Karol Kurach
Wydział Matematyki, Informatyki i Mechaniki UW

Prywatność – raj utracony?

Temat prywatności pojawia się w mediach dosyć regularnie – zazwyczaj w kontekście jej łamania. Aby nie szukać daleko, wystarczy wspomnieć ostatnie problemy firmy Sony z wyciekiem danych (w tym adresów, numerów kart kredytowych) wielu milionów klientów[1], czy też protesty mieszkańców przeciwko nagrywaniu ich domów przez samochody Google Street View[2], co uzasadnione było możliwością wykorzystania tych zdjęć przez złodziei.

W pracy postanowiłem przeanalizować temat zagrożeń prywatności we współczesnym świecie. Czy możemy jeszcze w ogóle mówić o czymś takim jak prywatność? Jeśli tak, to w jakim stopniu ona istnieje? Jak technologie najbliższych 10-15 lat mogą to zmienić?

Czy prywatność jeszcze istnieje?

Ustalmy na początek co w ogóle rozumiemy pod pojęciem prywatności. Postanowiłem na potrzeby analizy użyć definicji podawanej przez Wikipedię – jest to *„możliwość jednostki lub grupy osób do utrzymania swych danych oraz osobistych zwyczajów i zachowań nieujawnionych publicznie”*[3]. Czy przy tak postawionych wymaganiach statystyczna osoba może czuć, że posiada sferę prywatności?

Patrząc na ilość istniejących obecnie technologii, które potencjalnie mogłyby posłużyć do kontrolowania ludzi wydaje się, że już niestety nie. Wymieńmy tylko te najpopularniejsze: kamery monitoringu w miejscach publicznych (w niektórych miastach już obecnie nie ma miejsc w centrum, które nie byłyby objęte zasięgiem kamer), foto-radary na drogach, systemy kontroli dostępu do pomieszczeń (identyfikatory), możliwość lokalizacji pozycji osoby na podstawie danych z telefonów komórkowych, karty kredytowe zdradzające gdzie aktualnie jesteśmy (np. gdy właśnie dokonaliśmy opłaty w sklepie), albo gdzie planujemy być. Do tego dochodzą również liczne zagrożenia w świecie wirtualnym: zbieranie informacji o naszych preferencjach w Internecie przez wyszukiwarki, analiza naszej prywatnej korespondencji w celu wyświetlania sprofilowanych reklam, śledzenie naszej aktywności przy pomocy tzw. ciasteczek (aktualnie zabronione w Unii Europejskiej jeśli użytkownik nie wyrazi zgody[4]) i wiele innych.

Podane przykłady to oczywiście tylko część zagrożeń. Nie będziemy ich tutaj szczegółowo omawiać z trzech powodów: są to technologie już istniejące a nie „nowe”; zostały wielokrotnie opisane w pracach studenckich z lat ubiegłych[5] oraz większość z nich jest zapewne znana czytelnikowi (co najmniej ze słyszenia). Zamiast tego postaram się przewidzieć jakie nowe zagrożenia mogą powstać w ciągu najbliższych 10-15 lat.

Zagrożenia przyszłości

Większość byłych uczestników wykładu „Nowe Technologie” w swoich pracach jest zgodna, iż w dzisiejszych czasach utrzymanie prywatności jest tak trudne, że praktycznie niemożliwe. Część piszących wyrażało nadzieję, że nowe wynalazki nie ograniczą naszej prywatności w większym stopniu niż to ma miejsce obecnie. Moim zdaniem będzie wręcz przeciwnie i nawet nie trzeba się tutaj odwoływać do wizji z „Matrixa” czy też innych futurystycznych metod, które by mogły powstać w bliżej nieokreślonej przyszłości. Wystarczy spojrzeć nad czym aktualnie pracują naukowcy zatrudnieni przez wywiad albo duże koncerny informatyczne.

Przetwarzanie obrazu - rozpoznawanie twarzy

Technologią, która może bardzo wpłynąć na naszą prywatność, jest rozpoznawanie twarzy. W chwili obecnej pracuje nad nią intensywnie np. firma Google[6]. Co prawda, takie systemy już istnieją i są wykorzystywane np. przez policję, ale daleko im do doskonałości. Albo działają na mocno uproszczonych modelach twarzy (przez co traci się dokładność), albo działają zbyt wolno, żeby można było je stosować w czasie rzeczywistym (i na większej bazie danych, niż tylko zbiór osób, które popełniły kiedykolwiek przestępstwo).

Wyobraźmy sobie teraz co się stanie w momencie gdy te lepsze algorytmy powstaną i dodatkowo zwiększy się moc obliczeniowa (np. dzięki procesorom zbudowanym z wykorzystaniem grafenu). Jadąc w metrze będziemy mogli zrobić komuś zdjęcie swoim telefonem komórkowym i dowiedzieć się od razu kto to jest. Albo inaczej – osobie, która monitoruje jakiś obszar (np. lotnisko) do zapisu z kamer mogłyby się dodawać automatyczne podpisy kto jest kim. System informowałby od razu odpowiednie służby gdzie się znajduje przestępca poszukiwany listem gończym, potencjalny terrorysta albo... wróg polityczny, jeśli by wykorzystać tę technologię do złych celów.

Zauważmy również, że podczas porównywania twarzy obecne algorytmy wykorzystują jedynie zdjęcia 2D, a mogłyby cały trójwymiarowy model głowy. Pytanie skąd brać te modele – każdy człowiek musiałby pozwolić się zeskanować, żeby było co porównywać. Być może skaner 3D przyszłości będzie potrafił to wykonać w sekundę bez zgody osoby skanowanej (tak jak obecnie zwykłym aparatem możemy zrobić zdjęcie 2D). Możliwe również, że skanowanie głowy w 3D stanie się obowiązkowe dla obywateli, jak obecnie obowiązkowe są zdjęcia do dowodów osobistych albo pobieranie odcisków palców od osób starających się o wjazd do USA.

Przetwarzanie tekstu

Kolejną technologią, nad którą aktualnie prowadzone są bardzo intensywne badania to tzw. przetwarzanie tekstu naturalnego (ang. „Natural Language Processing"). Ostatecznym celem jest „zrozumienie" przez maszynę sensu przetworzonego tekstu. Przykładowo, komputer dostaje podręcznik do historii w postaci elektronicznej, uczy się z niego, a następnie na jego podstawie odpowiada na pytania. Użytkownik może zadawać pytania w języku naturalnym, np. *„Kiedy Wielka Brytania przystąpiła do II Wojny Światowej"*, a komputer musi ze zdań, które były w podręczniku: *„II WŚ zaczęła się pierwszego września 1939. Dwa dni później Wielka Brytania przyłączyła się do wojny."* wywnioskować poprawną odpowiedź czyli 3. września. Pierwsze próby takiej analizy (jeszcze kilkanaście lat temu) były bardzo prymitywne i pozwalały na znajdowanie odpowiedzi jedynie w bardzo szczegółowo zdefiniowanych warunkach – np. zadajemy tylko pytania postaci *„kiedy urodził się X"*.

Obecnie dzięki wysiłkowi m.in. inżynierów z firmy IBM powstały o wiele bardziej zaawansowane techniki do przetwarzania tekstów i uczenia maszynowego. Najnowsze dzieło IBM, czyli superkomputer Watson w teleturnieju „va banque" pokonał byłych ludzkich mistrzów[7]. Można argumentować, że ten teleturniej również wymusza definiowanie pytań i odpowiedzi w specyficznej formie, ale widać bardzo wyraźny skok jakościowy. Człowiek pyta – maszyna odpowiada. To nie szachy czy inne gry logiczne, które przekładają się na język matematyki albo które można symulować. To normalny język z jego wszelkimi zawiłościami i prawdziwa wiedza dotycząca świata.

Biorąc pod uwagę postęp w tej dziedzinie na przestrzeni ostatnich 10 lat można wnioskować, że Watson III, który powstanie za 15 lat będzie potrafił odpowiadać na bardzo skomplikowane pytania. Pomijając oczywiste zalety płynące z posiadania takiej maszyny, zastanówmy się co by było w przypadku jeśli by go naładować nie informacjami historycznymi, ale aktualnymi danymi o świecie? Może np. analizując dane banków, telefonów, itp. będzie potrafił szybko odpowiadać na pytania *„Który z podatników zarobił więcej niż zadeklarował?"* albo *„Podaj nazwiska ludzi, którzy pisali o naszej partii źle w Internecie?"*. To już się robi trochę niepokojące, a zwłaszcza biorąc pod uwagę, że prawdopodobnie już wkrótce większość systemów operacyjnych będzie działać w tzw. „chmurze" i nasze prywatne dokumenty, zamiast na lokalnych dyskach, będą znajdowały się w miejscach, do których taki Watson może mieć łatwy dostęp.

„Don't be evil”

Moim zdaniem, nie jesteśmy w stanie zatrzymać rozwoju technologii zagrażającej naszej prywatności. Nie pozwolą na to koncerny, w których interesie jest wiedzieć o nas coraz więcej, jak również służby wywiadu, dla których jest to duże ułatwienie pracy i sposób na zwiększenie skuteczności. Powyżej opisane przykłady to jedynie kilka wybranych technologii, nad którymi aktualnie pracują naukowcy. Pominięte zostały chociażby takie potencjalne zagrożenia przyszłości jak np. rozpoznawanie dźwięku czy wzrost mocy obliczeniowej Echelonu – systemu do podsłuchu i analizy rozmów w kanałach telekomunikacyjnych[8].

Pytaniem otwartym pozostaje, czy wymienione technologie rzeczywiście zostaną kiedyś wykorzystane przeciwko społeczeństwu, czy pozostaną jedynie zagrożeniem teoretycznym, w praktyce dającym o wiele więcej dobrego niż złego. Zostaje nam jedynie czekać i wierzyć, że jednak większość firm przyjmie założenia podobne do Googlowego „Don't be evil”[9]. Choć jak niestety wiemy, nawet autorom tego motta nie zawsze udawało się go przestrzegać...[10]

Bibliografia:

[1] http://www.zyciewarszawy.pl/artykul/594409.html
[2] http://www.telegraph.co.uk/technology/google/5095241/Google-Street-View-Residents-block-street-to-prevent-filming-over-crime-fears.html
[3] http://pl.wikipedia.org/wiki/Prywatno%C5%9B%C4%87
[4] http://thenextweb.com/eu/2011/03/09/new-eu-cookie-law-threatens-to-annoy-users-and-send-startups-packing/
[5] http://www.fuw.edu.pl/~szczytko/NT/sprawozdania2008.html
[6] http://www.webpronews.com/google-face-recognition-app-in-development-2011-03
[7] http://di.com.pl/news/36056,0,Komputer_od_IBM_pokonuje_czlowieka_w_Va_Banque_wideo.html
[8] http://en.wikipedia.org/wiki/Echelon_(signals_intelligence)
[9] http://en.wikipedia.org/wiki/Don't_be_evil
[10] http://www.theregister.co.uk/2010/04/22/google_streetview_logs_wlans/