30. Międzynarodowa Konferencja Rzeczników Ochrony Danych
Strasburg, 17 października 2008

Projekt rezolucji w sprawie ochrony danych w serwisach społecznościowych

Projektodawca: Rzecznik Ochrony Danych Landu Berlin, Niemcy

Współautorzy:
Narodowa Komisja Informatyki i Wolności (CNIL), Francja;
Federalny Rzecznik Ochrony Danych, Niemcy;
Garante per la protezione dei dati personali, Włochy;
Rzecznik Ochrony Danych, Nowa Zelandia;
Rzecznik Ochrony Danych i Informacji (FDPIC), Szwajcaria

Rezolucja
Serwisy społecznościowe[1] stały się bardzo popularne w ostatnich latach. Pozwalają one swym użytkownikom wchodzić w interakcje oparte na samodzielnie stworzonych profilach osobowych, które przyczyniają się do ujawniania na bezprecedensową skalę informacji o ich właścicielach i innych osobach. Serwisy społecznościowe dają nowe możliwości komunikacji i wymiany wszelkiego rodzaju informacji w czasie rzeczywistym, mogą jednak również stanowić zagrożenie dla prywatności swych użytkowników i innych osób: dane różnych osób, w tym ogromne ilości zdjęć i filmów, stają się publicznie (i globalnie) dostępne w bezprecedensowy sposób i w bezprecedensowej ilości. Osoby, których dane dotyczą mogą stracić kontrolę nad tym, jak ich dane będą używane przez inne osoby po opublikowaniu w sieci. Choć określenie „społecznościowy" sugeruje, że ujawnianie danych osobowych przypominać może dzielenie się informacją z przyjaciółmi, tak jak odbywa się to podczas osobistych kontaktów, informacje z profilu mogą w istocie być dostępne dla wszystkich członków serwisu (liczonych w milionach).

Obecnie ochrona przed kopiowaniem wszelkiego rodzaju danych osobowych z profili – przez innych członków serwisu lub nieupoważnione strony trzecie – i użyciem ich do tworzenia innych profili bądź publikowaniem w innych miejscach – jest bardzo słaba. Całkowite usunięcie informacji po ich opublikowaniu w internecie może być bardzo trudne, a w niektórych przypadkach niemożliwe: nawet po usunięciu ze strony, na której zostały pierwotnie zamieszczone (np. serwisu społecznościowego), kopie mogą pozostać w posiadaniu stron trzecich lub dostawców serwisów społecznościowych. Dane osobowe z profili mogą także „wyciekać" poza serwis, jeśli zostaną zaindeksowane przez wyszukiwarki. Ponadto niektórzy dostawcy serwisów społecznościowych udostępniają dane stronom trzecim poprzez interfejsy programu użytkownika (API), pozostające pod kontrolą tych stron trzecich.

Szeroko dyskutowanym przykładem wtórnego użycia danych jest sprawdzanie przez dział kadr profile osób starających się o pracę lub pracowników: według doniesień pracy, już jedna trzecia zarządzających zasobami ludzkimi przyznaje się do używania w pracy danych z serwisów społecznościowych, np. do celów weryfikacji lub uzupełniania danych osób ubiegających się o pracę.

---

[1] "Serwis społecznościowy służy do tworzenia i potwierdzania sieci społecznych osób, które mają podobne zainteresowania lub chcą poznać zainteresowania innych […]. Większość serwisów społecznościowych oparta jest na sieci i dostarcza użytkownikom wielu sposobów komunikacji […]". Cytat z Wikipedii:
http://en.wikipedia.org/wiki/Social_network_service .

Informacje z profili i dane o ruchu wykorzystywane są także przez dostawców serwisów społecznościowych do przesyłania użytkownikom profilowanych wiadomości marketingowych.

Bardzo możliwe jest, że w przyszłości pojawią się kolejne nieoczekiwane zastosowania informacji z profili użytkowników.

Inne stwierdzone dotąd zagrożenia dla prywatności i bezpieczeństwa to między innymi zwiększone ryzyko kradzieży tożsamości, ułatwionej przez szeroką dostępność danych z profili użytkowników i przez możliwość przejmowania profili przez nieupoważnione strony trzecie. 30. Międzynarodowa Konferencja Rzeczników Ochrony Danych przypomina, że zagrożenia te zostały już przeanalizowane w "Raporcie i wytycznych w sprawie prywatności w serwisach społecznościowych" ("Memorandum Rzymskie")[2] z 43. posiedzenia Międzynarodowej Grupy Roboczej ds. Prywatności w Telekomunikacji oraz w Stanowisku ENISA Nr 1 "Kwestie bezpieczeństwa i zalecenia dla internetowych portali społecznościowych"[3] (październik 2007).

Rzecznicy ochrony danych zebrani na Konferencji Międzynarodowej są przeświadczeni, że konieczne jest, po pierwsze, przeprowadzenie szczegółowej kampanii informacyjnej obejmującej wszystkie strony zainteresowane z sektorów publicznego i prywatnego – od organów administracji rządowej po instytucje edukacyjne, od dostawców serwisów społecznościowych po związki konsumentów i użytkowników, obejmującej również samych rzeczników ochrony danych – aby zapobiec licznym zagrożeniom związanym z użytkowaniem serwisów społecznościowych.

Zalecenia
Biorąc pod uwagę szczególny charakter tych serwisów oraz krótko- i długoterminowe zagrożenia dla prywatności osób, Konferencja wydaje następujące zalecenia dla użytkowników i dostawców serwisów społecznościowych:

<u>Użytkownicy serwisów społecznościowych</u>

Organizacje dbające o dobro użytkowników serwisów społecznościowych – w tym dostawcy usług, władze i organy ochrony danych – powinny pomagać w edukacji użytkowników w zakresie ochrony ich danych osobowych i przekazywać im następujące informacje.

1. Publikacja informacji
Użytkownicy serwisów społecznościowych powinni uważnie przemyśleć jakie dane osobowe – jeśli w ogóle – zamieszczają na profilu w serwisach społecznościowych. Powinni pamiętać, że opublikowane informacje bądź zdjęcia mogą później zostać użyte np. podczas procesu rekrutacyjnego. W szczególności osoby nieletnie powinny unikać ujawniania adresu domowego i numeru telefonu.

Użytkownicy powinni rozważyć użycie pseudonimu zamiast prawdziwego nazwiska w profilu, mając jednak przy tym na uwadze, że działanie takie nie daje pełnej ochrony, gdyż osoby trzecie mogą odgadnąć, kto kryje się za pseudonimem.

2. Prywatność innych osób
Użytkownicy powinni również szanować prywatność innych osób. Powinni zachowywać szczególną ostrożność publikując dane innych osób (w tym zdjęcia, także te oznaczone) bez zgody tych osób.

---

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491
[3] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

Dostawcy serwisów społecznościowych

Na dostawcach serwisów społecznościowych spoczywa szczególny obowiązek ostrożności i działania w interesie osób korzystających z serwisów. Poza spełnianiem wymogów przepisów o ochronie danych powinni oni stosować się również do poniższych zaleceń.

1. Przepisy i standardy w zakresie prywatności
Dostawcy działający na terenie różnych krajów bądź globalnie powinni przestrzegać standardów w zakresie prywatności obowiązujących w krajach, w których działają. W tym celu powinny, w miarę potrzeb, kontaktować się z organami ochrony danych.

2. Informowanie użytkowników
Dostawcy serwisów społecznościowych powinni informować użytkowników o przetwarzaniu ich danych osobowych w sposób przejrzysty i otwarty. Powinni także podawać proste, zrozumiałe informacje o możliwych konsekwencjach zamieszczania danych osobowych w profilu oraz innych zagrożeniach bezpieczeństwa, a także dostępie do danych, jaki osoby trzecie (np. organy wymiaru sprawiedliwości) mogą uzyskać legalnie. Takie informacje powinny obejmować także wskazówki dotyczące obchodzenia się z danymi osobowymi innych osób zawartymi w profilu danego użytkownika.

3. Kontrola przez użytkowników
Dostawcy powinni zwiększać kontrolę użytkowników nad wykorzystaniem danych z ich profili przez innych członków społeczności. Powinni zapewnić możliwość ograniczenia wyświetlania całych profili lub zawartych w nich danych w wyszukiwarkach serwisu.

Dostawcy powinni także pozwolić na kontrolę użytkowników nad wtórnym wykorzystaniem danych z profili i danych o ruchu np. do celów marketingu profilowanego. Opcją minimalną powinna być możliwość opt-out dla ogólnych danych z profilu oraz opt-in dla danych szczególnie chronionych (np. o przekonaniach politycznych czy orientacji seksualnej) oraz danych o ruchu.

4. Ustawienia domyślne przyjazne dla prywatności
Ponadto, dostawcy powinni zapewniać przyjazne dla prywatności ustawienia domyślne dla informacji z profilu użytkownika. Ustawienia domyślne odgrywają kluczową rolę w ochronie prywatności użytkowników: wiadome jest, że jedynie niewielki odsetek osób korzystających z serwisu wprowadza w nich zmiany. Ustawienia takie powinny być szczególnie restrykcyjne jeśli serwis społecznościowy skierowany jest do osób nieletnich.

5. Bezpieczeństwo
Dostawcy powinni nieprzerwanie utrzymywać i poprawiać bezpieczeństwo swych systemów informacyjnych i chronić użytkowników przed nielegalnym dostępem do ich profili, stosując uznane dobre praktyki (w tym niezależnych audytów i certyfikacji) podczas projektowania, tworzenia i wykorzystywania aplikacji.

6. Prawo dostępu
Dostawcy powinni zapewnić osobom (niezależnie od tego, czy są użytkownikami serwisu), prawo dostępu i, w razie konieczności, poprawiania wszystkich ich danych osobowych znajdujących się w posiadaniu dostawców.

7. Usuwanie profili użytkowników
Dostawcy powinni pozwalać użytkownikom na łatwe zakończenie członkostwa, usunięcie profile oraz wszelkich danych i innych treści, jakie zamieścili w serwisie.

8. Korzystanie z serwisu pod pseudonimem

Dostawcy powinni umożliwić tworzenie i korzystanie z profili oznaczonych pseudonimami, i zachęcać użytkowników do korzystania z tej możliwości.

9. Dostęp stron trzecich
Dostawcy powinni podejmować skuteczne środki zapobiegające zastosowaniu robotów internetowych na danych profili użytkowników.

10. Indeksowalność profili użytkowników
Dostawcy powinni zapewnić, że dane użytkownika będą wyświetlane w zewnętrznych wyszukiwarkach jedynie, jeśli uprzednio wyraził na to wyraźną, świadomą zgodę. Nieindeksowalność profili przez wyszukiwarki powinna stanowić ustawienie domyślne.