

Polityka prywatności, ciasteczka i śledzące strony

18 listopada 2014

Czy zastanawialiście się kiedyś, na czym zarabiają firmy oferujące w sieci „darmowe” usługi, takie jak poczta elektroniczna? Poruszając się po Internecie, wszędzie zostawiacie cyfrowe ślady – to one są walutą, którą opłacacie darmowe usługi. Wyjaśniamy, co na temat swoich użytkowników wiedzą odwiedzane strony internetowe i co się z tą wiedzą dzieje.

CO WIE STRONA, CZYLI DLACZEGO WARTO CZYTAĆ POLITYKI PRYWATNOŚCI

Gdy wchodzicie na stronę internetową, automatycznie przesyłacie jej swój adres IP oraz informacje o przeglądarce – są to dane, dzięki którym można was zidentyfikować.

Dopuszczalny zakres zbieranych przez polskich usługodawców informacji wynika z ustawy o świadczeniu usług drogą elektroniczną. Wyróżnia ona trzy kategorie danych: informacje niezbędne do świadczenia usługi (na przykład w przypadku sklepu on-line może to być nie tylko imię i nazwisko, ale także numer karty kredytowej), dane podane dobrowolnie przez użytkowników i tzw. dane eksploatacyjne, wśród których są m.in. informacje o tym, kiedy weszliśmy na stronę, jak długo na niej przebywaliśmy i to, z jakiego systemu operacyjnego korzystaliśmy.

Mimo że na podstawie danych eksploatacyjnych można ustalić osobę korzystającą z usługi, to właśnie te dane są najsłabiej chronione – po anonimizacji mogą być one wykorzystywane do celów reklamy czy badania rynku. Ale i tak polskie firmy – ograniczone obowiązującymi w Polsce przepisami – mają znacznie mniejsze możliwości wykorzystywania naszych danych, niż te mające siedzibę w USA. Do takiego wniosku prowadzi lektura

tzw. polityk prywatności publikowanych przez te firmy.

W polityce prywatności można znaleźć informacje:

- jakie dane o użytkownikach zbiera strona,
- w jaki sposób dane będą wykorzystywane,
- komu dane będą udostępniane,
- kim jest podmiot, który dysponuje danymi – jaka jest jego nazwa, status prawny i adres.

Lektura polityki prywatności, poza zwiększeniem wiedzy o skali pozostawianych przez nas internetowych „śladów”, ma szczególne znaczenie w przypadku korzystania z serwisów społecznościowych: to w niej znajdują się chociażby informacje o tym, kto może oglądać publikowane przez nas zdjęcia i inne treści. Warto się z tą polityką zapoznawać regularnie, bo niestety np. Facebook co jakiś czas zaskakuje swoich użytkowników kolejnymi zmianami ustawień prywatności.

Co ważne, choć nie mamy wpływu na treść polityk prywatności, część usługodawców daje pozwala użytkownikom samodzielnie skonfigurować ustawienia prywatności. Warto zwrócić na to uwagę, bo domyślne ustawienia zwykle najslabiej chronią prywatność. Sami musimy zadbać o zgłoszenie sprzeciwu wobec przetwarzania części danych czy włączenie określonych ustawień. Czasem zdarza się, że jeśli nie skorzystamy z możliwości wzmocnienia prywatności w określonym terminie, później taka opcja będzie już niedostępna.

Dane zostawiane przez nas na stronach internetowych są bardzo atrakcyjne dla wielu podmiotów komercyjnych, dlatego do ich zbierania wykorzystywane są różne narzędzia. Najpopularniejsze to tzw. ciasteczka (cookies), czyli niewielkie pliki tekstowe wysyłane przez strony i zapisywane na twardym dysku użytkownika. Niektóre ciasteczka (np. służące do zapisywania haseł czy danych formularzy, które wypełniał użytkownik), są

bardzo pomocne, a wręcz konieczne do normalnego funkcjonowania stron. Ale na tym ich możliwości się nie kończą – część ciasteczek służy śledzeniu aktywności użytkowników Internetu. Co więcej, na komputerze są zapisywane nie tylko ciasteczka odwiedzanej strony, ale również ciasteczka pochodzące od firm zewnętrznych (tzw. third party cookies), do których stron odwołuje się odwiedzana strona.

To, komu przekazywane są dane o naszej obecności na konkretnej stronie, zazwyczaj nie jest widoczne na pierwszy rzut oka. Dość łatwo można to sprawdzić na przykład za pomocą [specjalnej wtyczki](#) do przeglądarki Mozilla Firefox. Wystarczy jeden dzień zwykłego surfowania po internecie, by zorientować się, jak wiele podmiotów (nawet takich, o których istnieniu nie mieliśmy bladego pojęcia) zbiera informacje na nasz temat z wielu różnych źródeł.

Jeśli na jakiegokolwiek odwiedzanej przez nas stronie znajdują się wtyczki Facebooka czy innych serwisów społecznościowych (w ten sposób dodaje się np. komentarze albo pokazuje fanów), dane trafiają również tam. Wystarczy być zalogowanym na swoje konto (albo nawet zalogować się na nie później, nie usuwając wcześniej ciasteczek), by zostać zidentyfikowanym jako konkretna osoba. Oznacza to, że administratorzy serwisów społecznościowych, mogą bez większej trudności śledzić aktywność swoich użytkowników w sieci.

Obowiązujące od marca tego roku przepisy Prawa telekomunikacyjnego przewidują, że instalacja plików cookie (z wyłączeniem tych niezbędnych do funkcjonowania strony) możliwa jest pod warunkiem wcześniejszego poinformowania nas o ciasteczkach i uzyskaniu naszej wyraźnej zgody na ich zapisanie. To dlatego od jakiegoś czasu możemy zauważyć pojawiające się na większości stron informacje o wykorzystywaniu ciasteczek. Warto ograniczyć możliwość pozyskiwania informacji na nasz temat przy pomocy ciasteczek, modyfikując odpowiednio ustawienia przeglądarki (w czym pomocna będzie [„Instrukcja świadomego ciasteczkowicza”](#)) lub

instalując odpowiednie wtyczki (np. Cookie Monster).

CO STRONA MOŻE ZROBIĆ ZE SWOJĄ WIEDZĄ? DRUGIE ŻYCIE DANYCH

Czasami dane zbierane przez strony są wykorzystywane tylko do poprawienia jakości usługi: Fundacja Panoptikon wykorzystuje informacje o ruchu na stronie, żeby wygenerować statystyki, które ułatwiają sprawne administrowanie stroną i zapewnienia mu wysokiej jakości merytorycznej – będziemy wiedzieli, ile osób otworzyło ten tekst i ile spędziło czasu, czytając go, co pozwoli ocenić, czy tekst Was zainteresował...

Natomiast lektura wielu polityk prywatności prowadzi do wniosku, że z danymi internautów może się dziać niemal wszystko! Na przykład Google wykorzystuje dane, by „zaoferować dostosowane treści – np. w postaci trafniejszych wyników wyszukiwania oraz reklam”. I co najważniejsze, nasze dane są często przekazywane podmiotom trzecim współpracującym ze stroną internetową, na którą zajrzeliśmy – szczegółową (bardzo długą!) [listę takich podmiotów](#) publikuje w swojej polityce prywatności m.in. firma Paypal.

Można więc powiedzieć, że często dotyczące nas informacje zyskują drugie życie – są przedmiotem handlu, wędrują między hurtowniami danych i służą do profilowania. Dzięki nim firmy marketingowe określają, które produkty warto reklamować konkretnemu konsumentowi, a reklamodawcy mogą przesyłać konsumentom spersonalizowane oferty.

Zbieranie danych w celu tworzenia profili osobowych wzbudza poważne wątpliwości i generuje nowe zagrożenia dla naszej prywatności. Szczególnie dotyczy to przypadków, w których profilowanie jest wykorzystywane przy podejmowaniu istotnych decyzji, np. o przyznaniu kredytu. Ponieważ profilowanie opiera się na korelacjach statystycznych, z definicji jest ono obarczone marginesem błędu. A więc nierozzerwalnie wiąże się z ryzykiem dyskryminacji i wykluczenia. Warto zatem poświęcić trochę czasu, żeby zadbać o swoją prywatność w sieci i

ograniczyć ilość pozostawianych cyfrowych śladów.

Autorzy: Wojciech Klicki, Katarzyna Szymielewicz, Anna
Wąlkowiak

Źródło: [Fundacja Panoptikon](#)