GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH OSOBOWYCH

881/11/PL
WP 185

Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych

Przyjęta w dniu 16 maja 2011 r.

SPIS TREŚCI

1. Wprowadzenie 3
2. Kontekst: różne infrastruktury geolokalizacji 4
    2.1 Dane stacji bazowej 4
    2.2 Technologia GPS 5
    2.3 WiFi 5
        2.3.1 Punkty dostępu WiFi 5
3. Zagrożenia dla prywatności 7
4. Ramy prawne 8
    4.1 Dane stacji bazowej przetwarzane przez operatorów telekomunikacyjnych 8
    4.2 Dane stacji bazowej, dane WiFi i GPS przetwarzane przez dostawców usług społeczeństwa informacyjnego 9
        4.2.1 Zastosowanie zmienionej dyrektywy o prywatności i łączności elektronicznej 9
        4.2.2 Zastosowanie dyrektywy o ochronie danych 10
5. Zobowiązania wynikające z przepisów dotyczących ochrony danych 12
    5.1 Administrator danych 12
        5.1.1 Administratorzy infrastruktury geolokalizacji 12
        5.1.2 Dostawcy aplikacji wyposażonych w funkcję geolokalizacji i usług geolokalizacyjnych 13
        5.1.3 Twórca systemu operacyjnego 13
    5.2 Obowiązki innych stron 14
    5.3 Uzasadnione podstawy 14
        5.3.1 Inteligentne urządzenia przenośne 14
        5.3.2 Punkty dostępu WiFi 17
    5.4 Informacje 18
    5.5 Prawa osób, których dotyczą dane 19
    5.6 Okresy przechowywania 20
6. Wnioski 20

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH
ustanowiona na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając art. 29 i art. 30 ust. 1 lit. a) i ust. 3 przedmiotowej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZY DOKUMENT:

1. Wprowadzenie

Informacja geograficzna odgrywa ważną rolę w naszym społeczeństwie. Prawie wszystkie działania i decyzje ludzi zawierają element geograficzny. Zasadniczo, kiedy informacja wiąże się z lokalizacją, jej wartość wzrasta. Z położeniem geograficznym można powiązać różne rodzaje informacji, takie jak dane finansowe, dane dotyczące zdrowia i inne dane dotyczące zachowania konsumentów. Wraz z szybkim rozwojem technologicznym i rosnącą popularnością inteligentnych urządzeń przenośnych powstaje nowa kategoria usług opartych na lokalizacji.

Celem niniejszej opinii jest wyjaśnienie ram prawnych mających zastosowanie do usług geolokalizacyjnych dostępnych w inteligentnych urządzeniach przenośnych lub generowanych przez inteligentne urządzenia przenośne, które mogą łączyć się z Internetem i są wyposażone w czujniki lokalizacyjne, takie jak GPS. Przykłady tych usług to: mapy i nawigacja, usługi spersonalizowane pod względem geolokalizacji (w tym najbliższe użyteczne miejsca - POI), rozszerzona rzeczywistość, geotagowanie treści internetowych, śledzenie miejsc pobytu przyjaciół, kontrola dzieci oraz reklama oparta na lokalizacji.

W niniejszej opinii odniesiono się również do trzech najważniejszych rodzajów infrastruktury stosowanych w celu zapewnienia usług geolokalizacyjnych, mianowicie GPS, stacji bazowych GSM i WiFi. Szczególną uwagę poświęcono nowej infrastrukturze opartej na lokalizacji punktów dostępu WiFi.

Grupa Robocza jest świadoma faktu, że istnieje wiele innych usług, które przetwarzają dane dotyczące lokalizacji i mogą powodować problemy związane z ochroną danych. Usługi te są zróżnicowane i obejmują systemy biletów elektronicznych i systemów opłat za przejazd samochodów oraz usługi nawigacji satelitarnej, śledzenie lokalizacji na przykład za pomocą kamer i geolokalizacji adresów IP. W związku z szybkim rozwojem technologicznym, szczególnie w odniesieniu do mapowania bezprzewodowych punktów dostępu, w połączeniu z faktem, że nowi uczestnicy rynku przygotowują się do opracowania nowych usług opartych na lokalizacji, korzystających ze stacji bazowej oraz danych GPS i WiFi, Grupa Robocza zdecydowała jednak, że w szczególności należy wyjaśnić wymogi prawne obowiązujące w odniesieniu do tych usług na mocy dyrektywy o ochronie danych.

W niniejszej opinii w pierwszej kolejności opisano technologię, następnie określono i oceniono zagrożenia dla prywatności, a następnie przedstawiono wnioski dotyczące stosowania odpowiednich artykułów prawnych w odniesieniu do różnych administratorów danych, którzy gromadzą i przetwarzają dane dotyczące lokalizacji otrzymane z urządzeń przenośnych. Dotyczy to na przykład dostawców infrastruktury geolokalizacji, producentów inteligentnych telefonów przenośnych i twórców aplikacji opartych na geolokalizacji.

W niniejszej opinii nie oceniono szczególnej technologii geotagowania powiązanej z tzw. technologią web 2.0, w której użytkownicy włączają informacje oparte na geograficznych punktach odniesienia do serwisów społecznościowych, takich jak Facebook lub Twitter. W niniejszej opinii nie zostaną również szczegółowo omówione inne technologie geolokalizacyjne stosowane w celu łączenia ze sobą urządzeń na stosunkowo małym obszarze (w centrach handlowych, portach lotniczych, budynkach biurowych itd.), takie jak Bluetooth, ZigBee, funkcja geo-fence i identyfikatory RFID oparte na technologii bezprzewodowej, mimo że wiele wniosków niniejszej opinii w odniesieniu do uzasadnionej podstawy, informacji i praw osób, których dotyczą dane, ma zastosowanie także do powyższych technologii, gdy są one stosowane do geolokalizacji osób za pośrednictwem wykorzystywanych przez nie urządzeń.

2. Kontekst: różne infrastruktury geolokalizacji

2.1 Dane stacji bazowej

Obszar obsługiwany przez różnych operatorów telekomunikacyjnych jest podzielony na obszary znane powszechnie jako komórki. Aby możliwe było korzystanie z przenośnego telefonu lub połączenie z Internetem przy użyciu łączności 3G, urządzenie przenośne musi się połączyć z anteną (zwaną dalej stacją bazową), która obsługuje daną komórkę. Komórki obejmują obszary o różnych rozmiarach, w zależności od zakłóceń spowodowanych na przykład przez góry i wysokie budynki.

Zawsze, gdy urządzenie przenośne jest włączone, jest ono połączone z konkretną stacją bazową. Operator telekomunikacyjny stale rejestruje te połączenia. Każda stacja bazowa posiada niepowtarzalny numer identyfikacyjny i jest zarejestrowana w konkretnej lokalizacji. Zarówno operator telekomunikacyjny, jak i wiele urządzeń przenośnych może korzystać z sygnałów pochodzących z pokrywających się komórek (sąsiadujących ze sobą stacji bazowych), aby ustalić położenie urządzenia przenośnego ze zwiększoną dokładnością. Technikę tę nazywa się również triangulacją.

Dokładność można dodatkowo zwiększyć za pomocą takich informacji, jak RSSI (wskaźnik mocy odbieranego sygnału), TDOA (różnica czasu przyjścia sygnałów) i AOA (kąt odbioru sygnału).

Dane stacji bazowej można wykorzystywać w innowacyjny sposób, na przykład w celu wykrywania korków drogowych. Każda droga charakteryzuje się średnią prędkością dla każdej pory dnia, ale jeżeli przekazanie danych do następnej stacji bazowej trwa dłużej, niż oczekiwano, najwyraźniej utworzył się korek drogowy.

Podsumowując, metoda pozycjonowania zapewnia szybkie, szacunkowe wskazanie lokalizacji, ale niezbyt dokładne w porównaniu z danymi GPS i WiFi. Dokładność wynosi około 50 metrów w gęsto zaludnionych obszarach miejskich, ale nawet kilka kilometrów w obszarach wiejskich.

2.2 Technologia GPS

Inteligentne urządzenia przenośne posiadają chipsety z odbiornikami GPS, które określają ich lokalizację.

Technologia GPS (Globalny System Pozycjonowania) wykorzystuje 31 satelitów, z których każdy obraca się na jednej z sześciu różnych orbit wokół Ziemi[1]. Każdy satelita przekazuje bardzo dokładny sygnał radiowy.

Urządzenie przenośne może określić swoją lokalizację, jeżeli czujnik GPS wychwytuje co najmniej cztery takie sygnały. W odróżnieniu od danych stacji bazowej sygnał GPS przenosi się tylko w jedną stronę. Podmioty zarządzające satelitami nie są w stanie śledzić urządzeń, które odebrały sygnał radiowy.

Technologia GPS zapewnia precyzyjne pozycjonowanie, z dokładnością od 4 do 15 metrów. Poważną wadą technologii GPS jest fakt, że charakteryzuje ją stosunkowo wolne uruchamianie[2]. Kolejną wadą tej technologii jest to, że nie działa w ogóle lub nie działa dobrze w pomieszczeniach. W praktyce technologia GPS jest zatem często łączona z danymi stacji bazowej lub z mapowanymi punktami dostępu WiFi.

2.3 WiFi

2.3.1 Punkty dostępu WiFi

Stosunkowo nowym źródłem informacji geolokalizacyjnych jest wykorzystywanie punktów dostępu WiFi. Technologia ta jest podobna do wykorzystywania stacji bazowych. Obie technologie opierają się na niepowtarzalnym numerze identyfikacyjnym (przypisanym przez stację bazową lub punkt dostępu WiFi), który może zostać wykryty przez urządzenie przenośne i przesłany do usługi, która posiada lokalizację każdego niepowtarzalnego numeru identyfikacyjnego.

---

[1] Globalny System Pozycjonowania składa się z satelitów umieszczonych na orbicie przez Stany Zjednoczone Ameryki do celów wojskowych. Do 2014 r. Komisja Europejska zamierza umieścić na orbicie system Galileo, czyli sieć 18 satelitów zapewniającą bezpłatne, niewojskowe globalne pozycjonowanie satelitarne. Umieszczenie pierwszych dwóch satelitów ma nastąpić w 2011 r., kolejnych dwóch w 2012 r. Źródło: Komisja Europejska, „Commission presents midterm review of Galileo and EGNOS" [Komisja przedstawia przegląd śródokresowy systemów Galileo i EGNOS], 25 stycznia 2011 r., URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displayType=news&tpa_id=0&item_id=4835

[2] W celu przyspieszenia wstępnego wykrywania sygnału GPS można wcześniej załadować tak zwane tęczowe tablice zawierające oczekiwane pozycjonowanie różnych satelitów w ciągu następnych kilku tygodni.

Niepowtarzalny numer identyfikacyjny każdego punktu dostępu WiFi to jego adres MAC (kontrola dostępu do medium transmisyjnego). Adres MAC jest niepowtarzalnym identyfikatorem przypisywanym do interfejsu sieci i zazwyczaj rejestrowanym na sprzęcie komputerowym, takim jak układy pamięciowe lub karty sieciowe w komputerach, telefonach, laptopach lub punktach dostępu[3].

Punkty dostępu WiFi można wykorzystać jako źródło informacji geolokalizacyjnych, ponieważ bez przerwy zgłaszają one swoje istnienie. Większość punktów dostępu do Internetu szerokopasmowego domyślnie posiada również antenę WiFi. W domyślnym ustawieniu większości powszechnie wykorzystywanych punktów dostępu w Europie połączenie pozostaje włączone również w przypadku, gdy użytkownik podłączył swój komputer (komputery) do punktu dostępu jedynie za pomocą przewodów kablowych. W porównaniu z technologią radiową punkt dostępu WiFi bez przerwy przekazuje swoją nazwę sieciową i swój adres MAC, nawet jeżeli nikt nie korzysta z połączenia i nawet jeżeli treści połączenia bezprzewodowego są zaszyfrowane w standardzie WEP, WPA lub WPA2.

Istnieją dwa różne sposoby gromadzenia adresów MAC punktów dostępu WiFi[4].

1. Skanowanie aktywne: przesyłanie aktywnych żądań[5] do wszystkich pobliskich punktów dostępu WiFi i rejestrowanie odpowiedzi. Odpowiedzi te nie obejmują informacji na temat urządzeń połączonych z punktem dostępu WiFi.

2. Skanowanie pasywne: rejestrowanie okresowych ramek sygnału nawigacyjnego przekazywanych przez każdy punkt dostępu (zazwyczaj 10 razy na sekundę). W ramach niestandardowej alternatywy niektóre narzędzia bardziej szczegółowo rejestrują wszystkie ramki WiFi przekazywane przez punkty dostępu, w tym również te, które nie wysyłają sygnałów nawigacyjnych. Jeżeli ten rodzaj skanowania przeprowadza się bez właściwego celowego zastosowania prywatności, może to prowadzić do gromadzenia danych wymienianych między punktami dostępu a urządzeniami połączonymi z tymi punktami. W ten sposób mogą być rejestrowane adresy MAC komputerów stacjonarnych, laptopów i drukarek. Tego rodzaju skanowanie może również prowadzić do niezgodnego z prawem rejestrowania treści połączeń. Powyższe treści można łatwo odczytać, jeżeli właściciel punktu dostępu WiFi nie włączył szyfrowania WiFi (WEP/WPA/WPA2).

Lokalizację punktu dostępu WiFi można obliczyć na dwa różne sposoby.

1. Statycznie/jednorazowo: administratorzy danych sami gromadzą adresy MAC punktów dostępu WiFi, poruszając się pojazdami wyposażonymi w anteny. Rejestrują dokładną szerokość i długość geograficzną pojazdu w momencie przechwytywania

---

3 Przykładem adresu MAC jest: 00-1F-3F-D7-3C-58. Adres MAC punktu dostępu WiFi nazywa się BSSID (identyfikator podstawowego zestawu usług).

4 Skanowanie aktywne i pasywne zostały znormalizowane w standardzie IEEE 802.11 w celu wykrycia punktów dostępu.

5 W celu zgromadzenia adresów MAC zbierający przesyła „sygnał próbkujący" (ang. *probe request*) do wszystkich punktów dostępu.

sygnału i mogą w ten sposób obliczyć lokalizację punktów dostępu w oparciu między innymi o moc sygnału.

2. Dynamicznie/nieprzerwanie: użytkownicy usług geolokalizacyjnych automatycznie gromadzą adresy MAC przechwytywane przez ich urządzenia korzystające z WiFi, kiedy używają oni na przykład mapy on-line w celu określenia własnej lokalizacji (Gdzie jestem?). Urządzenie przenośne przesyła następnie wszystkie dostępne informacje do usługodawcy geolokalizacji, w tym adresy MAC, SSID i moc sygnału. Administrator danych może wykorzystywać te ciągłe obserwacje do obliczania lub podawania dokładniejszych lokalizacji punktów dostępu WiFi w swojej bazie danych z mapowanymi punktami dostępu WiFi.

Należy zauważyć, że urządzenia przenośne nie muszą „łączyć się" z punktami dostępu WiFi, aby gromadzić informacje na temat WiFi. Automatycznie wykrywają one obecność punktów dostępu (w trybie aktywnego lub pasywnego skanowania) i automatycznie gromadzą dotyczące ich dane.

Ponadto telefony przenośne żądające podania ich geolokalizacji nie tylko wysyłają dane WiFi, ale często również wszelkie inne informacje dotyczące lokalizacji, jakie posiadają, w tym dane GPS i dane stacji bazowych. Umożliwia to usługodawcy obliczanie lokalizacji „nowych" punktów dostępu WiFi lub podawanie dokładniejszej lokalizacji punktów dostępu WiFi, które już znajdują się w bazie danych. W ten sposób gromadzenie informacji dotyczących punktów dostępu WiFi jest w bardzo skuteczny sposób zdecentralizowane, czego niekoniecznie muszą być świadomi klienci.

Podsumowując: geolokalizacja oparta na punktach dostępu WiFi zapewnia szybką i – dzięki ciągłym pomiarom – coraz dokładniejszą lokalizację.

3. Zagrożenia dla prywatności

Inteligentne urządzenie przenośne jest bardzo ściśle powiązane z konkretną osobą. Większość osób zazwyczaj trzyma swoje urządzenia przenośne blisko siebie, w kieszeni lub torbie, bądź też w szafce nocnej przy swoim łóżku.

Rzadko zdarza się, aby dana osoba pożyczała takie urządzenie innej osobie. Większość ludzi zadaje sobie sprawę, że ich urządzenia przenośne zawierają szereg bardzo prywatnych informacji, od wiadomości e-mail po prywatne zdjęcia, od historii przeglądanych stron do na przykład listy kontaktów.

Umożliwia to dostawcom usług opartych na geolokalizacji zdobycie prywatnych informacji dotyczących nawyków i schematów postępowania właściciela takiego urządzenia oraz tworzenie obszernych profilów. Ze schematu braku aktywności w nocy można wywnioskować miejsce, w którym śpi dana osoba, a z regularnego schematu podróżowania rano można wywnioskować lokalizację pracodawcy.

Schemat może również zawierać dane pochodzące ze schematów przemieszczania się znajomych, w oparciu o tzw. *wykres społeczny*[6].

Wzorzec zachowania może obejmować również *specjalne kategorie danych*, jeżeli odkrywa on na przykład wizyty w szpitalu i miejscach o znaczeniu religijnym, obecność na demonstracjach politycznych lub obecność w innych szczególnych miejscach ujawniających dane na przykład dotyczące życia seksualnego. Profile te mogą zostać wykorzystane do podjęcia decyzji, które w znaczący sposób dotyczą właściciela.

Technologia stosowana w inteligentnych urządzeniach przenośnych umożliwia ciągłe monitorowanie danych dotyczących lokalizacji. Smartfony mogą bez przerwy zbierać sygnały ze stacji bazowych i punktów dostępu WiFi. Z technicznego punktu widzenia monitorowanie może być prowadzone potajemnie, bez informowania o tym właściciela. Monitorowanie może być również prowadzone częściowo potajemnie, kiedy ludzie „zapominają" lub nie są właściwie poinformowani o tym, że usługi lokalizacyjne są włączone, lub kiedy zmienia się ustawienia dostępności danych dotyczących lokalizacji z „prywatnych" na „publiczne".

Nawet jeżeli ludzie celowo udostępniają swoje dane geolokalizacyjne w Internecie za pomocą usług dotyczących miejsca pobytu i geotagowania, nieograniczony i pełny dostęp stwarza nowe zagrożenia, które mogą obejmować kradzież danych i włamania, a nawet fizyczną napaść i nękanie.

Podobnie jak w przypadku innych nowych technologii, poważnym zagrożeniem związanym z wykorzystywaniem danych dotyczących lokalizacji jest rozrost funkcji, czyli fakt, że w związku z dostępnością nowego rodzaju danych obierane są nowe cele, których nie przewidziano w momencie pierwotnego gromadzenia danych.

4. Ramy prawne

Właściwe ramy prawne stanowi dyrektywa o ochronie danych (95/46/WE). Ma ona zastosowanie w każdej sytuacji, w której w wyniku przetwarzania danych dotyczących lokalizacji przetwarzane są dane osobowe. Dyrektywa o prywatności i łączności elektronicznej (2002/58/WE zmieniona dyrektywą 2009/136/WE) ma zastosowanie jedynie do przetwarzania danych stacji bazowej przez publiczne usługi i sieci łączności elektronicznej (operatorów telekomunikacyjnych).

4.1 Dane stacji bazowej przetwarzane przez operatorów telekomunikacyjnych

Operatorzy telekomunikacyjni stale przetwarzają dane stacji bazowej w ramach świadczenia publicznych usług łączności elektronicznej[7]. Mogą oni również przetwarzać dane stacji bazowej w celu świadczenia usług o wartości dodanej. Grupa

---

[6] „Wykres społeczny" to pojęcie wskazujące widoczność znajomych na stronach serwisów społecznościowych i możliwość wywnioskowania wzorców zachowania z danych dotyczących znajomych.

[7] Należy zauważyć, że zapewnianie publicznych hotspotów WiFi przez dostawców usług telekomunikacyjnych również kwalifikuje się jako publiczna usługa łączności elektronicznej, dlatego powinno przede wszystkim spełniać wymogi określone w przepisach dyrektywy o prywatności i łączności elektronicznej.

Robocza zajęła się już przedmiotową sprawą w opinii 5/2005 (WP115). Mimo że niektóre przykłady podane w opinii nieuchronnie się zdezaktualizowały ze względu na wprowadzanie technologii internetowej i czujników w coraz mniejszych urządzeniach, wnioski i zalecenia prawne przedmiotowej opinii pozostają ważne w odniesieniu do wykorzystywania danych stacji bazowej.

1. W związku z tym, że dane dotyczące lokalizacji uzyskane ze stacji bazowych odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, podlegają one przepisom dotyczącym ochrony danych osobowych ustanowionym w dyrektywie 95/46/WE z dnia 24 października 1995 r.
2. Dyrektywa 2002/58/WE z dnia 12 lipca 2002 r. (zmieniona w listopadzie 2009 r. dyrektywą 2009/136/WE) również ma zastosowanie, zgodnie z definicją zawartą w art. 2 lit. c) przedmiotowej dyrektywy:
   „dane dotyczące lokalizacji" oznaczają wszelkie dane przetwarzane w sieci łączności elektronicznej wskazujące położenie geograficzne wyposażenia terminala użytkownika publicznie dostępnych usług łączności elektronicznej;

Jeżeli operator telekomunikacyjny oferuje połączoną usługę geolokalizacyjną opartą również na przetwarzaniu innych rodzajów danych dotyczących lokalizacji, takich jak dane GPS i WiFi, działanie takie kwalifikuje się jako publiczna usługa łączności elektronicznej. Jeżeli operator telekomunikacyjny dostarcza te dane geolokalizacyjne osobom trzecim, musi uzyskać uprzednią zgodę swoich klientów.

4.2 Dane stacji bazowej, dane WiFi i GPS przetwarzane przez dostawców usług społeczeństwa informacyjnego

4.2.1 Zastosowanie zmienionej dyrektywy o prywatności i łączności elektronicznej

Zazwyczaj przedsiębiorstwa, które dostarczają usługi i aplikacje lokalizacyjne, oparte na połączeniu danych stacji bazowej, danych GPS i danych WiFi, to przedsiębiorstwa świadczące *usługi społeczeństwa informacyjnego.* W związku z tym przedsiębiorstwa te są wyraźnie wyłączone z zakresu obowiązywania dyrektywy o prywatności i łączności elektronicznej, jak wynika ze ścisłej definicji usługi łączności elektronicznej (art. 2 lit. c) zmienionej dyrektywy ramowej (niezmieniony))[8].

Dyrektywa o prywatności i łączności elektronicznej nie ma zastosowania do przetwarzania danych dotyczących lokalizacji przez służby społeczeństwa informacyjnego, nawet jeżeli takie przetwarzanie odbywa się za pośrednictwem publicznej sieci łączności elektronicznej. Użytkownik może zdecydować się na przesłanie danych GPS przez Internet na przykład w trakcie korzystania z usług nawigacyjnych w Internecie. W takim przypadku sygnał GPS jest przekazywany na

[8] Dyrektywa 2002/21/WE z dnia 7 marca 2002 r., art. 2 lit. c): *„usługa łączności elektronicznej" oznacza usługę zazwyczaj świadczoną za wynagrodzeniem, polegającą całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze; nie obejmuje jednak usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej. Spod zakresu niniejszej definicji wyłączone są usługi społeczeństwa informacyjnego w rozumieniu art. 1 dyrektywy 98/34/WE, jeżeli nie polegają one całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej;*

poziomie aplikacji łączności internetowej niezależnie od sieci GSM. Dostawca usług telekomunikacyjnych działa wyłącznie jako kanał. Nie może uzyskać dostępu do danych GPS lub WiFi ani do danych stacji bazowej przesyłanych z i do inteligentnego urządzenia przenośnego między użytkownikiem/abonentem a usługą społeczeństwa informacyjnego bez użycia środków w znaczny sposób naruszających prywatność, takich jak *głęboka inspekcja pakietów (DPI)*.

4.2.2 Zastosowanie dyrektywy o ochronie danych

Jeżeli zmieniona dyrektywa o prywatności i łączności elektronicznej nie ma zastosowania, zgodnie z art. 1 ust. 2 zastosowanie ma dyrektywa 95/46/WE: „przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE zgodnie z celami przedstawionymi w ust. 1".

Na podstawie dyrektywy o ochronie danych dane osobowe oznaczają *wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość* – art. 2 lit. a) dyrektywy.

W motywie 26 dyrektywy zwrócono szczególną uwagę na pojęcie „możliwy do zidentyfikowania", określając, że „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby".

W motywie 27 dyrektywy określono szeroki zakres ochrony: „zakres tej ochrony nie może w swym skutku być zależny od zastosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia zasad".

W opinii 4/2007 w sprawie pojęcia danych osobowych Grupa Robocza przedstawiła obszerne wytyczne dotyczące definicji danych osobowych.

Inteligentne urządzenia przenośne

Inteligentne urządzenia przenośne są nierozerwalnie powiązane z osobami fizycznymi. Zazwyczaj można je zidentyfikować w sposób bezpośredni lub pośredni.

Po pierwsze, operator telekomunikacyjny zapewniający dostęp do sieci GSM i do przenośnego Internetu zazwyczaj posiada rejestr zawierający imię i nazwisko, adres i informacje dotyczące konta bankowego każdego klienta, w połączeniu z kilkoma niepowtarzalnymi numerami urządzenia, takimi jak IMEI i IMSI.

Po drugie, zakup dodatkowego oprogramowania do urządzenia (*aplikacje*) zazwyczaj wymaga numeru karty kredytowej i w ten sposób powiększa kombinację niepowtarzalnego numeru lub numerów i danych dotyczących lokalizacji z danymi identyfikującymi bezpośrednio.

Pośrednią identyfikację można osiągnąć poprzez połączenie niepowtarzalnego numeru lub numerów urządzenia z co najmniej jedną obliczoną lokalizacją.

Każde inteligentne urządzenie przenośne posiada co najmniej jeden niepowtarzalny identyfikator, czyli adres MAC. Urządzenie może posiadać inne niepowtarzalne numery identyfikacyjne, dodane przez producenta systemu operacyjnego. Identyfikatory te mogą być przekazywane i dalej przetwarzane w ramach usług geolokalizacyjnych. Lokalizację konkretnego urządzenia można rzeczywiście obliczyć z bardzo dużą dokładnością, w szczególności jeżeli połączone są różne infrastruktury geolokalizacji. Taka lokalizacja może wskazać adres domu lub pracodawcę. Możliwe jest zidentyfikowanie właściciela urządzenia, w szczególności dzięki regularnym obserwacjom.

Kiedy rozważa się dostępne środki potrzebne do identyfikowania, należy uwzględnić sytuację, w której ludzie zamieszczają w Internecie coraz większą ilość danych osobowych dotyczących lokalizacji, na przykład poprzez publikowanie lokalizacji swojego domu lub miejsca pracy w połączeniu z innymi danymi identyfikującymi. Takie podawanie danych może następować również bez ich wiedzy, kiedy są geotagowani przez inne osoby. Sytuacja ta ułatwia powiązanie lokalizacji lub wzorca zachowania z daną osobą.

Ponadto, zgodnie z opinią 4/2007 w sprawie pojęcia danych osobowych, należy zauważyć, że niepowtarzalny identyfikator w powyższym kontekście umożliwia śledzenie użytkownika konkretnego urządzenia i w ten sposób umożliwia „wyodrębnienie" użytkownika, nawet jeżeli jego prawdziwe nazwisko nie jest znane.

Punkty dostępu WiFi
Możliwość pośredniego identyfikowania ma zastosowanie również do punktów dostępu WiFi[9]. Adres MAC punktu dostępu WiFi w połączeniu z jego obliczoną lokalizacją jest nierozerwalnie powiązany z lokalizacją właściciela punktu dostępu.

Stosownie wyposażony administrator danych może z coraz większą precyzją obliczać lokalizację punktu dostępu WiFi w oparciu o moc sygnału i o ciągłe aktualizacje lokalizacji za pomocą użytkowników jego usługi geolokalizacyjnej.

Za pomocą tych zasobów w wielu przypadkach można zidentyfikować małą grupę mieszkań lub domów, w których mieszka właściciel punktu dostępu. Łatwość, z jaką możliwe jest zidentyfikowanie tego właściciela na podstawie adresu MAC, będzie zależeć od otoczenia:

- na rzadko zaludnionych obszarach, w których adres MAC wskazuje pojedynczy dom, właściciela miejsca zamieszkania można bezpośrednio określić za pomocą takich narzędzi, jak rejestry własności domu, bazy danych zawierające informacje o użytkownikach, wykazy osób uprawnionych do głosowania w wyborach lub nawet proste zapytanie w wyszukiwarce[10];
- na gęściej zaludnionych obszarach za pomocą zasobów, takich jak moc sygnału lub SSID (które może wykryć każda osoba posiadająca urządzenie wyposażone w WiFi), można określić dokładną lokalizację punktu dostępu i w

[9] Punkty dostępu WiFi można nawet identyfikować bezpośrednio, jeżeli dostawca dostępu do Internetu posiada rejestr adresów MAC dla routerów WiFi, które dostarcza swoim zidentyfikowanym klientom.

[10] Dostępność takich rejestrów lub katalogów jest różna w poszczególnych państwach członkowskich.

ten sposób w wielu przypadkach potwierdzić tożsamość osoby lub osób mieszkających dokładnie w miejscu (domu lub mieszkaniu), w którym znajduje się punkt dostępu;
- na bardzo gęsto zaludnionych obszarach nawet z pomocą informacji dotyczących mocy sygnału adres MAC wskaże szereg mieszkań jako potencjalną lokalizację punktu dostępu. W tych okolicznościach nie można bez znacznego wysiłku dokładnie sprawdzić, kto dokładnie mieszka w mieszkaniu, w którym znajduje się punkt dostępu.

Fakt, że w niektórych przypadkach właściciela urządzenia nie można obecnie zidentyfikować bez znacznego wysiłku, nie przeszkadza w sformułowaniu ogólnego wniosku, że połączenie adresu MAC punktu dostępu WiFi z jego obliczoną lokalizacją należy traktować jako dane osobowe.

W tych okolicznościach i przy uwzględnieniu faktu, że mało prawdopodobne jest, aby administrator danych mógł rozróżnić przypadki, w których można zidentyfikować właściciela punktu dostępu WiFi, i przypadki, w których nie można go zidentyfikować, administrator danych powinien traktować wszystkie dane dotyczące routerów WiFi jako dane osobowe.

Należy przypomnieć, że przetwarzanie przedmiotowych danych geolokalizacyjnych niekoniecznie musi mieć na celu zidentyfikowanie użytkowników. Na fakt, czy zidentyfikowanie właścicieli punktów dostępu WiFi wymaga znacznego wysiłku, wpływają w znacznej mierze możliwości techniczne, jakimi dysponuje administrator danych lub inna osoba, która ma ich zidentyfikować.

5. Zobowiązania wynikające z przepisów dotyczących ochrony danych

5.1 Administrator danych

W kontekście usług geolokalizacyjnych on-line świadczonych przez służby społeczeństwa informacyjnego można wyróżnić trzy niezależne funkcje, charakteryzujące się różnymi obowiązkami w zakresie przetwarzania danych. Są to: administrator infrastruktury geolokalizacji; dostawca konkretnej aplikacji wyposażonej w funkcję geolokalizacji lub usługi geolokalizacyjnej oraz twórca systemu operacyjnego inteligentnego urządzenia przenośnego. W praktyce przedsiębiorstwa często odgrywają równocześnie wiele ról, na przykład gdy łączą system operacyjny z bazą danych z mapowanymi punktami dostępu WiFi i z platformą reklamową.

5.1.1 Administratorzy infrastruktury geolokalizacji

Podobnie jak operatorzy telekomunikacyjni, którzy przetwarzają lokalizację konkretnego urządzenia za pomocą swoich stacji bazowych, właściciele baz danych z mapowanymi punktami dostępu WiFi przetwarzają dane osobowe, kiedy obliczają lokalizację konkretnego inteligentnego urządzenia przenośnego. Ponieważ

administratorzy określają zarówno cele, jak i środki takiego przetwarzania, są administratorami danych w rozumieniu art. 2 lit d) dyrektywy o ochronie danych.

Należy podkreślić, że konkretne urządzenie jest nieodzowne przy obliczaniu jego lokalizacji, ponieważ przekazuje swoje dane dotyczące lokalizacji (często połączenie danych GPS, WiFi i pochodzących ze stacji bazowej) i niepowtarzalne numery identyfikacyjne z sąsiednich punktów dostępu WiFi do właściciela bazy danych[11]. Takie urządzenie spełnia również kryterium przewidziane w art. 4 ust. 1 lit. c) dyrektywy o ochronie danych: *środki znajdujące się na terytorium państwa członkowskiego*.

Ponieważ adres MAC punktu dostępu WiFi w połączeniu z jego obliczoną lokalizacją należy traktować jako dane osobowe, zgromadzenie tych danych również prowadzi do przetwarzania danych osobowych. Bez względu na sposób, w jaki gromadzone są te dane (jednorazowo lub bez przerwy), właściciel takiej bazy danych powinien wypełniać obowiązki zawarte w dyrektywie o ochronie danych.

5.1.2 Dostawcy aplikacji wyposażonych w funkcję geolokalizacji i usług geolokalizacyjnych

Inteligentne urządzenia przenośne umożliwiają zainstalowanie oprogramowania od osób trzecich, czyli tak zwanych *aplikacji*. Przedmiotowe aplikacje mogą przetwarzać dane dotyczące lokalizacji (i inne dane) pochodzące z inteligentnych urządzeń przenośnych, niezależnie od twórcy systemu operacyjnego lub administratorów infrastruktury geolokalizacji.

Przykłady tych usług to: prognoza pogody, która przewiduje możliwość deszczu w ciągu następnych kilu godzin w konkretnym regionie, usługa oferująca informacje dotyczące pobliskich sklepów, usługa identyfikowania zgubionego telefonu lub usługa pokazująca lokalizację znajomych.

Dostawca aplikacji będącej w stanie przetwarzać dane geolokalizacyjne jest administratorem danych w zakresie przetwarzania danych osobowych w wyniku instalacji i stosowania aplikacji.

Oczywiście nie ma potrzeby instalowania na inteligentnym urządzeniu przenośnym za każdym razem oddzielnego oprogramowania. Do wielu usług geolokalizacyjnych można uzyskać dostęp za pomocą przeglądarki. Przykładem takiej usługi jest stosowanie mapy on-line w celu oprowadzenia osoby po mieście.

5.1.3 Twórca systemu operacyjnego

Twórca systemu operacyjnego inteligentnego urządzenia przenośnego może być administratorem danych w zakresie przetwarzania danych geolokalizacyjnych, jeżeli ma bezpośredni kontakt z użytkownikiem i gromadzi dane osobowe (na przykład

[11] Urządzenie przenośne może przekazać dalej różne odebrane dane geolokalizacyjne, aby administrator mógł obliczyć jego lokalizację lub aby samo urządzenie mogło obliczyć swoją lokalizację. W obu przypadkach urządzenie stanowi podstawowe wyposażenie służące do przetwarzania danych.

żądając wstępnej rejestracji lub gromadząc informacje dotyczące lokalizacji w celu poprawy jakości usług). Jako administrator danych twórca systemu musi stosować domyślne zasady prywatności, aby zapobiec potajemnemu monitorowaniu przez samo urządzenie lub przez różne aplikacje i usługi.

Twórca systemu jest również administratorem w zakresie danych, które przetwarza, jeżeli urządzenie posiada funkcję nawiązywania połączenia z producentem (ang. *phone home*) w odniesieniu do lokalizacji tego urządzenia. W związku z tym, że twórca decyduje w tym przypadku o środkach i celach przepływu danych, jest on administratorem w zakresie przetwarzania tych danych. Często przytaczanym przykładem funkcji nawiązywania połączenia z producentem jest automatyczne dostarczanie aktualizacji strefy czasowej w oparciu o lokalizację.

Po trzecie twórca systemu jest administratorem danych, jeżeli oferuje platformę reklamową lub środowisko przypominające sklep internetowy z aplikacjami i jest w stanie przetwarzać dane osobowe wynikające z (instalacji i stosowania) aplikacji wyposażonych w funkcję geolokalizacji niezależnie od dostawców aplikacji.

5.2 Obowiązki innych stron

Istnieje wiele innych stron on-line umożliwiających (dalsze) przetwarzanie danych dotyczących lokalizacji, takich jak przeglądarki, strony portali społecznościowych lub środki przekazu, które umożliwiają na przykład geotagowanie. Jeżeli one zawierają infrastrukturę geolokalizacji w ramach swojej platformy, spoczywa na nich istotny obowiązek decydowania o domyślnych ustawieniach aplikacji (domyślne włączona („ON") lub wyłączona („OFF")). Mimo że przedmiotowe strony są administratorami danych jedynie w takim zakresie, w jakim same aktywnie przetwarzają dane osobowe, odgrywają one istotną rolę w zapewnieniu legalności przetwarzania danych przez administratorów danych, takich jak dostawcy konkretnych aplikacji, jeżeli na przykład chodzi o przejrzystość i jakość informacji dotyczących przetwarzania danych lokalizacyjnych.

5.3 Uzasadnione podstawy

5.3.1 Inteligentne urządzenia przenośne

Jeżeli operatorzy telekomunikacyjni chcą wykorzystywać dane stacji bazowej do świadczenia usług dodanych na rzecz klienta, zgodnie ze zmienioną dyrektywą o prywatności i łączności elektronicznej muszą uzyskać uprzednią zgodę klienta. Muszą również upewnić się, że klient został poinformowany o warunkach takiego przetwarzania.

Biorąc pod uwagę wrażliwość przetwarzania (schematów) danych dotyczących lokalizacji, *zgoda po uprzednim poinformowaniu* jest również główną, mającą zastosowanie podstawą uzasadnienia przetwarzania danych w przypadku przetwarzania lokalizacji inteligentnych urządzeń przenośnych w kontekście usług społeczeństwa informacyjnego.

Zgodnie z art. 2 lit. h) dyrektywy o ochronie danych zgoda musi być dobrowolnym, konkretnym i świadomym wyrażeniem przyzwolenia przez osobę, której dane dotyczą.

W zależności od zastosowanego rodzaju technologii urządzenie użytkownika odgrywa stosunkowo aktywną rolę w przetwarzaniu danych geopozycyjnych. Urządzenie może przekazywać dane dotyczące lokalizacji z różnych źródeł dowolnej osobie trzeciej. Nie należy mylić tej zdolności technicznej z legalnością takiego przetwarzania danych. Jeżeli domyślne ustawienia systemu operacyjnego pozwalają na przekazywanie danych dotyczących lokalizacji, brak interwencji ze strony jego użytkowników nie powinien być traktowany jako dobrowolne wyrażenie zgody.

W zakresie, w jakim twórcy systemów operacyjnych i innych usług społeczeństwa informacyjnego sami aktywnie przetwarzają dane geolokalizacyjne (na przykład przy uzyskiwaniu dostępu do informacji dotyczących lokalizacji z urządzenia lub za pomocą urządzenia), muszą oni wcześniej poinformować o tym swoich użytkowników i uzyskać ich zgodę. Musi być jasne, że takiej dobrowolnej zgody nie można uzyskać poprzez obowiązkową akceptację warunków ogólnych ani poprzez wprowadzenie możliwości rezygnacji. Usługi lokalizacyjne powinny być domyślnie wyłączone, a użytkownicy mogą każdorazowo wyrazić zgodę na włączenie określonych aplikacji.

Zgoda pracowników

Zgoda traktowana jako uzasadniona podstawa przetwarzania danych jest problematyczna w kontekście zatrudnienia. W opinii na temat przetwarzania danych osobowych w kontekście zatrudnienia Grupa Robocza napisała: „w przypadku, gdy wymagana jest zgoda pracownika, a niewyrażenie zgody prowadzi do rzeczywistej lub potencjalnej szkody, zgoda taka nie jest ważna pod względem spełnienia wymogów art. 7 lub 8, ponieważ nie została wyrażona dobrowolnie. Jeżeli pracownik nie ma możliwości odmowy, wówczas nie można mówić o zgodzie. (...) Trudno ocenić sytuację, w której wyrażenie zgody jest warunkiem zatrudnienia. Pracownik teoretycznie może odmówić wyrażenia zgody, ale konsekwencją takiego działania może być utrata możliwości zatrudnienia. W takim przypadku zgoda nie jest wyrażona dobrowolnie i dlatego nie jest ważna"[12]. Pracodawcy, zamiast dążyć do uzyskania zgody pracowników, muszą zastanowić się, czy rzeczywiście istnieje konieczność i uzasadniony powód kontrolowania dokładnej lokalizacji pracowników, oraz rozważyć taką konieczność w świetle podstawowych praw i wolności pracowników. W przypadkach, w których można odpowiednio uzasadnić taką konieczność, podstawę prawną przetwarzania danych może stanowić uzasadniony interes administratora danych (art. 7 lit. f) dyrektywy o ochronie danych). Pracodawca musi zawsze poszukiwać najmniej uciążliwych środków, unikać ciągłego monitorowania i na przykład wybrać system, który wysyła powiadomienie, jeśli pracownik przekroczy granice wcześniej określonej, wirtualnej strefy. Pracownik musi być w stanie wyłączyć urządzenie monitorujące poza godzinami pracy i musi otrzymać instrukcje, jak to zrobić. Urządzenia monitorowania pojazdów nie są urządzeniami monitorowania pracowników. Ich funkcją jest śledzenie lub monitorowanie lokalizacji pojazdów, w których są zainstalowane. Pracodawcy nie powinni postrzegać ich jako urządzeń do śledzenia lub monitorowania zachowania

[12] WP48, Opinia 8/2001 w sprawie przetwarzania danych osobowych w kontekście zatrudnienia.

lub miejsca pobytu kierowców lub innych pracowników, na przykład poprzez wysyłanie powiadomień o prędkości, z jaką porusza się pojazd.

Zgoda dzieci

W niektórych przypadkach zgodę w imieniu dzieci muszą wyrazić rodzice lub inni przedstawiciele prawni. Oznacza to na przykład, że dostawca aplikacji wyposażonej w funkcję geolokalizacji musi powiadomić rodziców o gromadzeniu danych geolokalizacyjnych od ich dzieci i wykorzystywaniu tych danych oraz musi uzyskać zgodę rodziców, zanim zacznie gromadzić, a następnie wykorzystywać informacje dotyczące ich dzieci. Niektóre aplikacje wyposażone w funkcję geolokalizacji zaprojektowano specjalnie na potrzeby nadzoru rodzicielskiego, na przykład poprzez ciągłe wskazywanie lokalizacji urządzenia na stronie internetowej lub wysyłanie powiadomienia w przypadku, gdy urządzenie opuszcza wcześniej określony obszar. Stosowanie takich aplikacji jest problematyczne. W opinii nr 2/2009[13] na temat ochrony danych osobowych dzieci Grupa Robocza Art. 29 napisała: „nigdy nie powinna mieć miejsca sytuacja, w której ze względów bezpieczeństwa dzieci stają się przedmiotem nadmiernego nadzoru ograniczającego ich niezależność. W związku z tym należy znaleźć równowagę między ochroną intymności i prywatności dzieci a ich bezpieczeństwem".

Zgodnie z ramami prawnymi rodzice są odpowiedzialni za zapewnienie swoim dzieciom prawa do prywatności. Jeżeli rodzice uznają, że zastosowanie takiej aplikacji jest uzasadnione w określonych okolicznościach, dzieci muszą przynajmniej zostać o tym poinformowane oraz w miarę możliwości jak najwcześniej powinny mieć możliwość udziału w podjęciu decyzji o zastosowaniu takiej aplikacji.

Zgoda musi dotyczyć konkretnie każdego z różnych celów, dla których przetwarzane są dane. Administrator danych musi dokładnie sprecyzować, czy jego usługi ograniczają się do udzielania dobrowolnej odpowiedzi na pytanie „Gdzie teraz jestem"? czy też jego celem jest uzyskanie odpowiedzi na pytania „Gdzie jesteś, gdzie byłeś(-aś) i gdzie będziesz w przyszłym tygodniu?". Innymi słowy, administrator danych musi zwrócić szczególną uwagę na zgodę w odniesieniu do celów, których nie spodziewa się osoba, której dotyczą dane, jak na przykład profilowanie lub reklama behawioralna.

Jeżeli nastąpi istotna zmiana celów przetwarzania danych, administrator danych musi ponownie uzyskać stosowną zgodę. Na przykład jeżeli firma oświadczyła, że nie będzie udostępniać danych osobowych żadnym osobom trzecim, ale teraz chciałaby udostępniać takie dane, musi uzyskać uprzednią zgodę każdego klienta. Brak odpowiedzi (lub inny scenariusz rezygnacji) nie jest wystarczający.

Ważne jest, aby odróżnić zgodę na usługę jednorazową od zgody na regularne korzystanie z usługi. Na przykład w celu korzystania z konkretnej usługi geolokalizacyjnej konieczne może być włączenie usług geolokalizacyjnych w urządzeniu lub przeglądarce. Jeżeli funkcja geolokalizacji jest włączona, każda strona internetowa może odczytać szczegóły lokalizacji użytkownika danego inteligentnego urządzenia przenośnego. Grupa Robocza Art. 29 uważa, że aby zapobiec ryzyku

[13] WP160, Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół).

ukrytego monitorowania, konieczne jest nieustanne ostrzeganie przez urządzenie, że geolokalizacja jest włączona, na przykład za pomocą stale widocznej ikony.

Grupa Robocza zaleca, aby dostawcy aplikacji wyposażonych w funkcję geolokalizacji lub usług geolokalizacyjnych po stosownym okresie ubiegali się o uzyskanie ponownej indywidualnej zgody (nawet jeśli nie nastąpiła jakakolwiek zmiana w sposobie przetwarzania danych). Na przykład niewłaściwe byłoby kontynuowanie przetwarzania danych dotyczących lokalizacji w sytuacji, gdy użytkownik nie korzystał aktywnie z usługi w ciągu ostatnich 12 miesięcy. Nawet jeśli osoba korzysta z usługi, należy co najmniej raz w roku (lub częściej, jeżeli wymaga tego charakter przetwarzania danych) przypomnieć jej o tym, w jaki sposób przetwarzane są jej dane, oraz przedstawić możliwość łatwej rezygnacji.

Osoby, których dotyczą dane, muszą mieć ponadto możliwość łatwego cofnięcia uprzednio wyrażonej zgody bez jakichkolwiek negatywnych konsekwencji dla użytkowania urządzenia. Niezależnie od europejskich dyrektyw o ochronie danych konsorcjum World Wide Web (W3C) opracowało wstępną specyfikację API geolokalizacji, w której podkreślono konieczność uzyskania uprzedniej, wyraźnej i świadomej zgody[14]. Konsorcjum W3C wyjaśnia w szczególności konieczność poszanowania wycofania zgody, doradzając podmiotom wdrażającym specyfikację, aby uznawały, że „treści dostępne pod danym adresem URL zmieniają się w taki sposób, że wcześniej udzielone zezwolenia na lokalizację nie mają już zastosowania w przypadku danego użytkownika; lub że użytkownicy mogą po prostu zmienić zdanie".

Przykład najlepszej praktyki dla dostawców aplikacji wyposażonych w funkcję geolokalizacji

Aplikacja, która chce korzystać z danych geolokalizacyjnych, wyraźnie informuje użytkownika o celu, do którego chce wykorzystać takie dane, oraz prosi o jednoznaczną zgodę na każde z różnych możliwych zastosowań. Użytkownik aktywnie wybiera poziom szczegółowości geolokalizacji (na przykład na poziomie państwa, miasta, kodu pocztowego lub maksymalną możliwą szczegółowość). Po aktywowaniu usługi lokalizacji na każdym ekranie stale widoczna jest ikona informująca o włączeniu usług lokalizacji. Użytkownik może w dowolnym momencie wycofać swoją zgodę bez konieczności opuszczania aplikacji. Użytkownik może również z łatwością i na trwałe usunąć wszelkie dane dotyczące lokalizacji przechowywane przez urządzenie.

5.3.2 Punkty dostępu WiFi

Na podstawie dyrektywy o ochronie danych przedsiębiorstwa mogą mieć uzasadniony interes w obowiązkowym gromadzeniu i przetwarzaniu adresów MAC oraz obliczaniu lokalizacji punktów dostępu WiFi w celu świadczenia usług geolokalizacyjnych.

Artykuł 7 lit. f) dyrektywy o ochronie danych, będący uzasadnioną podstawą przetwarzania danych, nakłada wymóg zachowania równowagi między

[14] Specyfikacja API geolokalizacji W3C: http://www.w3.org/TR/geolocation-API/

uzasadnionymi interesami administratora danych a podstawowymi prawami osób, których dotyczą dane. Uwzględniając częściowo statyczny charakter punktów dostępu WiFi, mapowanie punktów dostępu WiFi zasadniczo stanowi mniejsze zagrożenie dla prywatności właścicieli takich punktów dostępu niż śledzenie lokalizacji inteligentnych urządzeń przenośnych w czasie rzeczywistym.

Równowaga między prawami administratora danych a prawami osoby, której dotyczą dane, ma charakter dynamiczny. Aby uzasadnione interesy administratorów mogły z czasem z powodzeniem przeważać nad interesami osób, których dotyczą dane, administratorzy muszą opracować i wdrożyć gwarancje, takie jak prawo do łatwego i trwałego wycofania się z bazy danych bez konieczności przekazywania dodatkowych danych osobowych administratorowi takiej bazy danych. Mogą oni na przykład korzystać z oprogramowania, które automatycznie wykrywa, że dana osoba jest podłączona do konkretnego punktu dostępu[15].

Ponadto gromadzenie i przetwarzanie identyfikatorów sieci SSID nie jest konieczne do celów świadczenia usług geolokalizacyjnych. Dlatego też gromadzenie i przetwarzanie identyfikatorów SSID wykracza poza cel świadczenia usług geolokalizacyjnych opartych na mapowaniu lokalizacji punktów dostępu WiFi.

5.4 Informacje

Różni administratorzy danych muszą się upewnić, że właściciele inteligentnych urządzeń przenośnych są należycie informowani o kluczowych elementach przetwarzania danych zgodnie z art. 10 dyrektywy o ochronie danych, takich jak tożsamość administratora danych, cele przetwarzania danych, rodzaj danych, okres przetwarzania danych, prawa osób, których dotyczą dane, do wglądu do danych, poprawiania lub usuwania danych oraz prawa do cofnięcia zgody.

Ważność zgody jest nierozerwalnie związana z jakością informacji na temat usługi. Informacje muszą być jasne, wyczerpujące, zrozumiałe dla szerokiego grona odbiorców, którzy nie mają wiedzy technicznej, oraz stale i łatwo dostępne.

Informacje muszą być skierowane do szerokiego grona odbiorców. Administratorzy danych nie mogą zakładać, że ich klienci znają się na kwestiach technicznych tylko dlatego, że posiadają inteligentne urządzenie przenośne. Informacje muszą być dostosowane do wieku, jeżeli administrator wie, że dany produkt przyciąga młodzież.

---

[15] Możliwy jest następujący przypadek użycia:

1. Osoba, której dotyczą dane, wchodzi na określoną stronę internetową, na której może podać adres MAC swojego punktu dostępowego WiFi.
2. Jeżeli adres MAC pojawia się w bazie danych wraz z mapowanymi punktami dostępu WiFi, administrator danych może wyświetlić stronę weryfikacyjną zawierającą skrypt, który poprosi o podanie tablicy ARP urządzenia internetowego. Teoretycznie adresy WLAN MAC można wyświetlić za pomocą polecenia „ARP-a". Tabelę ARP można sporządzić w tle przy pomocy kodu zawartego w przeglądarce, takiego jak np. java.
3. Jeżeli adres MAC nie pojawi się w tabeli ARP, oznacza to, że użytkownik podłączony do bezprzewodowej sieci lokalnej (WLAN) jest użytkownikiem, który ma również dostęp do lokalnego adresu MAC WLAN. W ten sposób administrator danych weryfikuje żądanie usunięcia danych w sposób automatyczny i łatwy.

Jeżeli dostawcy aplikacji wyposażonych w funkcję geolokalizacji zamierzają obliczać lokalizację urządzenia więcej niż raz, muszą informować o tym swoich klientów tak długo, jak długo przetwarzają dane dotyczące lokalizacji. Muszą również umożliwić swoim klientom podtrzymanie lub wycofanie wyrażonej zgody. Aby móc osiągnąć te cele, dostawcy aplikacji powinni ściśle współpracować z twórcą systemu operacyjnego. Z technicznego punktu widzenia ma on najlepsze możliwości, jeżeli chodzi o utworzenie stale widocznej ikony przypominającej o tym, że dane dotyczące lokalizacji są przetwarzane. Twórca systemu operacyjnego ma także największe możliwości kontrolowania tego, czy nie oferuje się aplikacji, które potajemnie monitorują lokalizację inteligentnych urządzeń przenośnych.

Jeżeli twórca systemu operacyjnego wprowadził funkcję nawiązywania połączenia z producentem lub inne sposoby dostępu do danych dotyczących lokalizacji przechowywanych w urządzeniu lub w inny sposób uzyskuje dostęp do danych dotyczących lokalizacji, na przykład poprzez reklamodawców będących osobami trzecimi, musi on z wyprzedzeniem poinformować osobę, której dotyczą dane, o (szczegółowych i uzasadnionych) celach planowanego przetwarzania danych oraz o przewidywanym okresie przetwarzania danych.

Obowiązek informowania osób, których dotyczą dane, odnosi się również do administratorów baz danych z punktami dostępu WiFi objętymi geolokalizacją. Muszą oni w odpowiedni sposób podawać do wiadomości publicznej informacje o swojej tożsamości i celach przetwarzania danych oraz inne istotne informacje. Nie wystarczy sama wzmianka o możliwości pobierania danych na temat punktów dostępu WiFi w szczegółowym oświadczeniu w sprawie ochrony prywatności skierowanym do użytkowników aplikacji wyposażonej w funkcję geolokalizacji. Istnieje stosunkowo dużo środków (w trybie on-line i off-line) informowania opinii publicznej.

5.5 Prawa osób, których dotyczą dane

Osoby, których dotyczą dane, mają prawo dostępu do danych dotyczących lokalizacji pobranych przez różnych administratorów danych z ich inteligentnych urządzeń przenośnych, jak również do informacji na temat celów przetwarzania i odbiorców lub kategorii odbiorców, którym dane są ujawniane. Informacje muszą być przekazane w formacie czytelnym dla człowieka, tj. w postaci położenia geograficznego, a nie abstrakcyjnych numerów na przykład stacji bazowych.

Osoby, których dotyczą dane, mają również prawo wglądu do potencjalnych profili opartych na takich danych dotyczących lokalizacji. Jeżeli informacje dotyczące lokalizacji są przechowywane, użytkownicy powinni mieć możliwość aktualizowania, poprawiania lub usuwania takich informacji.

Grupa Robocza zaleca, aby administratorzy danych poszukiwali bezpiecznych sposobów zapewniania bezpośredniego dostępu on-line do danych dotyczących lokalizacji i potencjalnych profili. Kluczową kwestią jest, aby taki dostęp był zapewniany bez konieczności podawania dodatkowych danych osobowych w celu potwierdzenia tożsamości osób, których dotyczą dane.

5.6 Okresy przechowywania

Dostawcy usług geolokalizacyjnych i aplikacyjnych powinni określić okres przechowywania danych dotyczących lokalizacji nie dłuższy, niż jest to konieczne do celów, dla których dane były pobierane lub dla których są dalej przetwarzane. Muszą zapewnić usunięcie danych geolokalizacyjnych lub profili uzyskanych na podstawie takich danych po uzasadnionym okresie.

W przypadku, w którym gromadzenie anonimowych danych dotyczących historii lokalizacji przez twórcę systemu operacyjnego lub administratora infrastruktury geolokalizacji w celu aktualizowania lub udoskonalania świadczonych usług jest wyraźnie konieczne, należy dołożyć wszelkich starań, aby nie umożliwić (pośredniej) identyfikacji tych danych. W szczególności nawet jeżeli urządzenie przenośne jest identyfikowane za pomocą losowo przypisywanego niepowtarzalnego numeru identyfikacyjnego urządzenia (UDID), taki niepowtarzalny numer powinien być przechowywany wyłącznie do celów operacyjnych przez maksymalnie 24 godziny. Po tym okresie taki identyfikator UDID należy dodatkowo zanonimizować, biorąc pod uwagę fakt, że coraz trudniej osiągnąć rzeczywistą anonimizację oraz że połączone dane dotyczące lokalizacji w dalszym ciągu mogą prowadzić do identyfikacji. Nie powinno być możliwe powiązanie takiego UDID z wcześniejszymi lub późniejszymi UDID przypisanymi urządzeniu ani z jakimikolwiek stałymi identyfikatorami użytkownika lub telefonu (takimi jak adres MAC, numer IMEI lub IMSI lub jakimikolwiek innymi numerami konta).

Jeżeli chodzi o dane na temat punktów dostępu WiFi, po powiązaniu adresu MAC danego punktu dostępu WiFi z nową lokalizacją na podstawie ciągłych obserwacji właścicieli inteligentnych urządzeń przenośnych należy natychmiast usunąć wcześniejszą lokalizację, aby zapobiec jakiemukolwiek dalszemu wykorzystywaniu danych do niewłaściwych celów, takich jak marketing skierowany do osób, które zmieniły swoją lokalizację.

6. Wnioski

Przy pomocy technologii geolokalizacji, takich jak dane stacji bazowej, GPS i mapowane punkty dostępu WiFi, różnego rodzaju administratorzy danych mogą śledzić inteligentne urządzenia przenośne w różnych celach począwszy od reklamy behawioralnej po monitorowanie dzieci.

Ponieważ smartfony i komputery typu tablet są nierozerwalnie powiązane ze swoim właścicielem, schematy przemieszczania się tych urządzeń zapewniają bardzo dokładny wgląd w życie prywatne właścicieli. Jednym z największych zagrożeń jest fakt, że właściciele nie są świadomi tego, że przekazują informacje o swojej lokalizacji, ani tego, komu przekazują te informacje. Kolejne zagrożenie wiąże się z tym, że wyrażona zgoda na wykorzystywanie danych dotyczących lokalizacji przez niektóre aplikacje jest nieważna, ponieważ informacje na temat kluczowych elementów przetwarzania są niezrozumiałe, nieaktualne lub niewłaściwe z innych względów.

Różne obowiązki spoczywają na różnych zainteresowanych stronach, do których należą twórcy systemów operacyjnych, dostawcy aplikacji i osoby trzecie, takie jak

strony portali społecznościowych, które na swoich platformach mają wbudowane funkcje lokalizacji urządzeń przenośnych.

6.1 Ramy prawne

- Ramy prawne UE dla wykorzystywania danych geolokalizacyjnych z inteligentnych urządzeń przenośnych stanowi przede wszystkim dyrektywa o ochronie danych. Dane dotyczące lokalizacji, pochodzące z inteligentnych urządzeń przenośnych, są danymi osobowymi. Połączenie niepowtarzalnego adresu MAC i obliczonej lokalizacji punktu dostępu WiFi należy traktować jako dane osobowe.
- Co więcej, zmieniona dyrektywa o prywatności i łączności elektronicznej 2002/58/WE ma zastosowanie wyłącznie do przetwarzania danych stacji bazowej przez operatorów telekomunikacyjnych.

6.2 Administratorzy danych

- Można wyróżnić trzy rodzaje administratorów danych, tj. administratorów infrastruktury geolokalizacji (w szczególności administratorów mapowanych punktów dostępu WiFi); dostawców aplikacji wykorzystujących funkcję geolokalizacji i usług geolokalizacyjnych oraz twórców systemu operacyjnego inteligentnych urządzeń przenośnych.

6.3 Uzasadnione podstawy

- Ponieważ dane dotyczące lokalizacji, pochodzące z inteligentnych urządzeń przenośnych, ujawniają szczegółowe informacje osobiste na temat życia prywatnego właścicieli takich urządzeń, główną uzasadnioną podstawą do przetwarzania takich danych jest uprzednia świadoma zgoda.
- Zgoda nie może być uzyskana poprzez akceptację warunków ogólnych.
- Zgoda musi dotyczyć konkretnie każdego z różnych celów, dla których przetwarza się dane, w tym na przykład profilowania lub reklamy behawioralnej stosowanych przez administratora danych. Jeżeli nastąpi istotna zmiana celów przetwarzania danych, administrator danych musi ponownie uzyskać stosowną zgodę.
- Domyślnie usługi lokalizacji muszą być wyłączone. Ewentualny mechanizm rezygnacji nie stanowi odpowiedniego mechanizmu uzyskiwania świadomej zgody użytkownika.
- Zgoda jest problematyczna w odniesieniu do pracowników i dzieci. W przypadku pracowników pracodawcy mogą stosować tę technologię wyłącznie, jeśli jest to wyraźnie konieczne do osiągnięcia uzasadnionego celu, zaś takich samych celów nie można osiągnąć za pomocą mniej niepożądanych środków. W przypadku dzieci rodzice muszą ocenić, czy zastosowanie takiej aplikacji jest uzasadnione w szczególnych okolicznościach. Muszą oni przynajmniej poinformować o tym dzieci oraz w miarę możliwości jak najwcześniej umożliwić im udział w podjęciu decyzji o zastosowaniu takiej aplikacji.
- Grupa Robocza zaleca ograniczenie zakresu zgody pod względem czasowym oraz przypominanie użytkownikom o wyrażeniu takiej zgody co najmniej raz w roku. Grupa Robocza zaleca również, aby zgoda była dostatecznie szczegółowa w odniesieniu do precyzji danych dotyczących lokalizacji.

- Osoby, których dotyczą dane, muszą mieć możliwość łatwego cofnięcia uprzednio wyrażonej zgody bez jakichkolwiek negatywnych konsekwencji dla możliwości użytkowania urządzenia.
- W odniesieniu do mapowania punktów dostępu WiFi przedsiębiorstwa mogą mieć uzasadniony interes w obowiązkowym gromadzeniu i przetwarzaniu adresów MAC oraz obliczaniu lokalizacji punktów dostępu WiFi w celu świadczenia usług geolokalizacyjnych. Aby zachować równowagę między prawami administratora danych a prawami osoby, której dotyczą dane, administrator danych musi umożliwić łatwe i trwałe wycofanie się z bazy danych bez konieczności podawania dodatkowych danych osobowych.

6.4 Informacje

- Informacje muszą być jasne, wyczerpujące, zrozumiałe dla szerokiego grona odbiorców, które nie ma wiedzy technicznej, oraz stale i łatwo dostępne. Ważność zgody jest nierozerwalnie związana z jakością informacji na temat usługi.
- Strony trzecie, takie jak przeglądarki i strony portali społecznościowych, pełnią kluczową rolę w zakresie widoczności i jakości informacji na temat przetwarzania danych geolokalizacyjnych.

6.5 Prawa osób, których dotyczą dane

- Administratorzy informacji geolokalizacyjnych z urządzeń przenośnych powinni umożliwiać swoim klientom dostęp do ich danych dotyczących lokalizacji w formacie czytelnym dla człowieka oraz pozwalać na poprawianie i usuwanie niepotrzebnych danych osobowych.
- Osoby, których dotyczą dane, mają również prawo dostępu do możliwych profili opartych na takich danych dotyczących lokalizacji, ich poprawiania i usuwania.
- Grupa Robocza zaleca ustanowienie (bezpiecznego) dostępu on-line.

6.6 Okresy przechowywania

- Dostawcy aplikacji wykorzystujących funkcję geolokalizacji lub usług geolokalizacyjnych powinni wdrażać politykę przechowywania, która zapewnia usuwanie danych geolokalizacyjnych lub profili otrzymanych na podstawie takich danych po uzasadnionym okresie.
- Jeżeli twórca systemu operacyjnego lub administrator infrastruktury geolokalizacji przetwarza niepowtarzalny numer, taki jak adres MAC lub identyfikator UDID w odniesieniu do danych dotyczących lokalizacji, niepowtarzalny numer identyfikacyjny może być przechowywany wyłącznie do celów operacyjnych przez maksymalnie 24 godziny.

Sporządzono w Brukseli
dnia 16 maja 2011 r.

W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM