Rezolucja

w sprawie śledzenia w sieci i ochrony prywatności

35th INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS
PRIVACY: A COMPASS IN TURBULENT WORLD
Warsaw, 23-26 September 2013

Śledzenie w sieci (ang. web tracking) pozwala dostawcom usług monitorować każdy aspekt zachowania użytkownika w sieci. Rodzaj informacji, które mogą być gromadzone poprzez śledzenie (np. adresy IP, identyfikatory urządzenia, etc.), może prowadzić do identyfikacji określonej osoby, której dane dotyczą. Taka możliwość stwarza potencjał dla organizacji w zakresie tworzenia obszernego profilu na temat działań online możliwej do zidentyfikowania osoby, której dane dotyczą, przez długi czas.

Dane na temat działań użytkownika, gromadzone z komputera lub innego urządzenia (np. smartfona) podczas korzystania z różnych usług społeczeństwa informacyjnego w Internecie, są coraz częściej łączone, zestawiane i analizowane przez różne podmioty w różnych celach, począwszy od celów charytatywnych aż po cele komercyjne różnych podmiotów oferujących takie usługi lub ich części. Generowane profile zainteresowań (czy też „profile użytkowników") mogą być wzbogacone o dane ze „świata offline" dotyczące niemal każdego aspektu życia prywatnego, w tym informacje finansowe, jak również informacje dotyczące np. zainteresowań, problemów zdrowotnych, poglądów politycznych i/lub przekonań religijnych.

Zauważamy, że śledzenie oferuje określone korzyści konsumentom, takie jak zarządzanie siecią, bezpieczeństwo i zapobieganie oszustwom, oraz może ułatwić rozwój nowych produktów i usług. Niemniej śledzenie stwarza poważne zagrożenia dla ochrony prywatności obywateli w społeczeństwie informacyjnym, grożąc erozją kluczowych zasad przejrzystości, ograniczenia celu i możliwości kontroli przez osobę fizyczną.

W rezultacie wszyscy interesariusze, w tym rządy, organizacje międzynarodowe oraz dostawcy usług informacyjnych powinni traktować ochronę prywatności priorytetowo przy projektowaniu, zapewnianiu i wykorzystywaniu usług społeczeństwa informacyjnego.

W związku z powyższym Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności wzywa wszystkich interesariuszy, gdy to istotne i właściwe, do:

- przestrzegania zasady ograniczenia celu;
- zapewniania informacji i kontroli nad wykorzystywaniem elementów śledzenia, w tym sygnaturę urządzenia i przeglądarki (ang. device and browser fingerprinting);

- powstrzymania się od wykorzystywania niewidzialnych elementów śledzenia do celów innych niż bezpieczeństwo/wykrywanie oszustw lub zarządzanie siecią,
- powstrzymania się od wywodzenia zestawu poszczególnych elementów informacji (odcisków palców) w celu unikalnej identyfikacji i śledzenia użytkowników w celach innych niż bezpieczeństwo/ wykrywanie oszustw;
- zapewnienia odpowiedniej przejrzystości w zakresie wszystkich rodzajów praktyk śledzenia w sieci, aby umożliwić konsumentom świadome wybory;
- oferowania łatwych w użyciu narzędzi, które pozwolą użytkownikom na odpowiednią kontrolę nad gromadzeniem i wykorzystywaniem ich danych osobowych;
- unikania śledzenia dzieci oraz śledzenia na stornach skierowanych do dzieci przy braku możliwej do weryfikacji zgody rodzicielskiej;
- przestrzegania zasady uwzględniania ochrony prywatności w fazie projektowania (privacy-by-design) oraz przeprowadzania oceny wpływu na prywatność na początku nowych projektów;
- wykorzystywania technik, które zmniejszają wpływ na ochronę prywatności, takich jak anonimizacja / pseudonimizacja
- propagowania standardów technicznych na rzecz zapewnienia lepszej kontroli użytkownikowi (np. skuteczny standard „Do-Not-Track" – „Nie śledź").