.wsj.com/tech-europe/2012/02/08/student-group-challenges-facebook-on-privacy/.
[5] „Facebook's Data Pool", europe-v-facebook.org, http://www.europe-v-facebook.org/EN/Data Pool/datapool.html.
[6] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24

października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Dostępny w internecie: http://eur-lex.europa.eu/legal-content/pl/TXT/? uri=CELEX%3A31995L0046.
[7] Komisarz ds. Ochrony Danych, „Facebook Ireland Ltd, Report of Audit", 21 grudnia 2011, http://europe-v-facebook.org/Facebook_IrelandAuditReportFinal.pdf.
[8] Facebook, Zasady dotyczące danych, aktualizacja: 11 grudnia 2012, https://www.facebook.com/fulldatausepolicy.
[9] Komisja ds. Ochrony Danych Osobowych, „Facebook Ireland Ltd., Report of Re-Audit", 21 września 2012, http://europe-v-facebook.org/ODPC_Review.pdf.
[10] M. Vandor, „Your Twitter Archive", Twitter Blog, 19 grudnia 2012, https://blog. twitter.com/2012/your-twitter-archive.
[11] J. Valeski, „New Gnip & Twitter Partnership", Gnip – blog firmowy, 17 listopada 2010, http://blog. gnip.com/gnip-twitter-partnership/ [strona niedostępna].
[12] Mike w rozmowie z autorką, 21 września 2012.
[13] J. Angwin, J. Valentino-DeVries, „New Tracking Frontier: Your License Plates", „Wall Street Journal", 29 września 2012. Dostępny w internecie: http://online.wsj.com/article/SB10000872396390443995604578004723603
[14] Mike Griffin w rozmowie z autorką, 21 września 2012.
[15] M. Shnayerson, „The Net's Master Data-Miner", „Vanity Fair", grudzień 2004.
[16] „Company Overview of TLO, LLC", „Bloomberg Businessweek", http://investing. businessweek.com/research/stocks/private/snapshot. asp? privcapId=128678962 [dostęp: 25.04.2013].
[17] A. Woolner, „Hank Asher's Startup TLO Knows All About You", „Bloomberg Businessweek, „, 15 września 2011, http://www.businessweek.com/magazine/hank-ashers-startup-tlo-knows-all-about-you-09152011.html.
[18] TLO, LLC, „Press Release Honoring Frank", 12 stycznia 2013, http://www.tlo.com/hankpressrelease.html.
[19] Mike Griffin w rozmowie z autorką, 21 września 2012.
[20] E. Nakashima, R. O'Harrow Jr., „LexisNexis Parent Set to Buy ChoicePoint", „Washington Post", 22 lutego 2008, http://articles. washingtonpost.com/2008-02-22/business/36857083 1choicepoint-data-

broker-lexisnexis-group; oraz: R. O'Harrow Jr., „LexisNexis to Buy Seisint for $775 Million", „Washington Post", 15 lipca 2004, http://www.washingtonpost.com/wp-dyn/articles/A50577-2004 Jul14.html.
[21] Woolner, „Hank Asher's Startup".
[22] PeopleWise, https://www.peoplewise.com/people/report.
[23] D. Takahashi, „BeenVerified Hopes to Make Background Checks Easier and Cheaper", VentureBeat, 21 października 2008, http://venturebeat.com/2008/10/21/beenverified-hopes-to-make-background-checks-easier-and-cheaper/.
[24] J. Angwin, „Sites Are Accused of Privacy Failings", „Wall Street Journal", 13 lutego 2012. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970204136404577207183258570
[25] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.
[26] Acxiom Corp., raport roczny, http://www.sec.gov/Archives/edgar/data/733 269/000073326913000012/fir
[27] Acxiom Corp., „My Cluster", https://isapps. acxiom.com/personicx/personicx.aspx.
[28] D. Tynan, „Further Adventures in Data Mining, or Welcome to My Lear Jet Lifestyle", ITworld.com, 11 kwietnia 2013, http://www.itworld.com/it-management/352177/adventures-data-mining-or-welcome-my-lear-jet-lifestyle.
[29] AboutTheData.com, https://AboutTheData.com/.
[30] Datalogix, http://www.datalogix.com/about/.
[31] X. Wang, „Intelius May Revisit IPO After Shelving It in 2010, CEO Says", Bloomberg, 25 października 2011, http://www.bloomberg.com/news/2011-10-25/intelius-may-revisit-ipo-after-shelving-it-in-2010-ceo-says.html.
[32] „A Summary of Your Rights Under the Fair Credit Reporting Act", Consumer Response Center, Federalna Komisja Handlu, http://www.consumer. ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.
[33] „Fact Sheet: President Bush Signs the Fair and Accurate Credit Transactions Act of 2003", Biały Dom, 4 grudnia 2003, http://georgewbush-whitehouse.

archives.gov/news/releases/2003/12/20031204-3.html.
[34] J. Robertson, „Top Credit Agencies Say Hackers Stole Celebrity Reports", Bloomberg, 12 marca 2013, http://www.bloomberg.com/news/2013-03-12/Equifax-transunion-say-hackers-stole-celebrity-reports.html.
[35] Federalna Komisja Handlu, „Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003", grudzień 2012, http://ftc.gov/os/2013/02/130211factareport.pdf.
[36] eBureau, „About Us", http://www.ebureau.com/about [dostęp: 5.05.2013].
[37] eBureau, „Using Third Party Data and Analytics to Help You Manage Lead Quality: Part 2", blog: *eBureau Industry Blog*, 11 maja 2012, http://www.ebureau.com/blog/using-third-party-data-and-analytics-help-you-manage-online-lead-quality-part-2.
[38] eBureau, „Credit Risk Management", http://www.ebureau.com/credit-risk-management.
[39] eBureau, „Collections & Recovery", http://www.ebureau.com/collections-recovery.
[40] eBureau, „Income Estimator", http://www.ebureau.com/sites/default/files/file/datasheets/ebureauincome
[41] eBureau w e-mailu do autorki datowanym na 31 lipca 2013.
[42] V12 Group, „The PYCO Personality Score: The Science of Motivating Consumers to Respond", marzec 2012, http://www.v12groupinc.com/wp-content/uploads/2012/03/PYCO PersonalityScoreWhite-Paper.pdf.
[43] Yen Lee w rozmowie z asystentką autorki, Lauren Kirchner, 30 maja 2013.
[44] Yen Lee w e-mailu do asystentki autorki Lauren Kirchner, 4 czerwca 2013.
[45] B. Sullivan, „Lawyers Eye NSA Data as Treasure Trove for Evidence", NBC News, 21 czerwca 2013, http://www.cnbc.com/id/100834242.
[46] Sprawa Shearson kontra Departament Bezpieczeństwa Krajowego i in., sygn. 08-4582, szósty okręg, 2011, http://papersplease.org/wp/wp-content/uploads/2011/04/shearson-opinion-21apr2011.pdf.
[47] Julia Shearson w rozmowie z Lauren Kirchner, 3 września 2013.
[48] Shearson konta Departament Bezpieczeństwa Krajowego i in., nr 08-4582, szósty okręg, 2011.
[49] Julia Shearson w rozmowie z Lauren Kirchner, 3 września 2013.

[50] Federalne Biuro Śledcze w liście do autorki, 17 maja 2013.
[51] Edward Hasbrouck w rozmowie z autorką, 2 maja 2013.
[52] Sprawa Hasbrouck kontra Urząd Celny i Ochrony Granic Stanów Zjednoczonych, Sąd Dystryktowy dla Północnego Dystryktu Kalifornii, 2012.
[53] Edward Hasbrouck w rozmowie z autorką, 2 maja 2013.
[54] Ustawa o bezpieczeństwie transportu powietrznego, 2001. Dostępna w internecie: http://www.gpo.gov/fdsys/pkg/PLAW-107publ71/html/PLAW-107publ71.htm.
[55] 19 C.F.R. 122.49d – imienny rejestr pasażera (PNR), http://www.law. cornell. edu/cfr/text/19/122.49d.
[56] „Privacy Impact Assessment for the Automated Targeting System", Departament Bezpieczeństwa Krajowego, 1 czerwca 2012, http://www.dhs.gov/xlibrary/assets/privacy/privacypiacbpats006b.pdf.
[57] „EU Court Annuls Data Deal with US", BBC News, 30 maja 2006, http://news. bbc.co.uk/2/hi/europe/5028918.stm.
[58] „MEPs Back Deal to Give Air Passenger Data to US", BBC News, 19 kwietnia 2012, http://www.bbc.co.uk/news/world-europe-17764365.
[59] Colleen Schwartz (rzeczniczka prasowa Dow Jones) w rozmowie z autorką, 30 lipca 2013.

ROZDZIAŁ 7: PIERWSZA LINIA OBRONY

[1] Michael Tiffany, w rozmowie z autorką, 2 lutego 2013.
[2] Lawrence Wright, „The Spymaster", „New Yorker, 21 stycznia 2008, http://www.newyorker.com/reporting/2008/01/21/080121fafact_wright.
[3] J. Napolitano, „Achieving Security and Privacy", 2 maja 2012, Australijski Uniwersytet Narodowy, Canberra, http://www.dhs.gov/news/2012/05/02/remarks-secretary-homeland-security-janet-napolitano-achieving-security-and-privacy.
[4] „Comcast Partners with AG Blumenthal to Keep Kids Safe Online", „Red Orbit, 15 czerwca 2009, http://www.redorbit.com/news/entertainment/1705787/comcastpartnerswit
[5] A. Vance, „If Your Password Is 123456, Just Make It HackMe", „New York Times", 20 stycznia 2010, https://www.nytimes.com/2010/01/21/technology/21password.html?r=1&.
[6] „Consumer Password Worst Practices", The Imperva Application

Defense Center, 2010, http://www.imperva.com/docs/WPConsumerPasswordWorstPractices.pdf.
[7] „UK Adults Taking Online Password Security Risks", Ofcom, 23 kwietnia 2013, http://media. ofcom.org. uk/2013/04/23/uk-adults-taking-online-password-security-risks/.
[8] R. Anderson, *Security Engineering*, Wiley, Hoboken (New Jersey) 2008, s. 33, http://www.cl. cam. ac. uk/~rja14/Papers/SEv2-c02.pdf.
[9] J. Yan, A. Blackwell, R. Anderson, A. Grant, „Password Memorability and Security: Empirical Results", „IEEE Security & Privacy", wrzesień-październik 2004, http://homepages.cs.ncl.ac.uk/jeff. yan/jyanieeepwd.pdf.
[10] P. Inglesant, M.A. Sasse, „The True Cost of Unusable Password Policies: Password Use in the Wild", 15 kwietnia 2010, https://www.cl.cam.ac.uk/~rja14/shb10/angela2.pdf.
[11] Per Thorsheim (ekspert ds. bezpieczeństwa haseł) w rozmowie z Lauren Kirchner, 28 czerwca 2013.
[12] M. Kotadia, „Microsoft Security Guru: Jot Down Your Passwords", CNET, 23 maja 2005, http://news. cnet.com/Microsoft-security-guru-Jot-down-your-passwords/2100-735535716590.html? tag=nefd. pop.
[13] „Online Americans Fatigued by Password Overload Janrain Study Finds" (komunikat prasowy), Janrain, 23 sierpnia 2012, http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/.
[14] S. Michels, „Radio Frequency Identification Tags: Identity Theft Danger or Modern Aid?", 16 sierpnia 2010, http://www.pbs.org/newshour/rundown/2010/08/radio-frequency-identification-a-danger-or-a-help-1.html.
[15] „HTTPS Everywhere", Electric Frontier Foundation, https://www.eff.org/https-everywhere.
[16] „Google Authenticator", Google, Inc., iTunes App Store, https://itunes.apple.com/us/app/google-authenticator/id388497605? mt=8 [aktualizacja: 7.09.2013].
[17] Little Snitch, Objective Development Software GmbH, http://www.obdev.at/products/littlesnitch/index.html.
[18] SpiderOak, https://spideroak.com/.
[19] Ethan Oberman w rozmowie z autorką, 15 sierpnia 2012.
[20] M.M. Bagley, „M. Lax Blows Lead, Loses to Dartmouth", „Harvard Crimson", 10 maja 1999. Dostępny w internecie:

http://www.thecrimson.com/article/1999/5/10/m-lax-blows-lead-loses-to/.
[21] Ethan Oberman w rozmowie z autorką, 15 sierpnia 2012.
[22] Alan Fairless w rozmowie z autorką, 28 sierpnia 2012.
[23] Jeremi Gosney (PasswordsCon, współtwórca i prezes zarządu Stricture Group) w rozmowie z Lauren Kirchner, 12 lipca 2013.
[24] N. Anderson, „How I Became a Password Cracker", blog: *Ars Technica*, 24 marca 2013, http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/.
[25] R. Graham, „LinkedIn vs. Password Cracking", „Errata Security", 6 czerwca 2012, http://erratasec. blogspot.com/2012/06/linkedin-vs-password-cracking.html.
[26] Anderson, „How I Became a Password Cracker".
[27] D. Goodin, „Why Passwords Have Never Been Weaker – and Crackers Have Never Been Stronger", blog: *Ars Technica*, 20 sierpnia 2012, http://arstechnica.com/security/2012/08/passwords-under-assault/.
[28] P. Wagenseil, „LinkedIn, eHarmony Don't Take Your Security Seriously", „TechNewsDaily", NBC News, 8 czerwca 2012, http://www.nbcnews.com/technology/linkedin-eharmony-dont-take-your-security-seriously-819858.
[29] Jeffrey Goldberg w rozmowie z autorką, 14 maja 2013.
[30] „Row Between Wikileaks and Guardian over Security Breach", BBC News, 1 września 2011, http://www.bbc.co.uk/news/uk-14743410.
[31] D. Wheeler, „Open Source Password Strength Estimator", kwiecień 2012, https://dl. dropboxusercontent.com/u/209/zxcvbn/test/index.html.
[32] J. Bonneau, E. Shutova, „Linguistic Properties of Multi-Word Passphrases", USEC '12: Workshop on Usable Security, Kralendijk, Bonaire, Holandia, 2 marca 2012, http://www.jbonneau.com/doc/BS12-USEC-passphraselinguistics.pdf.
[33] A. Reinhold, „The Diceware Passphrase FAQ", http://world. std.com/~reinhold/dicewarefaq.html [aktualizacja: 18.04.2012].
[34] Bruce Marshall w rozmowie z asystentką autorki, Lauren Kirchner, 3 lipca 2013.
[35] N. Perlroth, „Government Announces Steps to Restore Confi dence in Encryption Standards", blog: *Bits*, NYTimes.com, 10 września 2013, http://bits. blogs. nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/? src=twrhp& r=0.

ROZDZIAŁ 8: POŻEGNANIE Z GOOGLE

[1] J. Airoldi, „Privacy and Library Rec ords, a Case Study in Whatcom County", „Journal of Educational Controversy", lato 2010, nr 2, http://www.wce.wwu.edu/Resources/CEP/eJournal/v005n002/a007.shtml.
[2] Deming, Washington, Population: Biuro Spisów Ludności Stanów Zjednoczonych 2010 and 2000 Interactive Map, Demographics, Statistics, Quick Facts, http://censusviewer.com/city/WA/Deming.
[3] Joan Airoldi (dyrektor, Whatcom County Library System, Washington) w rozmowie z autorką, 29 marca 2013.
[4] D. Garrett w rozmowie z Lauren Kirchner, 30 maja 2013.
[5] American Library Association, „State Privacy Laws Regarding Library Records", http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/statep
[6] Amory Peck (była przewodniczący rady nadzorczej systemu bibliotek hrabstwa Whatcom) w rozmowie z Lauren Kirchner, 7 czerwca 2013.
[7] Deborra Garrett w rozmowie z Lauren Kirchner, 30 maja 2013.
[8] Amory Peck w rozmowie z Lauren Kirchner, 7 czerwca 2013.
[9] P. Taylor, „Kramerbooks Declares Victory in Subpoena Battle", Freedom Forum, First Amendment Center, 22 czerwca 1998, http://www.freedomforum.org/templates/document. asp?documentID=9736.
[10] A. Peck, „Remarks Made by Amory Peck, Board of Trustees Chair, Whatcom County Library System" (Robert B. Downs Intellectual Freedom Reception), Uniwersytet Illinois w Urbana-Champaign, 15 stycznia 2005, http://www.lis. illinois. edu/articles/2005/01/remarks-made-amory-peck-board-trustees-chair-whatcom-county-library-system.
[11] Deborra Garrett w rozmowie z Lauren Kirchner, 30 maja 2013.
[12] N. Wong, „Judge Tells DoJ ‚No' on Search Queries", Google Official Blog, 17 marca 2006, http://googleblog. blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html.
[13] Order in re Grand Jury Subpoena to Amazon.com, 7 sierpnia 2006 (W.D. Wis. 2007), http://dig. csail. mit. edu/2007/12/In-re-grand-jury-subpoena-amazon. PDF.
[14] J. Angwin, „Secret Orders Target Email", „Wall Street Journal", 9 października 2011, http://online.wsj.com/article/SB10001424052970203476804576613284007311
[15] S.W. Smith, „Gagged, Sealed & Delivered: Reforming ECPA's Secret

Docket", „Harvard Law & Policy Review", 21 maja 2012, nr 6, https://papers. ssrn.com/sol3/papers. cfm? abstract id=2071399.
[16] Microsoft 2012 Law Enforcement Requests Report, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/#FAQs1.
[17] „Google Transparency Report", https://www.google.com/transparencyreport/userdatarequests/countries/?t=table & p=2012-06 [dostęp: 15.08.2013].
[18] Digital Due Process Coalition, http://www.digitaldueprocess.org/.
[19] Angwin, „Secret Orders Target Email".
[20] Dane Jasper, korespondencja z Lauren Kirchner, 2 września 2013.
[21] C.C. Miller, „Secret Court Ruling Put Tech Companies in Data Bind", „New York Times", 13 czerwca 2013, http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html.
[22] Sąd Nadzoru Wywiadu Stanów Zjednoczonych, sygn. 08-01, 22 sierpnia 2008, http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.
[23] D. Drummond, „Greater Transparency Around GovernmentRequests", Google Official Blog, 20 kwietnia 2010, http://googleblog. blogspot.com/2010/04/greater-transparency-around-government.html.
[24] „Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders", 18 czerwca 2013, http://www.wired.com/imagesblogs/threatlevel/2013/06/Foreign-Intelligence-Surveillance-Court-Motion-for-Declaratory-Judgment.pdf.
[25] Federalna Komisja Handlu, „FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network" (komunikat prasowy), 30 marca 2011, http://www.ftc.gov/opa/2011/03/google.shtm.
[26] Ch. Albanesius, „Google Settles Buzz Class-Action Suit for $8.5M", „PC Magazine", 3 września 2010, http://www.pcmag.com/article2/0,2817,2368714,00. asp.
[27] J. Angwin, J. Valentino-DeVries, „Google's iPhone Tracking", „Wall Street Journal", 17 lutego 2012. Dostępny w internecie: http://online.wsj.com/news/articles/SB10001424052970204880404577225380
[28] „Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser" (komunikat prasowy), Federalna Komisja Handlu, 9 sierpnia

2012, http://ftc.gov/opa/2012/08/google.shtm.
[29] Prokurator Generalny stanu Connecticut George Jepsen, „Attorney General Announces $7 Million Multistate Settlement with Google Over Street View Collection of WiFi Data" (komunikat prasowy), 12 marca 2013, http://www.ct.gov/ag/cwp/view. asp? Q=520518&A=2341.
[30] A. Whitten, „Updating Our Privacy Policy and Terms of Service", Google Official Blog, 24 stycznia 2012, http://googleblog. blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.
[31] J. Valentino-Devries, „What Do Google's Privacy Changes Mean for You?", blog: *Digits*, 25 stycznia 2012, WSJ.com, http://blogs.wsj.com/digits/2012/01/25/what-do-googles-privacy-changes-mean-for-you/.
[32] Rob Shilkin (rzecznik prasowy Google), korespondencja z autorką, 30 lipca 2013.
[33] „DuckDuckGo Privacy", DuckDuckGo, Inc., https://duckduckgo.com/privacy [dostęp: 20.08.2013].
[34] T. Mullaney, „Jobs Fight: Haves vs. the Have-Nots", „USA Today", 16 sierpnia 2012, http://usatoday30. usatoday.com/money/business/story/2012/09/16/jobs-fight-haves-vs-the-have-nots/57778406/1.
[35] M. Helft, D. Barboza, „Google Shuts Down Site in Dispute over Censorship", „New York Times", 22 marca 2010, http://www.nytimes.com/2010/03/23/technology/23google.html? r=0.
[36] Gabriel Weinberg (prezes zarządu, DuckDuckGo, Inc.) w rozmowie z autorką, 24 października 2012.
[37] „United Online, Inc., Acquires Opobox, Inc." (komunikat prasowy), „Houston Chronicle", 20 marca 2006, http://www.chron.com/news/article/PZ-United-Online-Inc-Acquires-Opobox-Inc-1654933.php.
[38] „Ads in Gmail", Google, Inc., https://support. google.com/mail/answer/6603? hl=en [dostęp: 29.09.2013].
[39] G. Greenwald, J. Ball, „The Top Secret Rules That Allow NSA to Use US Data Without a Warrant", „Guardian", 20 czerwca 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.
[40] A. Chen, „GCreep: Google Engineer Stalked Teens, Spied on Chats", Gawker, 14 września 2010, http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats.

[41] J. Kincaid, „This Is the Second Time a Google Engineer Has Been Fired for Accessing User Data", „TechCrunch", 14 września 2010, http://techcrunch.com/2010/09/14/google-engineer-fired-security/.
[42] B. Ross, V. Walter, A. Schecter, „Inside Account of U.S. Eavesdropping on Americans", ABC News, 9 października 2008. Dostępny w internecie: http://abcnews. go.com/Blotter/exclusive-inside-account-us-eavesdropping-americans/story? id=5987804.
[43] „Immersion: A People-centric View of Your Email Life", MIT Media Lab, https://immersion.media.mit.edu/ [dostęp: 20.08. 2013].
[44] D. Crawford, „NSA-Proof Your E-Mail in 2 Hours", blog: *Sealed Abstract*, 25 czerwca 2013, http://sealedabstract.com/code/nsa-proof-your-e-mail-in-2-hours/.
[45] Lavabit LLC, https://lavabit.com/ [dostęp: 2.07.2013; strona nie istnieje].
[46] M. Phillips, „How the Government Killed a Secure E-Mail Company", blog: *Elements*, „New Yorker", 8 sierpnia 2013, http://www.newyorker.com/online/blogs/elements/2013/08/the-government-versus-your-secrets.html.
[47] „About Us", Riseup. net, https://help.riseup.net/en/about-us [dostęp: 20.08. 2013].
[48] „Gdy wysyłacie e-mail poprzez riseup. net, wasz adres internetowy (adres IP) nie załączy się w wiadomości", Riseup. net – Riseup Email Help, https://help.riseup.net/en/email [dostęp: 20.08.2013].
[49] „Serwery poczty e-mail Lavabit rejestrują adres IP wykorzystywany do wysłania wiadomości wychodzącej – znajduje się on w nagłówku wychodzącej wiadomości. Z tego powodu, odbiorca wiadomości może wskazać adres IP, z jakiego wiadomość została do niego przesłana. Rejestrujemy tę informację w nagłówku wiadomości, aby organy ścigania mające w posiadaniu wiadomości naruszające przepisy prawa, mogły wskazać ich pierwotnego nadawcę. Lavabit nie gromadzi tych informacji", https://lavabit.com/privacy_policy.html [dostęp 2.07.2013; strona nie istnieje].
[50] „Social Contract", Riseup. net, https://help.riseup.net/en/social-contract.
[51] „Email Storage Quota", Riseup. net, https://www.riseup. net/en/quota.
[52] „Privacy Policy", Riseup. net, https://help.riseup.net/en/privacy-policy [dostęp: 20.08.2013].

[53] Ustawa o prywatności w łączności elektronicznej, https://it.ojp.gov/default.aspx? area=privacy&page=1285.
[54] M. Baker, „Thunderbird: Stability and Community Innovation", blog: *Lizard Wrangling*, 6 lipca 2012, http://blog.lizardwrangler.com/2012/07/06/thunderbird-stability-and-community-innovation/.
[55] „Postbox", Postbox, Inc., http://www.postbox-inc.com/index.php [dostęp: 20.08.2013].
[56] Sprawa przeciwko Google, Inc., sygn. 5:13-md-02430, Sąd Dystryktowy Stanów Zjednoczonych dla Północnego Dystryktu Kalifornii, 2013.
[57] Wniosek obrońcy Google, Inc. o oddalenie powództwa zbiorowego; „Memorandum of Points and Authorities in Support Thereof at 19", sprawa przeciwko Google, Inc. sygn. 5:13-md-02430, Sąd Dystryktowy dla Północnego Dystryktu Kalifornii, 2013.
[58] Lavabit LLC, https://lavabit.com/ [dostęp: 2.08.2013; strona nie istnieje].
[59] N. Perloth, S. Shane, „As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm", „New York Times", 3 października 2013, http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html? pagewanted=all&r=0.
[60] R. Singel, „Encrypted E-Mail Company Hushmail Spills to Feds", „Wired", 7 listopada 2007, http://www.wired.com/threatlevel/2007/11/encrypted-e-mai/.
[61] S. Sengupta, „Lavabit Founder Says He Had ‚Obligation' to Shut Service", blog: *Bits*, „New York Times", 12 sierpnia 2013, http://bits. blogs.nytimes.com/2013/08/12/lavabit-founder-says-he-had-obligation-to-shut-service/? r=0.
[62] L. Levinson, „My Fellow Users...", fanpage Lavabit LLC's, 8 sierpnia 2013, https://www.facebook.com/permalink.php?story_fbid=529849123730760&id=43228508348716.
[63] J. Callas, „To Our Customers", blog: *Silent Circle*, 9 sierpnia 2013, http://silentcircle. wordpress.com/2013/08/09/to-our-customers/.
[64] „Riseup and Government FAQ", Riseup. net, https://www.riseup.net/en/riseup-and-government-faq [dostęp: 20.08.2013].

ROZDZIAŁ 9: POZNAJCIE IDĘ

[1] K. Brady, *Ida Tarbell: Portrait of a Muckraker*, Seaview/Putnam, Nowy Jork 1984.
[2] J.T. Hancock, M.T. Woodworth, S. Goorha, „See No Evil: The Effect of Communication Medium and Motivation on Deception Detection", „Group Decision and Negotiation", lipiec 2009, nr 4, s. 327–43.
[3] J. Guillory, J.T. Hancock, „The Effect of LinkedIn on Deception in Resumes", „Cyberpsychology, Behavior, and Social Networking", luty 2012, nr 3, s. 135–40.
[4] J.T. Hancock, „The Future of Lying", wykład z serii TEDx, Winnipeg, Kanada, 13 września 2012, http://www.ted.com/talks/jeffhancock3typesofdigitallies.html#63003.
[5] J.T. Hancock, C. Toma, N. Ellison, „The Truth About Lying in Online Dating Profiles", „Proceedings of the SIGCHI Conference on Human Factors in Computing Systems" 2007, s. 449–52. Dostępny w internecie: http://dl. acm.org/citation.cfm? doid=1240624.1240697.
[6] Hancock, „The Future of Lying".
[7] D. Warkentin, M. Woodworth, J.T. Hancock, N. Cormier, „Warrants and Deception in Computer Mediated Communication", „Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work" 2010, s. 9–12. Dostępny w internecie: https://dl.acm.org/citation.cfm? id=1718922.
[8] I. Kant, *O domniemanym prawie do kłamstwa z pobudek miłości ludzkiej*, 1797.
[9] S. Bok, *Lying: Moral Choice in Private and Public Life*, Vintage, Nowy Jork 1999, s. 93.
[10] „Industry Group Adopts Foundation Standard for New Distribution Capability" (komunikat prasowy), Międzynarodowe Zrzeszenie Przewoźników Powietrznych, 19 października 2012, http://www.iata.org/pressroom/pr/pages/2012-10-19-02.aspx.
[11] „Frequent Fliers, Prepare to Pay More", „New York Times", 3 marca 2013, http://www.nytimes.com/2013/03/04/opinion/frequent-fliers-prepare-to-pay-more.html.
[12] J. Weiczner, „How the Insurer Knows You Just Stocked Up on Ice Cream and Beer", „Wall Street Journal", 25 lutego 2013. Dostępny w internecie: http://online.wsj.com/article/SB10001424127887323384604578326151014237
[13] P. Myerberg, „Dr. Phil: Tuiasosopo, romantically in love' with Te'o", „USA Today", 30 stycznia 2013,

http://www.usatoday.com/story/gameon/2013/01/30/dr-phil-ronaiah-tuiasosopo-confused-sexual-identity/1876995/.
[14] Jon Callas w rozmowie z autorką, 5 września 2012.
[15] Michael Sussmann w rozmowie z autorką, 23 stycznia 2013.
[16] „Tor: Overview", Tor Project, https://www.torproject.org/about/overview.html.en [dostęp: 2 października 2013].
[17] Amazon.com, Inc., „Amazon Betterizer", http://www.amazon.com/gp/betterizer [dostęp: 21.08.2013].
[18] H.N. Foerstel, *Surveillance in the Stacks: The FBI's Library Awareness Program*, Greenwood Press, Westport (Connecticut) 1991.
[19] American Library Association, „State Privacy Laws Regarding Library Records", http://www.ala.org/offices/oif/ifgroups/stateifcchairs/stateifcinaction/statep
[20] Marina Hoffmann Norville (wiceprezes, dyrektor komunikacji korporacyjnej w American Express) w rozmowie z Lauren Kirchner, 4 października 2013.
[21] „How Spamgourmet Works", https://spamgourmet.com/.
[22] MaskMe, Abine, Inc., https://www.abine.com/maskme/.
[23] „FAQ – Bitcoin", https://en. bitcoin. it/wiki/FAQ#HowcanIgetbitcoins.3F [dostęp: 21.08.2013].
[24] A. Chen, „The Underground Website Where You Can Buy Any Drug Imaginable", Kotaku.com, 1 czerwca 2011, http://kotaku.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable.
[25] K. Hill, „Living on Bitcoin for a Week: The Journey Begins", Forbes.com, 1 maja 2013, http://www.forbes.com/sites/kashmirhill/2013/05/01/living-on-bitcoin-for-a-week-the-journey-begins/.
[26] „Digital Currency E-Gold Indicted for Money Laundering and Illegal Money Transmitting" (komunikat prasowy), Departament Sprawiedliwości Stanów Zjednoczonych, 27 kwietnia 2007, http://www.justice.gov/opa/pr/2007/April/07crm 301.html.
[27] „Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges" (komunikat prasowy), Departament Sprawiedliwości Stanów Zjednoczonych, 21 lipca 2008, http://justice.gov/opa/pr/2008/July/08crm_635.html.
[28] M. Santora, W.K. Rashbaum, N. Perlroth, „Online Currency

Exchange Accused of Laundering $6 Billion", „New York Times", 28 maja 2013, http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html? ref=technology.
[29] D. McCullagh, „Crypto-Convict Won't Recant", Wired.com, 14 kwietnia 2000, http://www.wired.com/politics/law/news/2000/04/35620.
[30] J. Bell, „Assassination Politics", wiadomość na Google Groups, 23 stycznia 1996, https://groups. google.com/forum/? hl=en#! search/assasination $20politics $20jim $20bell|sort: date/list. libernet/Mo2RIiViYDE/Pp7BMppVDBYJ.
[31] „Bell Gets 11 Months in Prison, 3 Years Supervised Release, Fine", Associated Press, 12 grudnia 1997, http://cryptome.org/jdb/jimbell7.htm.
[32] D. Graeber, *Debt: The First 5,000 Years*, Melville House, Nowy Jork 2010, s. 120.

ROZDZIAŁ 10: PRZETRZĄSANIE KIESZENI

[1] J. Angwin, „Secret Orders Target Email", „Wall Street Journal", 9 października 2011. Dostępny w internecie: http://online.wsj.com/article/SB10001424052970203476804576613284007310
[2] I. Hunt, „The CIA's ‚Grand Challenges' with Big Data", GigaOM Structure: Data Conference 2013, http://new. livestream.com/accounts/74987/events/1927733/videos/14306067.
[3] D. McCullagh, A. Broache, „FBI Taps Cell Phone Mic as Eavesdropping Tool", CNET News, 1 grudnia 2006, http://news. cnet.com/2100-1029-6140191.html.
[4] „Verizon Forced to Hand Over Telephone Data – Full Court Ruling", „Guardian", 5 czerwca 2013, http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[5] Barack Obama w rozmowie z Charlie'em Rose'em, 16 czerwca 2013, http://www.charlierose.com/watch/60230424.
[6] E. Lichtblau, „Wireless Firms Are Flooded by Requests to Aid Surveillance", „New York Times", 8 lipca 2013, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&r=0.
[7] J. Angwin, S. Thurm, „Judges Weigh Phone Tracking", „Wall Street Journal", 9 listopada 2011,

http://online.wsj.com/article/SB10001424052970203733504577024092345458
[8] Nr 08-4227, „In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government", Sąd Apelacyjny USA dla Trzeciego Okręgu, 7 września 2010, https://www.eff.org/files/3d%20Circuit%20Opinion%20%28Cell%20Site%29
[9] Nr 11-20884, „In Re: Application of the United States of America for Historical Cell Site Data", Sąd Apelacyjny USA dla Piątego Okręgu, 30 lipca 2013, http://legaltimes.typepad.com/files/cell-site-5th.pdf.
[10] „The Origination and Evolution of Radio Traffic Analysis: The World War I Era", „Cryptologic Quarterly" (data publikacji nieznana), s. 21–40, http://www.nsa.gov/publicinfo/_files/cryptologicquarterly/trafficanalysis.p
[11] G. Danezis, R. Clayton, „Introducing Traffic Analysis", 26 stycznia 2007, https://research.microsoft.com/en-us/um/people/gdane/papers/TAIntro-book.pdf.
[12] „The Origination and Evolution of Radio Traffic Analysis".
[13] Praca zbiorowa, „Computerizing Traffic Analysis" [w:] „A Collection of Writings on Traffic Analysis, Vol. 4: Sources in Cryptologic History, Center for Cryptologic History", Agencja Bezpieczeństwa Krajowego, 1993. Dostępny w internecie: http://www.governmentattic.org/8docs/NSA-TrafficAnalysisMonograph1993.pdf.
[14] M. Apuzzo, „Hezbollah Unravels CIA Spy Network in Lebanon", Associated Press, 21 listopada 2011, http://www.guardian.co.uk/world/feedarticle/99 58834.
[15] „Retention Periods for Major Cellular Service Providers", Departament Sprawiedliwości Stanów Zjednoczonych, sierpień 2010, http://www.aclu.org/files/pdfs/freespeech/retentionperiodsofmajorcellulars
[16] S. 30 (111), „Truth in Caller ID Act of 2009", 22 grudnia 2010, http://www.govtrack.us/congress/bills/111/s30/text.
[17] Harlo Holmes w korespondencji e-mailowej z autorką, 19 maja 2013.
[18] Moxie Marlinspike w rozmowie z autorką, 20 marca 2013.
[19] J. Angwin, J. Valentino-Devries, „Apple, Google Collect User Data", „Wall Street Journal", 20 kwietnia 2011, http://online.wsj.com/article/SB10001424052748703983704576277101723453
[20] S. Thurm, Y.I. Kane, „Your Apps Are Watching You", „Wall Street Journal", 17 grudnia 2010,

http://online.wsj.com/article/SB10001424052748704694004576020083703
[21] A. Troianovski, „New Wi-Fi Pitch: Tracker", „Wall Street Journal", 18 czerwca 2012, http://online.wsj.com/article/SB10001424052702303379204577474961075248
[22] S. Datoo, „This Recycling Bin Is Following You", „Quartz", 8 sierpnia 2013, http://qz.com/112873/this-recycling-bin-is-following-you/.
[23] Z.M. Seward, S. Datoo, „City of London Halts Recycling Bins Tracking Phones of Passers-by", „Quartz", 12 sierpnia 2013, http://qz.com/114174/city-of-london-halts-recycling-bins-tracking-phones-of-passers-by/.
[24] Datoo, „This Recycling Bin Is Following You".
[25] „Our Mea sure ment Solutions", Verizon Wireless, http://business.verizonwireless.com/content/b2b/en/precision/our-measurement-solutions.html.
[26] „Our Updated Privacy Policy", AT&T, 28 czerwca 2013, http://www.attpublicpolicy.com/privacy/our-updated-privacy-policy-2/.
[27] Location Intelligence Conference, http://www.locationintelligence.net/.
[28] Geoweb Summit, http://geowebsummit.com/.
[29] Location Business Summit USA, http://www.mformobile.com/location-business-summit-usa/.
[30] Signal Conference: Chicago, http://www.federatedmedia.net/events/11/.
[31] JiWire, http://jiwire.com/audience.
[32] D. Staas (prezes zarządu JiWire), „Using Location Patterns to Power Big Data on Mobile", Signal Conference, Chicago, Illinois, 11 września 2012, http:// link.brightcove.com/services/player/bcpid1450672650001?bckey=AQ~~, AAA AFktgNgk~, QKA7V92zyumLLIZb3v45LGr2NPa naTlq&bclid=1826428698001&bctid=1843067500001.
[33] Will Smith w korespondencji z Alem Frankenem, 28 marca 2013, http://www.franken.senate.gov/files/docs/130328Euclid.pdf.
[34] „Sens. Franken, Blumenthal Introduce Bill to Protect Consumer Privacy on Mobile Devices" (komunikat prasowy), 15 czerwca 2011, http://www.franken.senate.gov/? p=pressrelease&id=1587.
[35] Will Smith w korespondencji z Alem Frankenem, 28 marca 2013.
[36] Y.-A. de Montjoye, C.A. Hidalgo, M. Verelysen, V.D. Blondel, „Unique in the Crowd: The Privacy Bounds of Human Mobility", „Scientific Reports", marzec 2013, nr 1376.

[37] A. Sadilek, J. Krumm, „Far Out: Predicting Long-Term Human Mobility", Association for the Advancement of Artificial Intelligence, 2012, https://research.microsoft.com/en-us/um/people/jckrumm/Publications%202012/Sadilek-KrummFar-OutAAAI-2012.pdf.
[38] „Greater Choice for Wireless Access Point Owners", oficjalny blog Google, Inc., 14 listopada 2011, http://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html.
[39] G. Dayal, „QuickStudy: Faraday Cages", „Computerworld", 23 sierpnia 2006. Dostępny w internecie: http://www.computerworld.com/s/article/9002661/Faradaycages?pageNumber=1.
[40] „Faraday Cages in Health Care", TNO Prevention and Health, http://web.archive.org/web/20060324100513/http://www.tno.nl/kwaliteit_zorg/faradaycagesinhealthc/046.pdf.
[41] John Strauchs w rozmowie z autorką, 5 marca 2013.
[42] Adam Harvey w rozmowie z autorką, 19 kwietnia 2013.
[43] Adam Harvey korespondencja z autorką, 12 sierpnia 2013.

ROZDZIAŁ 11: PROCEDURA WYJŚCIA

[1] „Privacy Policy: LinkedIn", LinkedIn Corp., http://www.linkedin.com/legal/privacy-policy [dostęp: 21.05.2013; od tego czasu zmienił się język komunikatu].
[2] Doug Madey (pracownik działu komunikacji, LinkedIn Corp.) w korespondencji e-mail z Lauren Kirchner, 12 września 2013.
[3] D. Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*, Harper Perennial, Nowy Jork 2009, s. 150.
[4] Tamże, s. 147.
[5] Autorka w rozmowach z Alexem Bennertem 26 lutego 2013 oraz z Rhea Drysdale 11 marca 2013.
[6] E. Mills, „LinkedIn Confirms Passwords Were ‚Compromised'", CNET, 6 czerwca 2012, http://news.cnet.com/8301-1009_3-57448465-83/linkedin-confirms-passwords-were-compromised/.
[7] „Privacy Policy: LinkedIn", LinkedIn Corporation.
[8] J. Donath, D. Boyd, „Public Displays of Connection", „BT Technology Journal", październik 2004, nr 22, s. 73,

http://www.danah.org/papers/PublicDisplays.pdf.
[9] N. Ambady, R. Rosenthal, „Thin Slices of Expressive Behavior as Predictors of Interpersonal Consequences: A Meta-Analysis", „Psychological Bulletin" 1992, nr 111, s. 256, http://ambadylab.stanford.edu/pubs/1992Ambady.pdf.
[10] L.F. Sessions, „*You Looked Better on MySpace*: Deception and Authenticity on Web 2.0", First Monday, vol 14, 6 lipca 2009, nr 7, http://firstmonday.org/ojs/index.php/fm/article/view/2539/2242#4a.
[11] J.S. Donath, „Identity and Deception in the Virtual Community", [w:] *Communities in Cyberspace*, Routledge, Nowy Jork 1999, s. 27.
[12] Tamże, s. 54.
[13] Tamże, s. 30.
[14] Donath, Boyd, „Public Displays of Connection", s. 72.
[15] Judith Donath w rozmowie z autorką, 4 kwietnia 2013.
[16] Gaebriella Todesco w rozmowie z autorką, 7 grudnia 2011.
[17] Gaebriella Todesco w rozmowie z autorką, 23 stycznia 2013.
[18] Gaebriella Todesco, e-mail do autorki, 21 marca 2013.
[19] Todesco w rozmowie z autorką, 7 grudnia 2011.
[20] Todesco w rozmowie z autorką, 23 stycznia 2013.
[21] E. Nakashima, „Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy", „Washington Post", 30 listopada 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503.html.
[22] J.C. Perez, „Facebook Will Shut Down Beacon to Settle Lawsuit", IDG News Service, 18 września 2009, http://www.pcworld.com/article/172272/facebookwillshutdownbeacontoset lawsuit.html.
[23] R. Pegoraro, „Facebook *Sponsored Stories* Turn You into the Ad", „Washington Post", 27 stycznia 2011, http://voices.washingtonpost.com/fasterforward/2011/01/facebooksponsore storiestur.html.
[24] D. Levine, „U.S. Judge Approves Facebook Privacy Settlement over Ads", Reuters, 26 sierpnia 2013, http://www.reuters.com/article/2013/08/26/net-us-facebook-privacy-settlement-idUSBRE97P0VG20130826.
[25] J. Guynn, „Facebook under Fire from Privacy Watchdogs over *Sponsored Stories* Ads", „Los Angeles Times", 4 września 2013.
[26] A. Oreskovic, „Google Unveils Plans for User Names, Comments to

Appear in Ads", Reuters, 14 października 2013, http://www.reuters.com/article/2013/10/14/net-us-google-ads-idUSBRE99A0S720131014.
[27] Ruchi Sanghvi, „New Tools to Control Your Experience", Facebook Blog, 9 grudnia 2009, http://blog.facebook.com/blog.php?post=196629387130.
[28] J. Angwin, „How Facebook Is Making Friending Obsolete", „Wall Street Journal", 15 grudnia 2009, http://online.wsj.com/article/SB126084637203791583.html.
[29] „Facebook Settles FTC Charges Th at It Deceived Consumers by Failing to Keep Privacy Promises", Federalna Komisja Handlu, 29 listopada 2011, http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.
[30] Zasady dotyczące danych, Facebook, https://www.facebook.com/fulldatausepolicy [ostatnio zmieniana: 11.12.2012].
[31] J. Angwin, „How Are You? No, How Are You Really?", „Wall Street Journal", 16 czerwca 2009, http://online.wsj.com/article/SB124510254756316521.html.
[32] Catalog Choice, TrustedID, https://www.catalogchoice.org/.
[33] „DeleteMe – Protect Your Personal Data and Reputation Online", Abine Inc., http://www.abine.com/deleteme/landing.php [dostęp: 21.05.2013].
[34] Jim Adler w rozmowie z autorką, 10 kwietnia 2013.
[35] Sarah Downey w rozmowie z autorką, 12 kwietnia 2013.
[36] „Privacy Policy Highlights", USA People Search, 7 maja 2013, http://www.usa-people-search.com/privacy.aspx.
[37] Sarah Downey, e-mail do autorki, 13 maja 2013.
[38] Lyn Chitow Oakes (rzeczniczka prasowa TrustedID Catalog Choice), e-maile wymieniane z autorką w dniu 29 lipca 2013.
[39] Free Phone Tracer, http://www.freephonetracer.com/.
[40] „Public Profile FAQ's", MyLife.com, Inc., http://www.mylife.com/faq.pub [dostęp: 21.05.2013].
[41] „How We're Different", PeopleSmart.com, http://www.peoplesmart.com/difference [dostęp: 4.10.2013].
[42] „Careers", Inflection LLC, http://inflection.com/careers/ [dostęp: 21.05.2013].
[43] Matthew Monahan, e-mail do autorki, 6 maja 2013.
[44] Matthew Monahan, e-mail do autorki, 7 maja 2013.

[45] Matthew Monahan w rozmowie z autorką, 14 maja 2013.
[46] M. Alex Johnson, „Cell Phone Directory Rings Alarm Bells", NBC News, 30 stycznia 2008, http://www.nbcnews.com/id/22902400/.
[47] S. Choney, „Company Shuts Down Cell Phone Directory", NBC News, 1 lutego 2008, http://www.nbcnews.com/id/22956815/.
[48] „Inflection Sells Archives.com to Ancestry.com Inc.", Inflection LLC, PR Newswire, 25 kwietnia 2012, http://www.prnewswire.com/news-releases/inflection-sells-archivescom-to-ancestrycom-inc-148969015.html.
[49] Matthew Monahan w rozmowie z autorką, 14 maja 2013.

ROZDZIAŁ 12: GABINET LUSTER

[1] Rayne Puertos w rozmowie z autorką, 12 lutego 2013.
[2] „The State of Data Collection on the Web", Krux Cross Industry Study, 2013.
[3] J. Angwin, „The Web's New Gold Mine: Your Secrets", „Wall Street Journal", 30 lipca 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989
[4] S. Stecklow, „On the Web, Children Face Intensive Tracking, „„Wall Street Journal", 17 września 2010, http://online.wsj.com/article/SB10001424052748703904304575497903523187
[5] M. Barbaro, T. Zeller Jr., „A Face Is Exposed for AOL Searcher No. 4417749", „New York Times", 9 sierpnia 2006. Dostępny w internecie: http://www.nytimes.com/2006/08/09/technology/09aol.html?r=0&gwh=2CACC912D19D87BDFD3A39B96C429022.
[6] A. Narayanan, V. Shmatikov, „Robust De-anonymization of Large Sparse Datasets", „Security and Privacy", 2008, s. 111–25, http://www.cs.utexas.edu/~shmat/shmatoak08netflix.pdf.
[7] J. Valentino-Devries, J. Singer-Vine, „They Know What You're Shopping For", „Wall Street Journal", 7 grudnia 2012, http://online.wsj.com/article/SB10001424127887324784404578143144132736214
[8] M.R. Calo, „Digital Market Manipulation" (praca badawcza nr 2013–27), Szkoła Prawa Uniwersytetu Waszyngton, 15 sierpnia 2013, http://papers.ssrn.com/sol3/papers.cfm? abstract_id=2309703.
[9] L. Brandimarte, A. Acquisti, G. Loewenstein, „Misplaced Confidences: Privacy and the Control Paradox", „Social Psychological and Personality Science", 9 sierpnia 2012,

http://spp.sagepub.com/content/early/2012/08/08/1948550612455931.abstra
[10] Calo, „Digital Market Manipulation".
[11] B.R. Shiller, „First Degree Price Discrimination Using Big Data" (dokument roboczy), Uniwersytet Brandeis, 20 sierpnia 2013, http://www.brandeis.edu/departments/economics/RePEc/brd/doc/Brandeis
[12] „Incognito Mode (Browse in Private)", Google, Inc., https://support.google.com/chrome/answer/95464? hl=en [dostęp: 22.08.2013].
[13] „Consumer Opt-Out", Network Advertising Initiative, http://www.networkadvertising.org/choices/.
[14] 2013 Krux Cross Industry Study.
[15] Adblock Plus, https://adblockplus.org/.
[16] NoScript Firefox extension, Inform Action, Open Source Software, noscript.net.
[17] DoubleClick by Google, http://www.google.com/doubleclick/ [dostęp: 28.03.2013].
[18] „Data Drives Everything" AddThis, http://www.addthis.com/data [dostęp: 28.03.2013].
[19] ConvergeDirect, http://www.convergedirect.com/technology/convergetrack/ [dostęp: 28.03.2013].
[20] „Join the Bazaarvoice Network", 2013, http://www.bazaarvoice.com/ [dostęp: 28.03.2013].
[21] „IBM Product Recommendations", http://www-03.ibm.com/software/products/us/en/personalized-product-recommendations/ [dostęp: 28.03.2013].
[22] Sarah Promisloff, e-mail do autorki, 27 czerwca 2013.
[23] „Privacy Policy", FreshDirect, LLC, https://www.freshdirect.com/help/privacypolicy.jsp [dostęp: 22.08.2013].
[24] Dan Jaye w rozmowie z autorką, 6 maja 2010.
[25] P.C. Judge, „David Wetherell: Internet Evangelist", „BusinessWeek", 25 października 1999, http://www.businessweek.com/1999/99_43/b3652001.htm.
[26] K. Regan, „Fallen Dot-Com Star CMGI Drops Stadium Deal", „E-Commerce Times", 6 sierpnia 2002, http://www.ecommercetimes.com/story/commerce/18904.html.
[27] Dan Jaye w rozmowie z autorką, 6 maja 2010.
[28] K. Kaye, „Tacoda Buy Could Bolster AOL Relevance in Web Ad

Arena", Clickz, 24 lipca 2007, http://www.clickz.com/clickz/news/1712324/tacoda-buy-could-bolster-aols-relevance-web-ad-arena.
[29] P.R. La Monica, „Google to Buy DoubleClick for $3.1 Billion", CNN Money, 13 kwietnia 2007, http://money.cnn.com/2007/04/13/technology/googledoubleclick/index.htr
[30] Ch. Isidore, „Microsoft Buys aQuantive for $6 Billion, Pays 85% Premium", CNN Money, 18 maja 2007, http://money.cnn.com/2007/05/18/technology/microsoftaquantive/.
[31] L. Bell, „New Online Data Company BlueKai Strives for Quality, Privacy", „Direct Marketing News", 15 września 2008, http://www.dmnews.com/new-online-data-company-bluekai-strives-for-quality-privacy/article/116668/.
[32] AdAge, „Custom Programs: BlueKai", http://brandedcontent.adage.com/adnetworkguide10/network.php?id=20 [dostęp: 5.10.2013].
[33] J. Angwin, „The Web's New Gold Mine: Your Secrets", „Wall Street Journal", 30 lipca 2010, http://online.wsj.com/article/SB100 01424052748703940904575395073512980
[34] E. Steel, „A Web Pioneer Profiles Users by Name", „Wall Street Journal", 25 października 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416
[35] Dan Jaye w rozmowie z autorką, 6 maja 2010.
[36] Tamże.
[37] A. Barr, „Google May Ditch *Cookie* as Online Ad Tracker", „USA Today", 17 września 2013, http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/.
[38] A. Tanner, „The Web Cookie Is Dying. Here's the Creepier Technology That Comes Next", „Forbes", 17 czerwca 2013, http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/.
[39] Ulotka FaceFirst, FaceFirst, LLC.
[40] Ch. Trlica, „Facial Recognition: A Game-Changing Technology for Retailers", „LP Magazine", maj-czerwiec 2013, http://www.lpportal.com/feature-articles/item/2482-facial-recognition-a-game-changing-technology-for-retailers.html.
[41] Ulotka FaceFirst.

[42] „How to Make an Infrared Mask to Hide Your Face from Cameras", WonderHowTo, opublikowany przez Amie, http://mods-n-hacks.wonderhowto.com/how-to/make-infrared-mask-hide-your-face-from-cameras-201280/.
[43] A. Harvey, „Exhibition: Stealth Wear: New Designs for Counter Surveillance", Primitive London, 4 stycznia 2013, http://www.primitivelondon.co.uk/exhibition-adam-harvey-stealth-wear-new-designs-for-counter-surveillance-presented-by-primitive-london-and-tank-magazine/.
[44] Ashkan Soltani w rozmowie z autorką, 29 marca 2013.
[45] Ashkan pokazał mi także dwa sposoby optymalizacji pracy wyszukiwarki, które zakładały pominięcie ostrzeżenia: „Zmiana tych zaawansowanch ustawień może zagrażać stabilności, bezpieczeństwu i działaniu tej aplikacji". Były to następujące sztuczki: włączyłam „Click_to_play", co uniemożliwiało działanie wtyczek dopóki sama ich nie aktywowałam, oraz ustawiłam skrypt „network.http.sendReferer-Header=0", który czyści nagłówki adresów w trakcie surfowania w sieci, dzięki czemu strony internetowe, które odwiedzam, nie wiedzą skąd się łączę.
[46] D. Cancel, „The Future of Ghostery", blog Davida Cancela, 19 stycznia 2010, http://davidcancel.com/the-future-of-ghostery/.
[47] A. DeMartino, „Better Advertising Acquires Ghostery", blog: *The Evidon*, 19 stycznia 2010, http://www.evidon.com/blog/better-advertising-acquires-ghostery.
[48] Istnieją także inne kompleksowe listy elementów do blokowania pochodzące ze społecznego źródła – takie jak EasyPrivacy, która może być dodana do rozszerzenia AdblockPlus – https://easylist-downloads.adblockplus.org/easyprivacy.txt. (5 października 2013 lista zawierała 8 376 elementów).
[49] Andy Kahl w rozmowie z autorką, 30 maja 2013.
[50] J. Angwin, „Wall Street Journal Privacy Series Inspires One Start-Up", blog: *Digits*, „Wall Street Journal", 27 lutego 2011, http://blogs.wsj.com/digits/2011/02/27/wall-street-journal-privacy-series-inspires-one-start-up/.
[51] A. Tsotsis, „Google Engineer Builds Facebook Disconnect", „TechCrunch", 20 października 2010, http://techcrunch.com/2010/10/20/google-facebook-disconnec/.
[52] Angwin, „One Start-Up".

[53] A. Tsotsis, „Former Googler Launches Disconnect, Browser Extension That Disables Third Party Data Tracking", „TechCrunch", 13 grudnia 2010, http://techcrunch.com/2010/12/13/former-googler-launches-disconnect-browser-extension-that-disables-third-party-data-tracking/.
[54] R. Empson, „Disconnect: Ex- Googlers Raise Funding to Stop Google, Facebook & More from Tracking Your Data", „TechCrunch", 22 marca 2012, http://techcrunch.com/2012/03/22/disconnect-me-raise/.
[55] Brian Kennish w rozmowie z autorką, 16 sierpnia 2012.
[56] Tamże.

ROZDZIAŁ 13: SAMOTNE KODY

[1] „The GNU Privacy Guard", Free Soft-ware Foundation, Inc., http:/gnupg.org/.
[2] „A Simple Interface to OpenPGP Email Security", The Enigmail Project, https://www.enigmail.net/home/index.php.
[3] „GnuPG Frequently Asked Questions", GnuPG, http://www.gnupg.org/faq/GnuPG-FAQ.html.
[4] „Extending Postbox", Postbox, Inc., http://www.postbox-inc.com/extensions.
[5] SourceForge, Inc., „PostBox 3.0.7 and Enigmail 1.2.3 Freezing Problem" (forum), http://sourceforge.net/p/enigmail/forum/support/thread/bfd56f75/?limit=25 #1d58.
[6] „The CrytpoParty handbook", wersja z 21 sierpnia 2013, http://www.cryptoparty.in/documentation/handbook.020-56903_ch01_2P.indd26311/27/138:43PM
[7] D. Yadron, „Snowden's Email Service Shuts", blog: *Digits*, „Wall Street Journal", 8 sierpnia 2013, http://blogs.wsj.com/digits/2013/08/08/snowdens-email-service-shuts/; oraz: „Snowden to Meet with Human Rights Groups in Moscow", Novinvite.com, 12 lipca 2013, http://www.novinite.com/viewnews.php?id=151966.
[8] „Angwin GPG Key", strona internetowa autorki, 11 lipca 2013, http://juliaangwin.com/contact/ed06b6f6/.
[9] Ch. Soghoian w rozmowie z autorką, 5 czerwca 2013.
[10] D. Robinson w rozmowie z autorką, 6 czerwca 2013.

[11] K. Fogel, „Karl Fogel's GPG Public Key", 22 listopada 2010, http://www.red-bean.com/kfogel/public-key.html.
[12] S. Stellin, „The Border Is a Back Door for U.S. Device Searches", „New York Times", 9 września 2013, http://www.nytimes.com/2013/09/10/business/the-border-is-a-back-door-for-us-device-searches.html.
[13] „U.S. Settles Lawsuit with Bradley Manning Supporter Who Had Laptop Seized at Airport", ACLU.org (komunikat prasowy), https://www.aclu.org/free-speech/us-settles-lawsuit-bradley-manning-supporter-who-had-laptop-seized-airport.
[14] V. Silver, „Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma", Bloomberg.com, 26 lipca 2012, http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html.
[15] N. Perlroth, „Software Meant to Fight Crime Is Used to Spy on Dissidents", „New York Times", 20 sierpnia 2012, http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html? ref=technology&r=0.
[16] V. Silver, „Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy", Bloomberg.com, 27 lipca 2012, http://www.bloomberg.com/news/2012-07-27/gamma-says-no-spyware-sold-to-bahrain-may-be-stolen-copy.html.
[17] J. Valentino-DeVries, J. Angwin, S. Stecklow, „Document Trove Exposes Surveillance Methods", „Wall Street Journal", 19 listopada 2011, http://online.wsj.com/article/SB10001424052970203611404577044192607407
[18] „The Surveillance Catalog", „Wall Street Journal", zaktualizowany 7 lutego 2012, http://projects.wsj.com/surveillance-catalog/.
[19] „Remote Monitoring and Infection Solutions, FinSpy" (broszura), FinFisher, Gamma Group, [w:] The Surveillance Catalog, „Wall Street Journal", http://projects.wsj.com/surveillance-catalog/documents/267841-merged-finspy/.
[20] „Remote Control System: Cyber Intelligence Made Easy", HackingTeam, [w:] The Surveillance Catalog, „Wall Street Journal", http://projects.wsj.com/surveillance-catalog/documents/267005-hacking-team-remote-control-system/#document/p3/a38816.
[21] Valentino-Devries, Angwin, Stecklow, „Document Trove Exposes Surveillance Methods".
[22] D. McCullagh, „FBI Remotely Installs Spyware to Trace Bomb

Threat", CNET, 18 lipca 2007, http://news.cnet.com/8301-107843-9746451-7.html#!.
[23] „In Re Warrant to Search a Target Computer at Premises Unknown", sprawa sygn. H-13-234M, Sąd Dystryktowy USA dla Wschodniego Dystryktu Teksasu, 2013, http://files.cloudprivacy.net/Order%20denying%20warrant.MJ%20Smith.042213.pdf.
[24] S. Gorman, J. Valentino-Devries, „New Details Show Broader NSA Surveillance Reach", „Wall Street Journal", 20 sierpnia 2013, http://online.wsj.com/article/SB10001424127887324108204579022874091732
[25] E. Holder, „Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended", 28 lipca 2004. Dostępny w internecie: https://s3.amazonaws.com/s3.documentcloud.org/documents/716634/exhibb.pdf.
[26] William Binney w rozmowie z autorką, 18 marca 2012.
[27] William Binney, Thomas Drake i Kirk Wiebe w rozmowie z autorką 24 maja 2012.
[28] N. Borysow, I. Goldberg, E. Brewer, „Off-the-Record Communication, or, Why Not to Use PGP", 2004. Dostępny w internecie: http://www.cypherpunks.ca/otr/otr-wpes.pdf; oraz: B. Whitley, „Students Develop Encryption for Instant Messaging", „Daily Californian", 22 lutego 2005, http://www.cypherpunks.ca/otr/press/www.dailycal.org/article.php%3fid=1
[29] Borisov, Goldberg, Brewer, „Off-the-Record Communication, or, Why Not to Use PGP".
[30] „Documentation", Tails, https://tails.boum.org/doc/index.en.html.
[31] B. Manning, „Bradley Manning's Statement Taking Responsibility for Releasing Documents to WikiLeaks", 28 lutego 2013, http://www.bradleymanning.org/news/bradley-mannings-statement-taking-responsibility-for-releasing-documents-to-wikileaks.
[32] K. Poulsen, K. Zetter, „U.S. Intelligence Analyst Arrested in Wikileaks Video Probe", blog: *Threat Level*, „Wired", 6 czerwca 2010, http://www.wired.com/threatlevel/2010/06/leak/.
[33] E. Blum-Dumontet, „Bradley Manning Legal Proceedings: Fact Sheet", WikiLeaks Press, 31 marca 2012, http://wikileaks-

press.org/bradley-manning-legal-procedures-fact-sheet/.
[34] „Core Tor People", The Tor Project, https://www.torproject.org/about/corepeople.html.en.
[35] „Notices", Jabber, Inc., http://www.jabber.org/notices.html.
[36] „Off-the-Record Messaging", The OTR Development Team, http://www.cypherpunks.ca/otr/people.php.
[37] Evan Schoenberg w rozmowie z autorką, 25 listopada 2012.
[38] P. Zimmermann, „Creator of PGP and Zfone: Background", blog osobisty: *philzimmermann.com*, http://www.philzimmermann.com/EN/background/index.html.
[39] „The GNU Privacy Guard", GnuPG, http://gnupg.org/.
[40] E. Hughes, „A Cypherpunk's Manifesto", 9 marca 1993. Dostępny w internecie: http://www.activism.net/cypherpunk/manifesto.html.
[41] P. Zimmermann, „Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation", blog osobisty: *philzimmermann.com*, 26 czerwca 1996, http://www.philzimmermann.com/EN/testimony/.
[42] P. Zimmermann, „Signifi cant Moments in PGP's History: Zimmermann Case Dropped", blog osobisty: *philzimmermann.com*, 12 stycznia 1996, http://www.philzimmermann.com/EN/news/PRZ case_dropped.html.
[43] J. Clausing, „White House Eases Export Controls on Encryption", „New York Times", 17 września 1999, http://www.nytimes.com/library/tech/99/09/biztech/articles/17encrypt.htm
[44] J. Markoff, „Technology; Wrestling over the Key to the Codes", „New York Times", 9 maja 1993, http://www.nytimes.com/1993/05/09/business/technology-wrestling-over-the-key-to-the-codes.html.
[45] S. Levy, „Battle of the Clipper Chip", „New York Times", 12 czerwca 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html? pagewanted=all&src=pm.
[46] Matt Blaze w rozmowie z autorką, 8 maja 2013.
[47] B. Schneier, *Applied Cryptology: Protocols, Algorithms, and Source Code in C*, Wiley, Nowy Jork 1996.
[48] S. Lohr, „Technology; Privacy on Internet Poses Legal Puzzle", „New York Times", 19 kwietnia 1999, http://www.nytimes.com/1999/04/19/business/technology-privacy-on-

internet-poses-legal-puzzle.html.
[49] P.H. Lewis, „Computer Jokes and Threats Ignite Debate on Anonymity", „New York Times", 31 grudnia 1994, http://www.nytimes.com/1994/12/31/us/computer-jokes-and-threats-ignite-debate-on-anonymity.html? pagewanted=all&src=pm.
[50] D. Mandl, „Life After Penet: The Remailer Is Dead, Long Live the Remailer", „Village Voice", 8 października 1996, http://wfmu.org/~davem/docs/penet.html; oraz: P.H. Lewis, „Behind an Internet Message Ser vice's Close", „New York Times", 6 września 1996, http://www.nytimes.com/1996/09/06/business/behind-an-internet-message-service-s-close.html.
[51] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*, Wiley, Nowy Jork 2000.
[52] N. Perlroth, J. Larson, S. Shane, „N.S.A. Able to Foil Basic Safeguards of Privacy on Web", „New York Times", 5 września 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
[53] B. Schneier, „NSA Surveillance: A Guide to Staying Secure", „Guardian", 6 września 2013, https://www.schneier.com/essay-450.html.
[54] R. Khatchadourian, „No Secrets: Julian Assange's Mission for Total Transparency", „New Yorker", 7 czerwca 2010, http://www.newyorker.com/reporting/2010/06/07/100607fafactkhatchado currentPage=all.
[55] Moxie Marlinspike w rozmowie z autorką, 20 marca 2013.
[56] N. Scola, „The Guardian Project: Building Mobile Security for a Dangerous World", blog: *Tech President*, Personal Democracy Plus, 31 marca 2011, http://techpresident.com/blog-entry/guardian-project-building-mobile-security-dangerous-world.
[57] „The TOR Project, Inc. and Affiliate, Consolidated Financial Statements and Reports Required for Audits in Accordance with Government Auditing Standards and OMB Circular A-133", Moody, Famiglietti & Andronico, 31 grudnia 2011 (także 2010). Dostępny w internecie: https://www.torproject.org/about/findoc/2011-TorProject-Amended-Final-Report.pdf.
[58] J. Angwin, „Secret Orders Target Email", „Wall Street Journal", 9 października 2011, http://online.wsj.com/article/SB10001424052970203476804576613284007310 mod=WSJwhattheyknow2011LeftTopNews.

[59] J. Beckett, „New Company's Fast Start/Network Associates Buys Software Firm for $36 Million", „San Francisco Chronicle", 2 grudnia 1997. Dostępny w internecie: http://www.sfgate.com/business/article/New-Company-s-Fast-Start-Network-Associates-2792220.php.
[60] N. Perlroth, „Security Pioneer Creates Ser vice to Encrypt Phone Calls and Text Messages", blog: *Bits*, „New York Times", 5 lutego 2013, http://bits.blogs.nytimes.com/2013/02/05/security-pioneer-creates-service-to-encrypt-phone-calls-and-text-messages/.
[61] Mike Janke w rozmowie z autorką, 5 listopada 2012.
[62] Jon Callas w rozmowie z autorką, 5 kwietnia 2013.

ROZDZIAŁ 14: WALCZĄC ZE STRACHEM

[1] D.D. Broughton, „Keeping Kids Safe in Cyberspace", AAP News, 1 sierpnia 2005, http://aapnews.aappublications.org/content/26/8/11.full.
[2] „A Parent's Guide to Internet Safety", Raporty i Publikacje Federalnego Biura Śledczego, http://www.fbi.gov/stats-services/publications/parent-guide.
[3] „Stop. Think. Connect" (broszura), Departament Bezpieczeństwa Krajowego, http://www.dhs.gov/xlibrary/assets/stc/stc-chatting-with-kids-printable.pdf.
[4] „Table 1: Crime in the United States by Volume and Rate per 100,000 Inhabitants, 1990–2009", Federalne Biuro Śledcze, http://www2.fbi.gov/ucr/cius2009/data/table01.html.
[5] CompStat. Report Covering the Week 9/16/2013 Through 9/22/2013, Policja Miasta Nowy Jork, http://www.nyc.gov/html/nypd/downloads/pdf/crimestatistics/cscity.pdf.
[6] A.M. Destefano, „FBI Crime Stats Mixed for NYC", „Newsday", 13 czerwca 2013, http://www.newsday.com/news/new-york/fbi-crime-stats-mixed-for-nyc-1.5479442; oraz: „Crime in the United States 2012", Federalne Biuro Śledcze, http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012.
[7] D. Finkelhor, L. Jones, „Have Sexual Abuse and Physical Abuse Declined Since the 1990s?", Crimes Against Children Research Center, listopad 2012, http://www.unh.edu/ccrc/pdf/CV267Have%20SA%20%20PA%20DeclineFA
7-12.pdf.

[8] D. Finkelhor, „Trends in Bullying and Peer Victimization", Crimes Against Children Research Center, styczeń 2013, http://cola.unh.edu/sites/cola.unh.edu/files/CV280Bullying PeerVictimization_Bulletin1-23-13withtobyedits.pdf.
[9] „Teen Homicide, Suicide and Firearm Deaths", Child Trends Data Bank, http://www.childtrends.org/? indicators=teen-homicide-suicide-and-firearm-deaths.
[10] „Teen Births", Child Trends DataBank, http://childtrends.org/? indicators=teen-births.
[11] D. Finkelhor, „The Internet, Youth Safety and the Problem of ‚Juvenoia'", Crimes Against Children Research Center, styczeń 2011, http://www.unh.edu/ccrc/pdf/Juvenoia%20paper.pdf.
[12] M.R. Lepper, D. Greene, „Turning Play into Work: Effects of Adult Surveillance and Extrinsic Rewards on Children's Intrinsic Motivation", „Journal of Personality and Social Psychology" 1975, nr 31, s. 479–86, http://www.jwalkonline.org/docs/Grad%20Classes/Fall%2007/Org%20Psy/
[13] D. Lazarus, „Precious Photos Disappear", „San Francisco Chronicle", 2 lutego 2005, http://www.sfgate.com/business/article/Precious-photos-disappear-2734149.php.
[14] Tytuł XIII – Ustawa o ochronie prywatności dzieci w internecie z 1998 roku, Federalna Komisja Handlu, http://www.ftc.gov/ogc/coppa1.htm.
[15] A. Troianovski, D. Yadron, „U.S. Expands Child Online Privacy Law to Cover Apps, Social Networks", „Wall Street Journal", 19 grudnia 2012, http://online.wsj.com/article/SB10001424127887323777204578189430101877
[16] D. Boyd, „Why Parents Help Children Violate Facebook's 13+ Rule", blog: *Apophenia*, 1 listopada 2011, http://www.zephoria.org/thoughts/archives/2011/11/01/parents-survey-coppa.html.
[17] D. Boyd, E. Hargittai, J. Schultz, J. Palfrey, „Why Parents Help Their Children Lie to Facebook About Age: Unintended Consequences of the *Children's Online Privacy Protection Act*", First Monday vol. 16, 7 listopada 2011, nr 11, http://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075.
[18] „FERPA General Guidance for Parents", Departament Edukacji Stanów Zjednoczonych, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html.
[19] C. Lestch, B. Chapman, „New York Parents Furious at Program,

inBloom, That Compiles Private Student Information for Companies That Contract with It to Create Teaching Tools", „New York Daily News", 13 marca 2013, http://www.nydailynews.com/new-york/student-data-compiling-system-outrages-article-1.1287990; oraz: „Our Vision: Personal Path, Common Ground", inBloom, https://www.inbloom.org/our-vision.
[20] D.M. West, „Using Technology to Personalize Learning and Assess Students in Real-Time", Brookings Institution, 6 października 2011, http://www.brookings.edu/~/media/research/files/papers/2011/10/06%20pe
[21] L. Haimson, „NYC Parent Sounds Alarm on Student Privacy", WNYC.org, 23 lipca 2103, http://www.wnyc.org/story/307074-what-you-need-know-about-inbloom-student-database/; oraz: A. Gaber (rzecznik prasowy inBloom), korespondencja z Lauren Kirchner, 29 sierpnia 2013.
[22] „FERPA General Guidance for Parents", Departament Edukacji Stanów Zjednoczonych, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/parents.html.
[23] N. Singer, „Deciding Who Sees Students' Data", „New York Times", 5 października 2013, http://www.nytimes.com/2013/10/06/business/deciding-who-sees-studentsdata.html? pagewanted=all&r=0.
[24] B. Gross, „Teen in Jail for Months over ‚Sarcastic' Facebook Th reat", CNN.com, 3 lipca 2013, http://edition.cnn.com/2013/07/02/tech/social-media/facebook-threat-carter/index.html; oraz: J. Carter, „Release My Son Justin Carter – Being Prosecuted for a Facebook Comment", Change.org, https://www.change.org/petitions/release-my-son-justin-carter-being-prosecuted-for-a-facebook-comment.
[25] B. Griggs, „Teen Jailed for Facebook ‚Joke' Is Released", CNN.com, 12 lipca 2013, http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/index.html.
[26] P. Modi, „Statement from Justin's Lawyer", Change.org, 12 lipca 2013, https://www.change.org/petitions/release-my-son-justin-carter-being-prosecuted-for-a-facebook-comment.
[27] R. Hartley-Parkinson, „‚I'm Going to Destroy America and Dig Up Marilyn Monroe': British Pair Arrested in U.S. on Terror Charges over Twitter Jokes", „Daily Mail", 31 stycznia 2012, http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html.
[28] J. Motal, „Charges Dropped over Facebook Apple Rant", „PC Magazine", 28 czerwca 2011,

http://www.pcmag.com/article2/0,2817,2387730,00.asp.
[29] Joe Lipari w rozmowie z autorką, 23 lipca 2013.
[30] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, „Teens and Mobile Apps Privacy", Pew Research Center's Internet & American Life Project, 22 sierpnia 2013, http://pewinternet.org/Reports/2013/Teens-and-Mobile-Apps-Privacy.aspx.
[31] A. Lenhart, M. Madden, S. Cortesi, U. Gasser, A. Smith, „Where Teens Seek Online Privacy Advice", Pew Research Center's Internet & American Life Project, 15 sierpnia 2013, http://pewinternet.org/Reports/2013/Where-Teens-Seek-Privacy-Advice.aspx.
[32] D. Boyd, A. Marwick, „Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies" (praca przedstawiona podczas sympozjum „A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", organizowanym przez Oxford Internet Institute's), 22 września 2011, http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf.
[33] Ghostery, Evidon, Inc., https://itunes.apple.com/us/app/ghostery/id472789016? mt=8.
[34] „Introducing Disconnect Kids!", Disconnect, https://www.disconnect.me/kids.

ROZDZIAŁ 15: DOKTRYNA NIESPRAWIEDLIWOŚCI

[1] „The Greensboro Chronology", International Civil Rights Center & Museum, http://www.sitinmovement.org/history/greensboro-chronology.asp.
[2] „American's Sewage System and the Price of Optimism", „Time", 1 sierpnia 1969, http://content.time.com/time/magazine/article/0,9171,901182,00.html.
[3] J.H. Adler, „Fables of the Cuyahoga: Reconstructing a History of Environmental Protection", „Fordham Environmental Law Journal" 2003, nr 14, s. 89–146.
[4] „Highlights from the Clean Air Act 40th Anniversary Celebration", Agencja Ochrony Środowiska Stanów Zjednoczonych, http://www.epa.gov/air/caa/40thhighlights.html.
[5] N. Stoner, „Celebrate the 40th Anniversary of the Clean Water Act", blog: *It's Our Environment*, U.S. EPA, 18 października 2012,

http://blog.epa.gov/blog/2012/10/cwa40/.
[6] J.R. Platt, „The Endangered Species Act at 40: Forty Things Journalists Should Know", Society of Environmental Journalists, 15 lipca 2013, http://www.sej.org/publications/sejournal-su13/endangered-species-act-40.
[7] M. Scott, J. Owens, „2009 Year of the River", „Cleveland Plain Dealer", 4 stycznia 2009, http://blog.cleveland.com/metro/2009/01/04CGRIVER.pdf.
[8] M. Scott, „Freshwater Mussels Found in Cuyahoga River, Indicating Improved Water Quality", „Cleveland Plain Dealer", 22 sierpnia 2009, http://www.cleveland.com/science/index.ssf/2009/08/freshwater_musselsf
[9] Dennis Hirsch w rozmowie z autorką, 26 lipca 2011.
[10] G. Hardin, „The Tragedy of the Commons", „Science", 13 grudnia 1968, nr 3859, s. 1423–48, http://www.sciencemag.org/content/162/3859/1243.full.
[11] Dennis Hirsch w rozmowie z autorką, 26 lipca 2011.
[12] D. Brin, *The Transparent Society*, Basic Book, Nowy Jork 1999.
[13] D. Brin, B. Goertzel, „David Brin on the Path to Positive Sousveillance", h+, 23 maja 2011, http://hplusmagazine.com/2011/05/23/david-brin-on-the-path-to-positive-sousveillance/.
[14] „Cop Who Pepper-Sprayed Students at Occupy Protest Wants Worker's Compensation for ‚Psychiatric Injury'", Associated Press, 26 lipca 2013, http://talkingpointsmemo.com/news/pepper-spray-cop-occupy-protest-wants-workers-compensation-for-psychiatric-injury.php.
[15] „Our Story", Satellite Sentinel Project, http://www.satsentinel.org/our-story.
[16] „Broken Agreement: Violations in the Demilitarized Border Zone by Sudan and South Sudan", Satellite Sentinel Project, maj 2013, http://www.satsentinel.org/sites/default/files/BrokenAgreement.pdf.
[17] B. Gellman, G. Miller, „U.S. Spy Network's Successes, Failures and Objectives Detailed in ‚Black Bud get' Summary", „Washington Post", 28 sierpnia 2013, http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html.
[18] D. Leigh, „Iraq War Logs Reveal 15,000 Previously Unlisted Civilian Deaths", „Guardian", 22 października 2010,

http://www.theguardian.com/world/2010/oct/22/true-civilian-body-count-iraq.
[19] D. Leigh, „Afghanistan War Logs: Secret CIA Paramilitaries' Role in Civilian Deaths", „Guardian", 25 lipca 2010, http://www.theguardian.com/world/2010/jul/25/afghanistan-civilian-deaths-rules-engagement.
[20] P. Lewis, „Bradley Manning Given 35-Year Prison Term for Passing Files to WikiLeaks", „Guardian", 21 sierpnia 2013, http://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence.
[21] A. Luhn, L. Harding, P. Lewis, „Edward Snowden Asylum: US ‚Disappointed' by Russian Decision", „Guardian", 21 sierpnia 2013, http://www.theguardian.com/world/2013/aug/01/edward-snowden-asylum-us-disappointed.
[22] D. Barrett, „U.S. Seized Phone Records of AP Staff", „Wall Street Journal", 13 maja 2013, http://online.wsj.com/article/SB10001424127887324715704578481461374133
[23] G. Pruitt (prezes zarządu i dyrektor generalny Associated Press), „Updated: AP Responds to Latest DOJ Letter", 14 maja 2013, http://blog.ap.org/2013/05/13/ap-responds-to-intrusive-doj-seizure-of-journalists-phone-records/.
[24] S. Shane, „Prosecutors Press Subpoena for Times Reporter in Leak Case", „New York Times", 26 sierpnia 2013, http://www.nytimes.com/2013/08/27/us/prosecutors-press-subpoena-for-times-reporter-in-leak-case.html? r=0.
[25] Ch. Savage, „Court Tells Reporter to Testify in Case of Leaked C.I.A. Data", „New York Times", 19 lipca 2013, http://www.nytimes.com/2013/07/20/us/in-major-ruling-court-orders-times-reporter-to-testify.html? pagewanted=all.
[26] J. Angwin, E. Steel, „Web's Hot New Commodity: Privacy", „Wall Street Journal", 28 lutego 2011, http://online.wsj.com/article/SB10001424052748703529004576160764037920
[27] Światowe Forum Ekonomiczne, „Personal Data: The Emergence of a New Asset Class (raport), styczeń 2011, http://www3.weforum.org/docs/WEFITTCPersonalDataNewAssetReport20
[28] Emily Steel, „Financial Worth of Data Comes In at Under a Penny a Piece", „Financial Times", 12 czerwca 2013, http://www.ft.com/intl/cms/s/0/3cb056c6-d343-11e2-b3ff-

00144feab7de.html? siteedition=intl#axzz2dglKkHpd.
[29] A. Acquisti, L.K. John, G. Loewenstein, „What Is Privacy Worth?", „Journal of Legal Studies", czerwiec 2013, nr 42, s. 249–74, http://www.jstor.org/stable/10.1086/671754.
[30] Alessandro Acquisti w rozmowie z autorką, 11 marca 2011.
[31] „Health Information Privacy", Departament Zdrowia i Usług Społecznych Stanów Zjednoczonych, http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html.
[32] „Privacy Act Issues Under Gramm – Leach – Bliley", Fedearlna Korporacja Ubezpieczeń Depozytów, http://www.fdic.gov/consumers/consumer/alerts/glba.html.
[33] Tytuł XIII – ochrona prywatności dzieci w internecie, http://www.ftc.gov/ogc/coppa1.pdf.
[34] Ustawa o prywatności z 1974 roku, http://www.justice.gov/opcl/privstat.htm
[35] Tytuł XIII.
[36] „Health Information Privacy", Departament Zdrowia i Usług Społecznych Stanów Zjednoczonych.
[37] „Memo on Sorrell v. IMS Health Inc." (notatka), Center for Democracy & Technology, 22 marca 2011, https://www.cdt.org/files/pdfs/20110324_SorrellvIMS.pdf.
[38] Sprawa Sorrell kontra IMS Health Inc., sygn. 131 S. Ct. 2653, 180 L. Ed. 2d 544, 23 czerwca 2011, http://www2.bloomberglaw.com/public/desktop/document/SorrellvIMSHe 2d5442011Court.
[39] „U.S. Terrorism Agency to Tap a Vast Database of Citizens", „Wall Street Journal", 13 grudnia 2012, http://online.wsj.com/article/SB10001424127887324478304578171623040640
[40] „Privacy: Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information", Rządowe Biuro Obrachunkowe Stanów Zjednoczonych, 18 czerwca 2008, http://www.gao.gov/assets/130/120411.html.
[41] Angwin, „U.S. Terrorism Agency to Tap a Vast Database of Citizens".
[42] Sprawa Gulet Mohamed kontra Eric Holder, Robert Mueller, Timothy Healy i in., skarga w związku z Trzecią Poprawką do Konstytucji USA, Sąd Dystryktowy USA dla Wschodniego Dystryktu Wirginii, 29 sierpnia 2013; oraz: M. Mazzetti, „Detained American Says He Was Beaten in Kuwait", „New York Times", 5 stycznia 2011,

http://www.nytimes.com/2011/01/06/world/middleeast/06detain.html?r=3&hp&.
[43] Sprawa Gulet Mohamed kontra Eric Holder Jr. i Janet Napolitano, sygn. 11-1924, styczeń 2013.
[44] „DHS Traveler Redress Inquiry Program (DHS TRIP)", Departament Bezpieczeństwa Krajowego, http://www.dhs.gov/dhs-trip.
[45] Sprawa Latif i in. kontra Holder i in., nr 11-35407, D.C. nr 3:10-cv-00750-BR, opinia, http://aclu-or.org/sites/default/files/ACLUORNoFly9thCircuit.pdf.
[46] Sprawa Gulet Mohamed kontra Eric Holder, Robert Mueller, Timothy Healy i in., skarga w związku z Trzecią Poprawką do Konstytucji Stanów Zjednoczonych.
[47] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Parlament Europejski, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=CELEX:31995L0046: en: NOT.
[48] „S. 779 – Commercial Privacy Bill of Rights Acts of 2011", 112 Kongres, 12 kwietnia 2011, http://www.opencongress.org/bill/112-s799/text.
[49] „Consumer Groups Welcome Bipartisan Privacy Effort, But Warn Kerry – McCain Bill Insufficient to Protect Consumers' Online Privacy", Center for Digital Democracy, 18 kwietnia 2011, http://www.democraticmedia.org/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-protect-consum.
[50] „Senators Kerry and McCain Introduce Privacy Bill; Legislation Could Undercut Information Economy", Stowarzyszenie Marketingu Bezpośredniego, 12 kwietnia 2011, http://www.the-dma.or/cgi/disppressrelease? article=1479+++++.
[51] „S. 779 – Commercial Privacy Bill of Rights Acts of 2011, Actions & Votes", 112 Kongres, 12 kwietnia 2011, http://www.opencongress.org/bill/112-s799/actionsvotes [strona niedostępna].
[52] „We Can't Wait: Obama Administration Unveils Blueprint for a *Privacy Bill of Rights* to Protect Consumers Online" (komunikat prasowy), Biuro Sekretarza Prasowego Białego Domu, 23 lutego 2012, http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-

obama-administration-unveils-blueprint-privacy-bill-rights.
[53] Ustawa o rzetelnej sprawozdawczości kredytowej, http://www.ftc.gov/os/statutes/031224fcra.pdf.
[54] N. Singer, „Secret E-Scores Chart Consumers' Buying Power", „New York Times", 18 sierpnia 2012, http://www.nytimes.com/2012/08/19/business/electronic-scores-rank-consumers-by-potential-value.html? pagewanted=all.
[55] J. Brill, „Reclaim Your Name" (wystąpienie publiczne w trakcie 23rd Computers Freedom and Privacy Conference, Washington, D.C.), 27 czerwca 2013, http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.
[56] J. Brill, „Demanding Transparency from Data Brokers", „Washington Post", 15 sierpnia 2013, http://www.washingtonpost.com/opinions/demanding-transparency-from-data-brokers/2013/08/15/00609680-0382-11e3-9259-e2aafe5a5f84story1.html.
[57] Bardzo dobrą analizę rządowych dragnetów można znaleźć u Christophera Slobogina: Ch. Slobogin, „Government Dragnets" (praca badawcza nr 10–37), Uniwersytet Vanderbilt, Wydział Prawa Publicznego, 14 lipca 2010, http://ssrn.com/abstract=1640108.
[58] M.M. Ahlers, „TSA Removing ‚Virtual Strip Search' Body Scanners", CNN.com, 19 stycznia 2013, http://www.cnn.com/2013/01/18/travel/tsa-body-scanners/index.html.
[59] „California Bans Forced RFID Tagging of Humans", Government Technology, 17 października 2007, http://www.govtech.com/security/California-Bans-Forced-RFID-Tagging-of.html? topic=117688.
[60] Sprawa David Floyd, Lalit Clarkson, Deon Dennis, David Ourlicht kontra miasto Nowy Jork, sygn. 08 Civ. 1034 (SAS), Sąd Dystryktowy Stanów Zjednoczonych dla Południowego Dystryktu Nowego Jorku, 2013, http://www.nyclu.org/files/releases/Floyd%20opinion.pdf.
[61] Sprawa Korematsu kontra Stany Zjednoczone, sygn. 323 U.S. 214, 1944, http://supreme.justia.com/cases/federal/us/323/214/case.html.
[62] Program Rejestru Uwalniania Substancji Toksycznych (TRI), Agencja Ochrony Środowiska USA, http://www2.epa.gov/toxics-release-inventory-tri-program.
[63] Lisa Heinzerling w rozmowie z autorką, 16 marca 2013.
[64] Slobogin, *Government Dragnets*.