Prywatność w internecie

Aby odpowiedzieć na pytanie, czy istnieje prywatność w sieci, należy cofnąć się do początków internetu i zastanowić się, przez kogo oraz w jakim celu została stworzona globalna sieć.
Pierwowzór Internetu, czyli ARPANET powstał w 1969 roku. Były to czasy zimnej wojny oraz tzw. wyścigu zbrojeń, a ARPANET był używany do celów militarnych.
Jednak w połowie lat 70 XX wieku, NSA (Amerykańska Agencja Bezpieczeństwa), została jednym ze sponsorów prężnie rozwijającego się odpowiednika dzisiejszego Internetu.
Już w 1977 roku, NSA było jednym z węzłów w dosyć rozległej sieci na terenie USA. Oznacza to, że mogła przechwytywać i podglądać ruch sieciowy innych komputerów. Prawdopodobnie wtedy powstała idea możliwości szpiegowania użytkowników tej sieci.

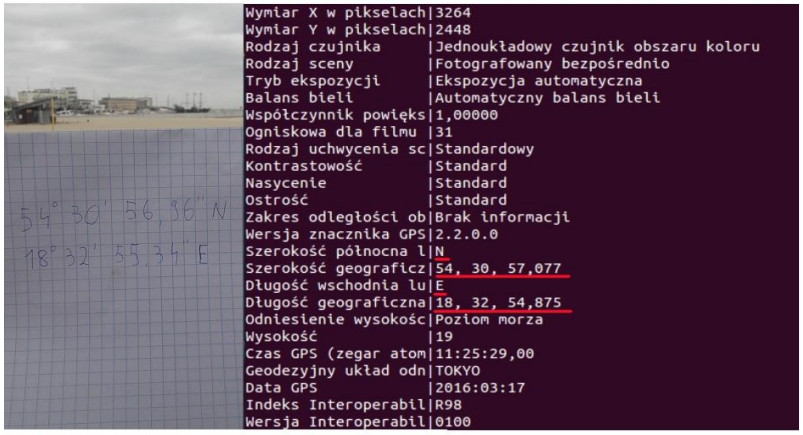
W 2013 roku nastąpił przełom i ludzie na nowo poznali cały internet, jego pochodzenie oraz do jakich celów został tak naprawdę stworzony. Dzięki Edwardowi Snowdenowi, byłemu pracownikowi CIA oraz NSA, społeczeństwo dowiedziało się między innymi o takich tajnych programach do szpiegowania jak XKEYSCORE[], TEMPORA, lub PRISM. Ogólnie, Internet ma za zadanie gromadzenie danych o użytkownikach przy pomocy takich firm jak: Microsoft, Google, Facebook, Yahoo!, Youtube, Skype, Apple oraz Dropbox.
Głównym celem agencji wywiadowczych NSA oraz GCHQ (w Wielkiej Brytanii) były informacje odnośnie wysyłanych e-maili, rozmów wideo, głosowych bądź tekstowych, loginów, haseł, udostępnionych plików oraz ogólnej charakterystyki użytkownika na podstawie serwisów społecznościowych. Następnie takie dane przekazywane są trzecim firmom lub agencje wywiadowcze korzystają z nich na własny użytek, jak to określają „w celach bezpieczeństwa narodowego”.
Oprócz instytucji rządowych, również wyżej wymienione firmy katalogują dane o użytkownikach. Najczęściej wykorzystują te dane, aby wychwycić słowa kluczowe, a później powiadomić policję o nielegalnych działaniach.

Należy sobie uświadomić przykrą prawdę: **w internecie nie ma prywatności.** Cała nasza aktywność jest rejestrowana i analizowana. Surfując, pozostawia się po sobie tyle cyfrowych "odcisków palców", że zgromadzenie tych informacji wystarczy do stworzenia naszego bardzo dokładnego profilu; osobowościach, znajomościach, przyzwyczajeniach, itd., itp.
Internet z jednej strony dał szeroką platformę komunikowania się ze światem, z drugiej jest również dzięki naszemu cynizmowi - pułapką infiltracji i utraty prywatności. Co gorsza, producenci nowych produktów IT (routery i systemy operacyjne) zostawiają otwarte "furtki", które ułatwiają penetrowanie naszych komputerów?

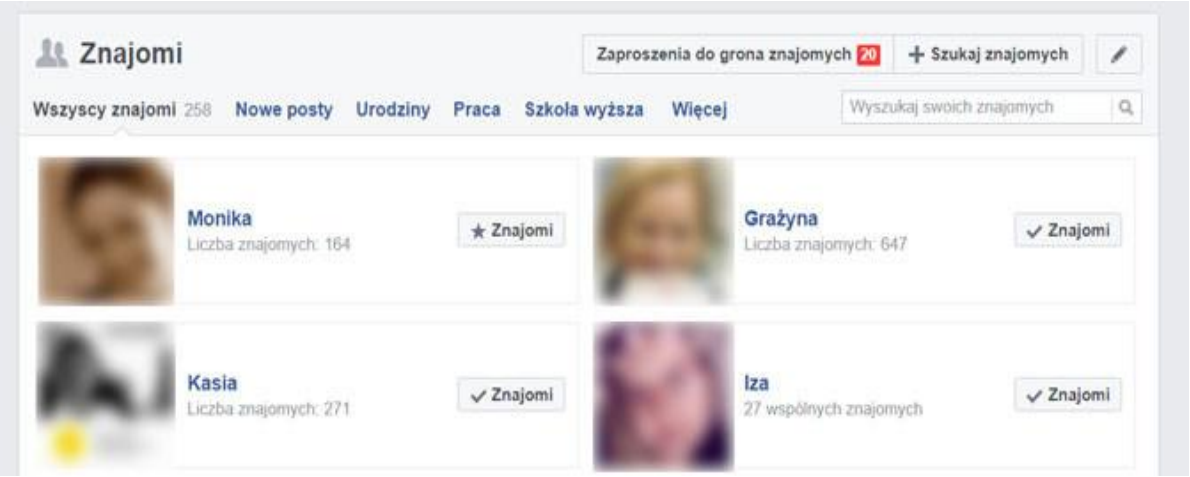
Huawej, Facebook, Google i inni.
Dziś możemy tylko wybrać, kto będzie nas lepiej szpiegować.

Używając Gmail, pozwalamy koncernowi czytać wszystkie wiadomości. Firma zapewnia wprawdzie ,ale sprawdzić tego nie można.

Nieważne, czy otwieramy wyszukiwanie Google, używamy okienka wyszukiwania czy też wpisujemy zadania bezpośrednio w pasku adresu, jeśli Google jest domyślną wyszukiwarką, to każde otwarcie strony internetowej jest protokołowane - nawet przy aktywnym trybie incognito.
Wszystkie dane, które zapisujemy w pamięci „Dysku Google", firma łączy z naszym profilem. Dlatego, choć zapisywanie wszystkich haseł i danych dostępowych jest bardzo praktyczne, to właściwie nie jest to dobry pomysł, bo Google ma do nich dostęp.
Czy pamiętamy jeszcze, z kim spotkaliśmy się 17 marca 2012 roku? Albo, kiedy po raz ostatni byliśmy u stomatologa? Google to wie, o ile korzystamy z Kalendarza Google do zarządzania naszymi terminami. Wtedy Google na stałe zapisuje terminy w naszym profilu.
Jeśli mamy androidowy telefon, to bez konta Google jego sensowne używanie jest praktycznie wykluczone. Daleko bezsensowne jest posługiwanie się fikcyjnym nazwiskiem, bo w sklepie musimy podać ważne dane osobowe.
Za każdym razem, kiedy włączamy telefon z Androidem albo na smartfon-ie otwieramy usługę Google, firma zapisuje naszą lokalizację i dodaje ją do naszego profilu lokalizacyjnego. W ten sposób Google wie na przykład, gdzie pracujemy albo, kiedy jesteśmy na urlopie.
Serwis Google „Zdjęcia" jest praktyczny, ale wysyłane do niego zdjęcia zna również firma Google nawet, jeśli są to fotografie prywatne, intymne czy wręcz pikantne. W ten sposób Google wie na przykład, kiedy, do których krajów podróżowaliśmy, kogo znamy i z kim często przebywamy.
Jeżeli do kontrolowania stanu naszego zdrowia używamy Google „Fit", Google wie, jak jesteśmy wysportowani, a nawet więcej; w naszym profilu firma zapisuje również wszystkie treningi i może dokładnie prześledzić, gdzie i kiedy biegaliśmy i jak często uprawiamy sport.
Google zapamiętuje każdy film, jaki oglądamy, i każde zapytanie wpisywane przez nas do YT. W ten sposób koncern może również dokładnie sprawdzić, jaką muzykę lubimy, co nas bawi i jakie produkty nas interesują.
Przycisk **Lubię to!** jest kluczowym narzędziem Facebooka. Okazji użycia słynnego like'a wszędzie jest mnóstwo: na stronach internetowych, firmowych profilach, przy zdjęciach, przy każdym pojedynczym wpisie i komentarzu i naturalnie w samym Facebooku. Przy każdym kliknięciu na „Lubię to" zdradzamy trochę więcej informacji o naszych upodobaniach
i antypatiach.
Rubryka z imprezami jest nie tylko narzędziem do planowania rozrywki. To zdradza Facebookowi, jakimi imprezami się interesujemy, w jakich imprezach uczestniczymy i jakie ignorujemy.
Każde kliknięcie na treści reklamowe w Facebooku jest skrupulatnie protokołowane. Łącząc te informacje z like'ami albo przynależnością do grup, Facebook ustala również, na co prawdopodobnie wydalibyśmy pieniądze.
Jeśli na naszym smartfon-ie zainstalowaliśmy Facebooka, to firma prawdopodobnie bardzo dokładnie wie, gdzie jesteśmy, bo aplikacja w ustawieniach standardowych może korzystać
z funkcji lokalizacyjnych. Jeżeli sami informujemy o naszej lokalizacji, to jest to dla Facebooka wskazówka, które miejsca są dla nas ważne albo, które miejsca lubimy. Bo przecież, z jakiego innego powodu publikowalibyśmy je w sieci?



Wysłane zdjęcie może zdradzić dokładne miejsce, w którym zostało zrobione. Opiera się to na dodawaniu meta danych Exif do pliku. Żeby to udowodnić, poniżej zamieszczone zdjęcie zawiera zapisane współrzędne GPS ze smartfon-a, następnie przy pomocy programu „Exif" wyodrębniono pozostałe informacje.
Jeśli korzystamy z facebookowego czata, zdradzamy portalowi, z kim utrzymujemy intensywne kontakty i czego one dotyczą. Archiwum danych udowadnia, że Facebook zapisuje nie tylko dane dotyczące naszej komunikacji, ale także jej treść.
Funkcja pisania postów i komentowania świetnie nadaje się do prowadzenia dyskusji. Jeśli jej używamy, Facebook dowiaduje się, w jakie tematy się angażujemy i może w ten sposób ustalić nasze poglądy, ale również wysnuć wnioski na temat naszych przekonań politycznych.
Funkcja łączenia w sieci jest potężną maszyną do gromadzenia danych. Nasi znajomi i ich znajomi bardzo wiele mówią o nas samych, bo Facebook wychodzi z założenia, że to nasi znajomi mają podobne zainteresowania.



Każdy, kto choć trochę interesuje się tematem prywatności w sieci wie, jak bardzo ryzykowne jest korzystanie z publicznych WI-FI, w parkach, pociągach czy kawiarniach.

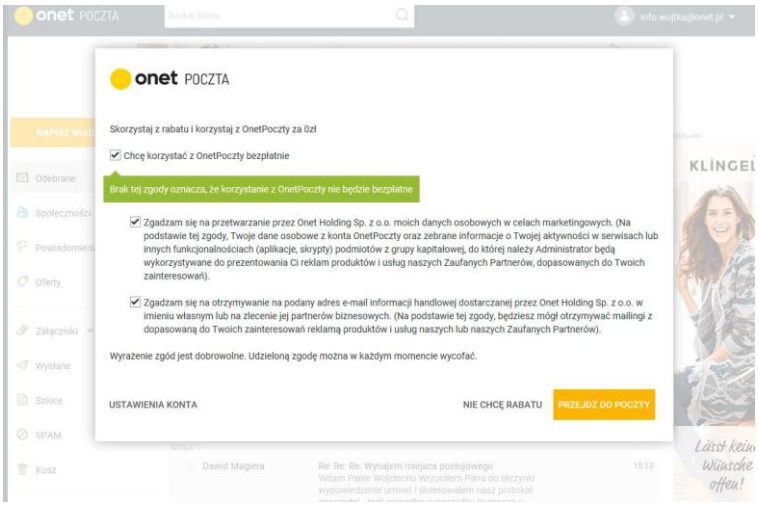
Gdyby w czasach analogowych ktoś chciał zdobyć takie informacje, jakie dostarcza internet przez zaledwie dobę, musiałby wynająć bardzo drogiego detektywa, który śledziłby użytkownika przez kilka tygodni, kilkanaście godzin dziennie.

Prócz globalnej kontroli, marketingu i manipulowania, istnieje jeszcze jeden cel masowego zbierania danych o ludziach. Jest nim budowa robota, który zastąpi człowieka. Stworzone profile służą do doskonalenia tzw. sztucznej inteligencji. Już dziś istnieją prototypy takiej maszyny wyglądem przypominającej człowieka. Są jeszcze problemy natury technicznej, ale ich rozwiązanie jest kwestią czasu. Materiału do realizacji tych celów dostarczamy sami.

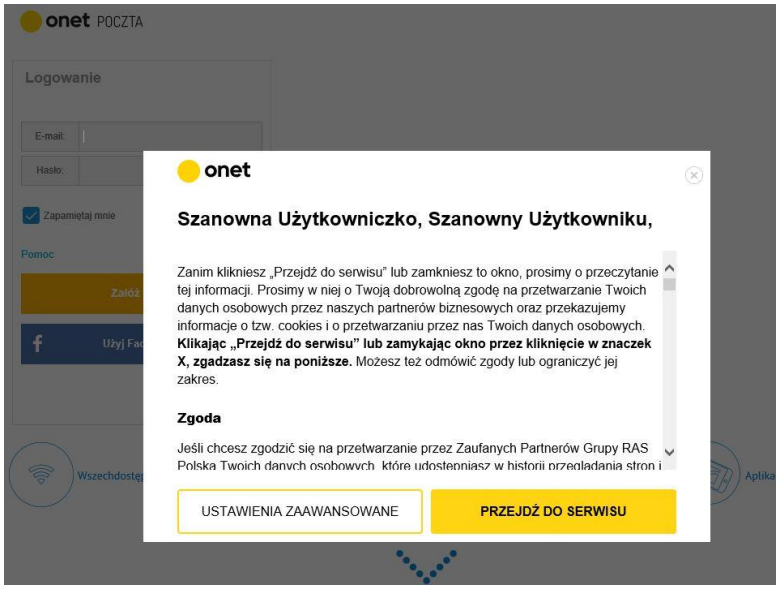
Metody ochrony.

Jestem przekonany, że można i nawet należy utrudnić szpiegowanie poprzez anonimową aktywność w internecie. Jest to metoda dostępna i łatwa dla każdego użytkownika.
Ludzie, którzy uważają, że nie mają nic do ukrycia, powinni się zapoznać z cytatem Edwarda Snowdena, mianowicie: „**Twierdzenie, że nie dbasz o swoją prywatność, ponieważ nie masz nic do ukrycia, nie różni się niczym od twierdzenia, że nie dbasz o wolność słowa, ponieważ nie masz nic do powiedzenia**”.
Zachowanie prywatności jest możliwe, pod warunkiem, że poza czujnością oraz zdrowym rozsądkiem, zostaną wykorzystane odpowiednie narzędzia, które pozwolą na jej zachowanie.
Żaden program nie zastąpi rozsądnego myślenia użytkownika. Nie dzielimy się z nieznajomymi osobami na mieście poufnymi informacjami, więc w internecie również nie powinniśmy tego robić.
Kolejną rzeczą do przemyślenia są nowe technologie oraz to, w jakim stopniu są one wykorzystywane do śledzenia użytkowników. Nikt nie kryje się z tym, że urządzenia takie jak SmartTv czy konsole, nagrywają i przekazują rozmowy w pokoju. W Chinach nawet do żelazka lub czajnika dołączany jest mikroczip, który rozsyła szpiegowskie oprogramowanie.

Lokalni szpiedzy wysyłają nam podstępne okienka, mające na celu zgodę na przekazywanie danych do firm marketingowych. Np. firma Onet parę miesięcy temu podstawiała użytkownikowi takie okienko:



Bez zaznaczenia obu kwadracików użytkownik nie mógł korzystać ze swojej poczty. Był to oczywiście szantaż Na skutek interwencji użytkowników to okienko zastąpiono innym:



Po kliknięciu myszą na pole „przejdź do serwisu”, komputer klienta jest po prostu penetrowany i plądrowany w poszukiwaniu pożądanych informacji. Można tego uniknąć zamykając okno. Podobnie okienka towarzyszą niektórym portalom w internecie. Jeżeli nie ma możliwości ich zamknięcia, pozostaje jedynie zrezygnowanie z ich czytania. W innym przypadku należy podać swoje dane osobowe. Można oczywiście podawać fałszywe.

Uważać trzeba na portale internetowe służące do „ściągania” oprogramowania z internetu, np.: „Dobre programy”, lub „Instalki”. Z reguły „dodatkowo” instaluje się również oprogramowanie szpiegowskie, albo wirusy. Ponadto są specjalnie tak prezentowane, że przez pomyłkę można sobie zainstalować takie złośliwe aplikacje.
Informacje zawarte w Cockie (przysłowiowe ciasteczka), zbiorach tymczasowych oraz hasłach, znajdujących się w opcjach internetowych systemów operacyjnych, są dla nas wygodne, z drugiej strony stanowią przysłowiową skarbnicę wiadomości dla osób "trzecich". Najlepszym sposobem jest zaznaczanie usuwania tych opcji.

Na rynku istnieje kolejny portal spłecznościowy – Minds - ale tym razem nastawiony na prywatność i bezpieczeństwo użytkowników.

Dostępna jest też bezpieczna skrzynka mail-owa – ProtonMail, dzięki której mail-e użytkowników nie są do wglądu przez różne służby. Oferuje silne szyfrowanie, nie trzyma logów oraz nie trzeba podawać żadnych danych osobowych. Jest całkowicie darmowa. Jest wersja też na telefony komórkowe.

Jedną z bezpiecznych przeglądarek jest TorBrowser. Została tak skonfigurowana, aby gwarantować anonimowość.
Bezpiecznym wariantem przeglądarki Chrome jest „SRWare Iron”. Zachowuje ona funkcjonalność Google, działa też podobnie, ale jej odmienność polega na tym, że nie przekazuje żadnych informacji do innych. Istnieje wersja na telefony komórkowe.
Innym przykładem jest przeglądarka „DuckDuckGo”, która po pierwsze - nie zbiera żadnych informacji o użytkowniku i po drugie - nie tworzy na ich podstawie żadnego profilu, pozwalającego na filtrowanie wyników. Działa podobnie jak Internet Explorer.
Innym narzędziem zapobiegającym szpiegowanie jest VPN. Jest do zastosowania na komputerze, tablecie, czy smartfon-ie. Połączenie Internetowe jest chronione protokołem SSL oraz 256-bitowym szyfrowaniem. Instalowanie i konfiguracja VPN wymaga jednak pomocy informatyka.
Osobiście na komputerze z systemem Windows 8 prof. używam dwóch przeglądarek w zależnościom potrzeb; albo „DuckDuckGo”, albo „SWare Iron”.
W przypadku sieci nie mam wyboru i na razie muszę używać Chrome, ale w routerze Fritz usunąłem adres IP i na serwerach skonfigurowałem usługę DHCP. To spowodowało, że ewentualni intruzi otrzymują fałszywy adres sieciowy. To mnie z zupełności zadowala i czuję się w miarę dobrze zabezpieczony.

Bezpieczeństwo w „chmurze”.

Technologia „chmury” to kolejny przykład na koncepcję, która z jednej strony przyniosła ogromną wygodę, a z drugiej - wielkie zagrożenie. Wysyłając swoje pliki na zewnętrzny serwer, nie dostaje się gwarancji, że nie mają do nich dostępu „trzecie instancje”. Dlatego rozsądnym rozwiązaniem jest szyfrowanie danych przed synchronizacją.
W tym temacie do dyspozycji jest trochę aplikacji, m.in. DiskCryptor, TrueCrypt czy Gpg4Win. Istnieją również kompletne programy do synchronizacji z „chmurami”, które posiadają wbudowany moduł szyfrowania. Są nimi, np.: CloudGogger, DrobBox czy OnDrive.
Ciekawe możliwości oferuje SpiderOak. Jest to aplikacja zintegrowana z firmowym dyskiem w „chmurze”, oferująca wysoki poziom ochrony przesyłanych plików.

Jeden z grona moich znajomych zameldował mi brak danych w „chmurze”. Po przeprowadzeniu „dochodzenia” okazało się, że po prostu jego baza danych z ostatnich 4 lat, dotycząca porad finansowych po prostu „rozpłynęła się w „chmurze”. To nie jest jedyny przykład.

Jest to powód, dla którego nie proponujemy rozwiązań w "chmurze". Dane mogą się "ulotnić", stać się łupem hakerów, konkurencji lub nieuczciwych ludzi. Ich przywrócenie do poprawnego stanu jest często sprawą bardzo kosztowną i czasochłonną, czasami wręcz niemożliwą.
Jeżeli są problemy "w chmurze", mamy inne rozwiązania, które dają lepszą gwarancję, że dane pozostaną dalej jedynie własnością firmy.
Według fachowców dane "w chmurze" atakowane są codziennie ponad 650 razy. Ta liczba powinna dawać już wyobrażenie o zagrożeniu.