NOWE TECHNOLOGIE I MY. GDZIE SIĘ PODZIAŁA NASZA PRYWATNOŚĆ?

MICHAŁ SZYCHOWIAK

Politechnika Poznańska

Niewątpliwie żyjemy dziś w świecie permanentnej inwigilacji, w którym nieustannie, zachłannie i coraz bardziej inwazyjnie pozyskuje się i gromadzi nasze prywatne dane. Szacuje się, że w 2020 roku ich rozmiar sięgnie dziesiątek zettabajtów (tryliardów bajtów)[1]. Lwia część tych informacji pochodzi z naszej świadomej codziennej aktywności w sieci (wg szacunków przeciętny użytkownik Internetu poświęca mu ponad 2 godziny dziennie[2]), ale coraz większy udział w pozyskiwaniu danych mają inne nowoczesne technologie, natarczywie zdobywające kolejne segmenty rynku. Zarówno najprostsze, jak i te najwymyślniejsze gadżety elektroniczne są dziś wyposażane w mechanizmy komunikacji bezprzewodowej, umożliwiające im dostęp do naszych sieci domowych i dalej do Internetu. W ciągu ostatnich 10 lat powstała i rozpowszechniła się niezliczona wręcz ilość technologii komunikacyjnych, protokołów, funkcji i usług, stworzonych – według zapewnień twórców – by oferować nam jak największą wygodę korzystania z dobrodziejstw wirtualnego świata. A kolejne wynalazki już ustawiają się w kolejce po swój kawałek rynku. Tylko czy aby na pewno jedynym celem ich istnienia jest przemożna chęć uczynienia naszego życia łatwiejszym i wygodniejszym?

[1] N. Patrignani, D. Whitehouse, Monica Gemo, „Forget About Privacy… or Not?", IFIP AICT 526, pp. 76–85, 2018

[2] „Average Time Spent per Day with Mobile Internet" www.emarketer.com

Czy część rynku nowych technologii przypadkiem nie celuje z premedytacją w pozyskiwanie bodaj najcenniejszego dziś surowca naturalnego naszej planety – informacji?

Informacje o nas, naszych zainteresowaniach, przyzwyczajeniach, preferencjach, które mniej czy bardziej świadomie pozostawiamy po swojej aktywności m.in. w serwisach społecznościowych, na forach dyskusyjnych, przeróżnych blogach, vlogach itp., stanowią prawdziwą żyłę złota dla agencji reklamowych i marketingowych, oraz wielu innych rodzajów firm potrzebujących ich do podejmowania decyzji biznesowych. Informacje te są dostępne niemal na wyciągnięcie ręki i to na ogół kompletnie za darmo. Nic dziwnego, że wielu zainteresowanych nie potrafi oprzeć się pokusie, opracowując coraz to bardziej wyrafinowane sposoby pozyskiwania naszych prywatnych danych.

Dzieje się aktualnie w tej materii dużo, i to, niestety, dużo złego. Na tyle dużo, że coraz więcej instytucji rządowych[3] i organizacji społecznych[4] zainteresowanych bezpieczeństwem i prywatnością obywateli bije na alarm.

Za część zagrożeń prywatności odpowiadają służby i agencje rządowe[5]. Przykładowo Chiny rozpoczęły właśnie budowę krajowego systemu oceniającego swoich obywateli (*China Social Credit System*), w ramach którego na indywidualnym koncie każdego obywatela ChRL gromadzone są swoistego rodzaju punkty (przypominające w swej istocie punkty karne przyznawane w wielu krajach za wykroczenia drogowe), będące podstawą indywidualnej oceny obywatela i ewentualnych przyszłych decyzji administracyjnych w odniesieniu do jego osoby. Tej punktacji podlega dość pokaźny zbiór codziennych aktywności – od nawyków zakupowych począwszy, na aktywności społecznej skończywszy[6].

---

[3] Przykładowo w Stanach Zjednoczonych: D. Solove, W. Hartzog, „The FTC and the new common law of privacy", Columbia Law Rev. 114(3), 583–676 (2014), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement; oraz w Unii Europejskiej: Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, „Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", ETS No. 108 + Report 14437, 2017.

[4] K. Szymielewicz, K. Iwańska, „Śledzenie i profilowanie w sieci", Raport fundacji Panoptykon, 2019, https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf; patrz też: https://panoptykon.org/zapleczeinternetu.

[5] Przykładowo: https://www.tvn24.pl/system-pegasus-i-pytania-do-cba-czarno-na-bialym,964972,s.html.

[6] R. Botsman, „Big data meets Big Brother as China moves to rate its citizens", Wired, https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion, 2017.

Paradoksalnie, dużo większą skalę osiągnął jednak międzynarodowy proceder pozyskiwania danych pojawiających się w sieci przy udziale samego użytkownika, rozwinięty przez serwisy internetowe (media społecznościowe, sklepy internetowe, instytucje finansowe i kredytowe itp.) i aplikacje mobilne instalowane we wszechobecnych telefonach komórkowych[7]. Dane pozyskiwane z tych źródeł są zbierane przez wyspecjalizowane firmy z sektora prywatnego – brokerów danych (zwykle o międzynarodowym zasięgu) i wykorzystywane do profilowania konsumentów, by ostatecznie zostać odsprzedanymi dalej za jak najwyższą cenę na elektronicznych giełdach danych osobowych.

Niektóre skutecznie wylansowane wśród młodzieży (i nie tylko) gry mobilne, całkowicie darmowe – oczywiście – nie służą praktycznie niczemu innemu jak tylko śledzeniu użytkownika, czego świadomość wśród tych ostatnich jest jeszcze cały czas niedostateczna[8].

Niebezpieczeństwo potencjalnie największej skali mogą skrywać zyskujące popularność wśród konsumentów na całym świecie różnorodne elektroniczne gadżety, określane wspólnym mianem Internetu Rzeczy lub Internetu Przedmiotów (ang. *Internet of Things*, IoT[9]). To bardzo pojemna kategoria urządzeń, obejmująca m.in. domowe urządzenia sieciowe (routery dostępowe, koncentratory IoT i in.), telewizory SmartTV, kamery monitorujące, inteligentne termostaty, mierniki energii i mediów, żarówki, ekspresy do kawy, lodówki i jeszcze wiele, wiele innych przedziwnych pomysłów naszpikowania przedmiotów codziennego użytku elektroniką, skądinąd zupełnie zbyteczną do ich normalnej pracy. Bardzo reprezentatywnym tego przykładem są chociażby „inteligentne" materace do łóżek, wymagające teraz elektrycznego zasilania (a jakże!), by móc świadczyć swoje „inteligentne" usługi użytkownikowi. Użytkownikowi, no i – rzecz jasna – producentowi, który zapewne chętnie odsprzeda wszelkie pozyskane informacje dalej, np. brokerom danych, najchętniej po cichu, na ile się tylko da, bez zbytecznego kłopotania użytkownika tym faktem. I na ile akurat pozwoli mu obowiązujące prawo (szczęśliwie dla konsumentów Unia Europejska narzuca tu pewne ograniczenia wynikające z RODO[10], jednak istotną trudnością okazuje się

[7] S. Kununka, N. Mehandjiev, P. Sampaio, „A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices Versus Compliance to Privacy Policy", IFIP AICT 526, pp. 301–313, 2018.

[8] D. Harborth, S. Pape, „Privacy Concerns and Behavior of Pokémon G. Players in Germany", IFIP AICT 526, pp. 314–329, 2018.

[9] J.H. Ziegeldorf et al., „Privacy in the Internet of Things: threats and challenges", Secur. Commun. Netw. 7, pp. 2728–2742, 2014.

[10] General Data Protection Regulation 2016/679/EU, http://eugdpr.org.

fakt, iż zasady prawne określane w uchwalanych przepisach zwykle nie poddają się łatwemu przełożeniu na rozwiązania technologiczne mające szanse sprawdzić się w praktyce[11]).

Tak czy inaczej, nagminne okazują się być przeróżne formy pozyskiwania prywatnych informacji przez urządzenia IoT[12]. Obszerne analizy rynku urządzeń IoT pod względem prywatności danych można znaleźć m.in. w wielu materiałach konferencyjnych[13].

Ogromna liczba oferowanych na tym rynku produktów niesie zagrożenie nie tylko dla naszej prywatności, ale i szerzej rozumianego bezpieczeństwa[14] (w tym kontekście coraz więcej krajów zaczyna niepokoić fakt, iż zdecydowana większość komponentów rynku elektronicznego jest produkowana w Państwie Środka). Od co najmniej 2014 roku znane są przypadki przejmowania przez hakerów kontroli nad tragicznie słabo zabezpieczonymi urządzeniami domowymi (nawet rzędu 100 tys. urządzeń jednorazowo[15]) i wykorzystywania ich – całkowicie bez świadomości właścicieli – do różnego rodzaju nielegalnego procederu, np. rozsyłania pocztowego spamu. Zagrożenia nie omijają nawet tak pozornie niewinnej kategorii urządzeń jak elektroniczne zabawki[16] czy elektroniczne nianie[17].

---

[11] M. Colesky, J.-H. Hoepman, C. Hillen, „A critical analysis of privacy design strategies", IEEE Security and Privacy Workshops, pp. 33–40, 2016; patrz też: O. Drozd, „Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC29100 into the Software Development Process", Privacy and Identity, IAICT vol. 476, pp. 129–140. Springer, 2016.

[12] J. Brookman, „Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency", IAPP, 2013, https://privacyassociation.org/news/a/erodingtrust-hownew-smart-tv-lacks-privacy-by-design-and-transparency/, patrz też: Shane Harris, „Your SmartTV is Spying on You, Basically", The Daily Beast, 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spyingon-youbasically.html również: https://zaufanatrzeciastrona.pl/post/szpieg-w-twoim-pokoju-o-telewizorach-sprytniejszych-od-widzow/.

[13] Przykładowo: Alexandr Railean, Delphine Reinhardt, „Life-Long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-Cycle of IoT Devices", IFIP AICT 526, pp. 132–149, 2018; również: M. Elkhodr, et al.: „A review of mobile location privacy in the Internet of Things", 10th Int'l Conference on ICT and Knowledge Engineering, 2012.

[14] Lily Hay Newman, „Pretty Much Every Smart Home Device You Can Think of Has Been Hacked", 2014, http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_ being_secure.html.

[15] Raport BITAG (Broadband Internet Technical Advisory Group), 2016, https://www.bitag.org/report-internet-of-thing-security-privacy-recommendations.php.

[16] Przykładowo: https://sekurak.pl/barbie-z-interfejsem-wifi-shackowana-i-przerobiona-na-szpiega/; również: https://sekurak.pl/inteligentne-misie-przejete-wyciek-800-000-kont-dostep-live-do-nagran-i-zdjec-uzytkownikow/.

[17] Loulla-Mae Eleftheriou-Smith, „Baby Monitors, CCTV Cameras and Webcams from U. Homes and Businesses Hacked and Uploaded onto Russian Website", The Independent

Szczególnie poważne zagrożenia dotyczą wszczepianych urządzeń biomedycznych (ang. *Implantable Medical Devices*,IMD), takich jak stymulatory serca, neurostymulatory, pompy insulinowe, kardiowertery/defibrylatory, monitory pulsu, ciśnienia, ECG, EMG itp. Większość tego typu urządzeń stosuje bardzo słabe zabezpieczenia – wystarczy wspomnieć choćby protokoły komunikacyjne bez użycia szyfrowania czy uwierzytelnianie dostępu poprzez hasła słabej jakości[18]. Całkiem realne scenariusze ataku mogą obejmować np. przypadki śmiertelnego porażenia prądem o wysokim napięciu (ok. 830V) z defibrylatora, zmianę częstotliwości pracy stymulatora serca czy wymuszenie ciągłej transmisji radiowej z urządzenia (kto wie, może nawet poprzez masowe wysyłanie spamu, w niedalekiej przyszłości?) i tym samym znacznie przyspieszone wyładowanie baterii.

Osobną kategorię zagrożeń niesie ze sobą coraz powszechniejsze monitorowanie i śledzenie obywateli. Technologia pozwala tu na bardzo wiele[19]. Reprezentatywnym przykładem mogą być podłączone do globalnej sieci samochody profilujące kierowców, przesyłające do centrów danych producenta informacje o historii wozu, w tym prędkości podróżowania, spalaniu oraz współrzędne geograficzne (tras i miejsc parkowania)[20].

Najpowszechniej dostępnymi danymi wykorzystywanymi współcześnie do śledzenia aktywności są metadane lokalizacyjne, rejestrowane m.in. wraz ze zdjęciami robionymi aparatami fotograficznymi lub telefonami wyposażonymi w układy lokalizacyjne (np. GPS lub GLONASS). Owe metadane, domyślnie zapisywane w nagłówkach plików graficznych przechowujących takie fotografie, pośród wielu różnych informacji zawierają dokładną datę zrobienia zdjęcia, współrzędne geograficzne i markę aparatu fotograficznego. Co prawda metadane lokalizacyjne można z takich plików łatwo usunąć, jednak większość z nas tego nie czyni, prawdopodobnie nie dostrzegając takiej potrzeby lub nie będąc nawet świadomymi, że taka możliwość istnieje.

(Nov. 20, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitorscctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto russian-website-9871830.html.

[18] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01.

[19] J. Brookman, G.S. Hans, „Why Collection Matters: Surveillance as a De Facto Privacy Harm", 2013, http://www.futureofprivacy.org/wp-content/uploads/BrookmanWhy-Collection-Matters.pdf.

[20] M. Corkery, J. Silver-Greenberg, „Miss a Payment? Good Luck Moving That Car", The New York Times, Sept. 24, 2014, http://dealbook.nytimes.com/2014/09/24/miss-apayment-good-luck-moving-that-car/.

Z tego powodu w 2018 roku doszło do kilku incydentów związanych z nieświadomym ujawnianiem tajnych lokalizacji przez pracowników używających telefonów z GPS, w których to przypadkach tajne ośrodki wojskowe zostały niechcący zdekonspirowane przez pozornie niewinną analizę metadanych rejestrowanych przez aplikacje zainstalowane w telefonach personelu[21].

Oczywiście z metadanych od lat korzystają służby specjalne. Już Edward Snowden ujawnił, że amerykańska Agencja Bezpieczeństwa Narodowego (NSA) kataloguje fotografie wgrywane przez użytkowników Internetu do sieci i umożliwia ich przeszukiwanie pod kątem metadanych (np. „znajdź zdjęcia wykonane tym samym aparatem", „wykonane w tym miejscu")[22]. Do wiadomości publicznej przeciekły też informacje na temat programu RIOT, który profiluje obywateli na podstawie informacji zbieranych z ich profili w sieciach społecznościowych[23]. Choć zwykli obywatele nie mają dostępu do narzędzi NSA, to mogą skorzystać z co najmniej kilku dostępnych powszechnie usług pozwalających na śledzenie lokalizacji osób z wykorzystaniem np. metadanych publikowanych przez nich zdjęć. Jednym z takich serwisów jest PleaseRobMe.com, monitorujący portale społecznościowe w celu ustalenia prawdopodobnej aktualnej lokalizacji użytkowników i wychwytujący tych z nich, którzy w danej chwili znajdują się poza domem, sugerując przy okazji, czyje mieszkanie jest zatem najprawdopodobniej obecnie puste.

W sukurs zwykłym użytkownikom mogą przyjść dostępne w Internecie różne narzędzia ograniczające w dużym stopniu wycieki osobistych informacji. I tak przykładowo, ochrona przed śledzeniem jest wbudowana w niektóre przeglądarki internetowe (np. Mozilla Firefox) bądź możliwa do łatwego dodania przez zainstalowanie odpowiednich tzw. rozszerzeń przeglądarki (np. Lightbeam).

Godne szerszego polecenia jest też mobilne narzędzie SpyAware[24], przydatne do monitorowania wycieków danych dokonywanych przez aplikacje zainstalowane w telefonie. W istocie jest to aplikacja śledząca aplikacje śledzące. Jak widać, śledzenie może być bronią obusieczną,

[21] Przykładowo: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. również: https://www.bellingcat.com/resources/articles/2018/07/08/ strava-polar-revealing-homes-soldiers-spies/.

[22] https://niebezpiecznik.pl/post/xkeyscore-jeszcze-gorszy-niz-prism-czyli-nsa-zbiera-wszystko-co-robisz-w-sieci/.

[23] https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/.

[24] https://play.google.com/store/apps/details?id=com.ls.android.threatmonitor.

toteż warto choć od czasu do czasu spróbować użyć jej na własną korzyść.

Szczęśliwie dla nas wszystkich można już zaobserwować pewne próby podejmowania wysiłków zmierzających do ustanowienia branżowych standardów[25] odnośnie do takiej budowy produktu i wytwarzania oprogramowania, aby wykluczyć lub zminimalizować zagrożenia, na jakie narażone są współcześnie (i potencjalnie również w najbliższej przyszłości) dane przetwarzane przez te produkty. Mowa przykładowo o metodologii DPbD (ang. *Data Protection by Design and by Default*)[26] odpowiadającej oczekiwaniom zdefiniowanym m.in. w art. 35 dyrektywy RODO i określanym wspólną nazwą *Privacy Enhancing Technologies*. Aby jednakże doczekać się praktycznych wyników w tej materii, wymagana będzie niewątpliwie nie tylko dobra wola inżynierów i programistów, ale jeszcze wola polityczna i silna presja społeczna.

[25] S. Brooks et al., „An Introduction to Privacy Engineering and Risk Management in Federal Systems", National Institute of Standards and Technology Internal Report 8062, 2017 patrz też: G. Danezis et al., „Privacy and data protection by design – from policy to engineering", European Union Agency for Network and Information Security, 2014

[26] K. Rommetveit, A. Tanas, N. van Dijk, „Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering", IFIP AICT 526, pp. 25–37, 2018