Żadnej prywatności, żadnej własności czyli świat w 2030r.

Światowe Forum Ekonomiczne (WEF) zostało założone pięćdziesiąt lat temu. Przez dziesięciolecia zyskiwało coraz większe znaczenie i stawało się jedną z wiodących platform futurystycznego myślenia i planowania. Jako miejsce spotkań światowych elit, WEF zrzesza liderów biznesu i polityki oraz kilku wybranych intelektualistów. Główną ideą forum jest globalna kontrola. Wolny rynek i indywidualny wybór nie są tu najważniejszymi wartościami, ale państwowy interwencjonizm i kolektywizm. Wolność indywidualna i własność prywatna mają zniknąć z tej planety do 2030 roku, zgodnie z prognozami i scenariuszami Światowego Forum Ekonomicznego.

Osiem prognoz

Wolność jednostki znów jest zagrożona. To, co może nas czekać, przewidywano w listopadzie 2016r., kiedy WEF opublikowało **„8 prognoz dla świata na rok 2030”**. Według scenariusza WEF świat stanie się zupełnie innym miejscem niż obecnie, ponieważ sposób, w jaki ludzie pracują i żyją, ulegnie głębokiej przemianie. Scenariusz dla świata w roku 2030 to coś więcej niż tylko prognoza. Jest to plan, którego realizacja drastycznie przyspieszyła od czasu ogłoszenia pandemii i wynikających z niej obostrzeń.

Według prognoz „Global Future Councils” z WEF, własność

prywatna i prywatność zostaną zniesione w ciągu następnej dekady. Nadchodzące wywłaszczenie pójdzie nawet dalej niż komunistyczne żądanie zniesienia własności środków produkcji i pozostawienia miejsca na własność prywatną. Projekcja WEF mówi, że również dobra konsumpcyjne nie będą już własnością prywatną.

Gdyby prognoza WEF spełniła się, ludzie musieliby wynajmować i pożyczać swoje artykuły pierwszej potrzeby od państwa, które byłoby wyłącznym właścicielem wszystkich towarów. Dostawy towarów byłyby reglamentowane zgodnie z punktami systemu zaufania społecznego [social credit system]. Zakupy w tradycyjnym rozumieniu znikną wraz z prywatnymi zakupami towarów. Każdy osobisty ruch byłby śledzony elektronicznie, a cała produkcja podlegałaby wymogom czystej energii i zrównoważonego środowiska.

Aby osiągnąć „zrównoważone rolnictwo”, podaż żywności będzie głównie wegetariańska. W nowej totalitarnej gospodarce usługowej rząd zapewni podstawowe zakwaterowanie, żywność i transport, resztę zaś trzeba pożyczyć od państwa. Wykorzystanie zasobów naturalnych zostanie ograniczone do minimum. We współpracy z kilkoma kluczowymi krajami światowa agencja ustaliłaby cenę emisji CO2 na niezwykle wysokim poziomie, aby zniechęcić do jego stosowania.

W filmie promocyjnym Światowe Forum Ekonomiczne podsumowuje te osiem prognoz w następujących stwierdzeniach:

1. Ludzie nie będą posiadać niczego. Towary są albo bezpłatne, albo muszą zostać pożyczone od państwa.

   –

2. Stany Zjednoczone nie będą już wiodącym supermocarstwem, ale dominować będzie kilka krajów.

   –

3. Narządy nie będą przeszczepiane, ale drukowane.

   –

4. Spożycie mięsa zostanie zminimalizowane.

   –

5. Nastąpią masowe przesiedlenia ludzi wraz z miliardami uchodźców.

   –

6. Aby ograniczyć emisję dwutlenku węgla, światowa cena zostanie ustalona na przesadnym poziomie.

   –

7. Ludzie będą mogli przygotowywać się do wyprawy na Marsa i rozpoczęcia podróży w poszukiwaniu obcego życia.

   –

8. Zachodnie wartości zostaną przetestowane do granic wytrzymałości.

Poza prywatność i własność

W publikacji dla Światowego Forum Ekonomicznego duńska ekoaktywistka Ida Auken, która w latach 2011–2014 pełniła funkcję ministra środowiska swojego kraju i nadal jest posłanką do duńskiego parlamentu (Folketing), opracowała scenariusz dla świata bez prywatności i własności. W „Witamy w roku 2030” wyobraża sobie świat, w którym „nie posiadam nic, nie mam prywatności i życie nigdy nie było lepsze”. Według jej scenariusza do 2030r. zakupy i posiadanie staną się przestarzałe, ponieważ wszystko, co kiedyś było produktem, będzie teraz usługą.

W tym jej idyllicznym nowym świecie ludzie mają swobodny dostęp do transportu, zakwaterowania, jedzenia i „wszystkich rzeczy, których potrzebujemy w życiu codziennym”. Ponieważ te rzeczy staną się bezpłatne, „w końcu posiadanie zbyt wielu rzeczy nie miało sensu”. Nie byłoby prywatnej własności domów i nikt nie płaciłby czynszu, „ponieważ ktoś inny korzysta z naszej wolnej przestrzeni, kiedy tylko my jej nie potrzebujemy”. Na przykład salon [pokój dzienny] będzie używany do spotkań biznesowych, gdy ktoś będzie nieobecny.

Obawy takie jak „choroby cywilizacyjne, zmiany klimatyczne, kryzys uchodźczy, degradacja środowiska, całkowite zakorkowanie miast, zanieczyszczenie wody i powietrza, niepokoje społeczne i bezrobocie” będą należeć już do przeszłości. Autorka przewiduje, że ludzie będą szczęśliwi, mogąc cieszyć się tak dobrym życiem, które jest o wiele lepsze „niż droga, którą podążaliśmy, gdzie stało się tak jasne, że nie możemy kontynuować tego samego modelu rozwoju”.

Ekologiczny raj

W swoim wystąpieniu w 2019r. na dorocznym spotkaniu Global Future Councils Światowego Forum Ekonomicznego Ida Auken przepowiadała, jak świat może wyglądać w przyszłości, „jeśli wygramy wojnę ze zmianami klimatycznymi”. Do 2030r., kiedy emisja CO2 zostanie znacznie zmniejszona, ludzie będą żyć w świecie, w którym mięso na talerzu „będzie rzadkim widokiem”, a woda i powietrze będą znacznie czystsze niż obecnie. W wyniku przejścia od kupowania towarów do korzystania z usług zniknie potrzeba posiadania pieniędzy, ponieważ ludzie będą wydawać coraz mniej na towary. Czas pracy będzie się skracał, a przybywać będzie czasu wolnego.

Auken widzi w przyszłości miasto, w którym samochody elektryczne zastąpią konwencjonalne pojazdy spalinowe. Większość dróg i miejsc parkingowych stanie się zielonymi parkami i strefami spacerowymi dla pieszych. Do 2030r. rolnictwo zamiast mięsa i nabiału będzie oferować głównie roślinne alternatywy dla żywności. Wykorzystanie gruntów do produkcji paszy dla zwierząt znacznie się zmniejszy, a przyroda ponownie rozprzestrzeni się na całym świecie.

Fabrykowanie zgody społecznej

Jak przekonać ludzi do zaakceptowania takiego systemu? Przynętą mającą zwabić masy są zapewnienia kompleksowej opieki zdrowotnej i gwarantowanego dochodu podstawowego. Promotorzy

Wielkiego Resetu obiecują świat bez chorób. Mówi się, że dzięki biotechnologicznie produkowanym narządom i zindywidualizowanym zabiegom medycznym opartym na genetyce możliwe jest radykalne wydłużenie średniej długości życia, a nawet nieśmiertelność. Sztuczna inteligencja wyeliminuje śmierć oraz wyeliminuje choroby i śmiertelność. Wśród firm biotechnologicznych trwa wyścig o znalezienie klucza do życia wiecznego.

Oprócz obietnicy przekształcenia każdego zwykłego człowieka w podobnego do boga nadczłowieka, obietnica „powszechnego dochodu podstawowego" jest bardzo atrakcyjna, szczególnie dla tych, którzy nie znajdą już pracy w nowej gospodarce cyfrowej. Uzyskanie dochodu podstawowego bez konieczności przechodzenia przez kierat i hańbę ubiegania się o pomoc społeczną jest wykorzystywane jako przynęta, aby uzyskać wsparcie biednych.

Koniecznie obejrzyj ten film:
Uwaga: Stany Zjednoczone stoją w obliczu NAJWIĘKSZEGO zagrożenia stulecia. Wojna jest tuż za rogiem. Zaraz stracisz wszystko, na co tak ciężko pracowałeś przez całe życie i nawet nie będzie to twoja wina! – twój dom, twój samochód, Twoja karta kredytowa będą bezwartościowe… LINK

Aby było to ekonomicznie opłacalne, zapewnienie dochodu podstawowego wymagałoby wyrównywania różnic płacowych. Techniczne procedury przekazu pieniędzy od państwa zostaną wykorzystane do promowania społeczeństwa bezgotówkowego. Wraz z cyfryzacją wszystkich transakcji pieniężnych każdy indywidualny zakup będzie rejestrowany. W konsekwencji władze rządowe miałyby nieograniczony dostęp do szczegółowego nadzoru nad tym, jak poszczególne osoby wydają swoje pieniądze. Uniwersalny dochód podstawowy w społeczeństwie bezgotówkowym zapewniłby warunki do narzucenia systemu kredytu społecznego i zapewniłby mechanizm sankcjonowania niepożądanych zachowań oraz identyfikacji tego, co zbędne i niepożądane.

Kto będzie władcą?

Światowe Forum Ekonomiczne milczy na temat tego, kto będzie rządził w tym nowym świecie.

Nie ma powodu oczekiwać, że nowi posiadacze władzy będą życzliwi. Jednak nawet gdyby czołowi decydenci nowego rządu światowego nie byli podli, ale byli po prostu technokratami, jaki powód miałaby administracyjna technokracja by przejmować się niepożądanymi? Jaki sens dla technokratycznej elity ma przekształcanie zwykłego człowieka w nadczłowieka? Po co dzielić się korzyściami płynącymi ze sztucznej inteligencji z masami, a nie zatrzymać bogactwa dla nielicznych?

Nie dając się zwieść utopijnym obietnicom, po trzeźwej ocenie planów musimy dojść do wniosku, że w tym nowym świecie nie będzie miejsca dla przeciętnego człowieka i zostanie on odsunięty razem z *„niezatrudnialnymi”* [unemployable] – „słabymi umysłowo” i „źle wychowanymi”. Za głoszeniem postępowej ewangelii sprawiedliwości społecznej przez promotorów Wielkiego Resetu i ustanowieniem nowego porządku świata kryje się złowrogi projekt eugeniki, który w sensie metody nazywa się obecnie „inżynierią genetyczną”, a jako ruch „transhumanizmem” – termin ukuty przez Juliana Huxleya, pierwszego dyrektora UNESCO.

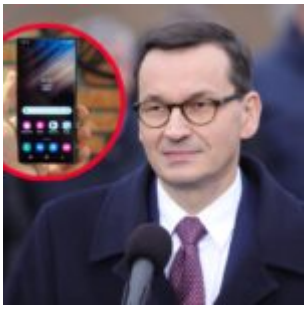
Promotorzy projektu milczą na temat tego, kto będzie władcą w tym nowym świecie. Dystopijny i kolektywistyczny charakter tych projekcji i planów jest wynikiem odrzucenia wolnego kapitalizmu. Tworzenie lepszego świata poprzez dyktaturę jest sprzecznością samą w sobie. Odpowiedzią na obecne problemy nie jest mniejszy, ale większy dobrobyt gospodarczy. Dlatego potrzebujemy więcej wolnego rynku i mniej planowania państwowego. Świat staje się coraz bardziej ekologiczny [greener] i obserwuje się już spadek tempa wzrostu światowej populacji. Tendencje te są naturalną konsekwencją tworzenia bogactwa poprzez wolne rynki.

Wniosek

Światowe Forum Ekonomiczne i powiązane z nim instytucje w połączeniu z kilkoma rządami i kilkoma firmami z branży zaawansowanych technologii chcą wprowadzić świat w nową erę bez własności i prywatności. Stawką są wartości takie jak indywidualizm, wolność i dążenie do szczęścia, które należy odrzucić na rzecz kolektywizmu i narzucenia „dobra wspólnego", które zdefiniuje samozwańcza elita technokratów. To, co jest sprzedawane społeczeństwu jako obietnica równości i zrównoważonego rozwoju ekologicznego, jest w rzeczywistości brutalnym atakiem na ludzką godność i wolność. Zamiast wykorzystywać nowe technologie jako narzędzie doskonalenia, Wielki Reset stara się wykorzystać możliwości technologiczne jako narzędzie zniewolenia. W tym nowym porządku świata państwo jest jedynym właścicielem wszystkiego. Od naszej wyobraźni zależy, kto zaprogramuje algorytmy zarządzające dystrybucją towarów i usług.

Źródło

Rząd prześwietli smartfony Polaków. Klamka zapadła



Idą zmiany w prawie komunikacji elektronicznej. Dadzą one służbom specjalnym większe możliwości inwigilowania Polaków

poprzez zbieranie najróżniejszych danych o nich.

Rząd dał zielone światło zmianom w **prawie komunikacji elektronicznej**. Dzięki nim służby specjalne otrzymają nie tylko dostęp do danych lokalizacyjnych smartfonów czy billingów, ale również – jak informuje dziennik.pl – do **treści przesyłanych e-maili** czy **zapisów rozmów na komunikatorach**.

Innymi słowy, do przesyłania danych o nas do służb będą zobowiązane nie tylko **firmy telekomunikacyjne**, ale także **dostawcy poczty elektronicznej oraz innych usług internetowych**. Rząd za pomocą nowego prawa chce pozyskiwać dane, które pozwolą na **jednoznaczną identyfikację użytkownika w sieci**.

Jeśli zamierzasz zapytać, **czy nowe przepisy będą zgodne z prawem Unii Europejskiej**, to spieszymy z odpowiedzią. **Oczywiście, że nie będą**. Co więcej, jak podaje **Dziennik Gazeta Prawna**, rząd doskonale zdaje sobie z tego sprawę. Podsekretarz stanu w Kancelarii Prezesa Rady Ministrów (KPRM) napisał w opinii do projektu nowych regulacji, że ***pogłębia on zakres niezgodności przepisów z prawem UE***. To jednak prawdopodobnie niczego nie zmienia w ocenie autorów nowego prawa.

Źródło

Prawie wszystkie rządowe witryny informacyjne

dotyczące COVID są tajnymi operacjami SZPIEGOWSKIMI

Europejscy naukowcy opracowali badanie ujawniające, że rządowe witryny informacyjne dotyczące (COVID-19 są koszmarem naruszającym prywatność – *niech opinia publiczna się strzeże*!

Dokument zatytułowany „Pomiar plików cookie w witrynach rządowych", finansowany przez Europejską Radę ds. Badań Naukowych (ERC), Unię Europejską (UE) i rząd hiszpański, wyjaśnia, że witryny rządowe są zasadniczo wykorzystywane jako „pojedynczy punkt" monitorowania i śledzenia całej populacji kraju" za pomocą plików cookie.

Badacze przyjrzeli się trzem różnym rodzajom stron internetowych, w tym oficjalnym rządowym stronom internetowym krajów „G20" na całym świecie; strony internetowe organizacji międzynarodowych, takich jak ONZ; oraz popularne strony internetowe wykorzystywane przez społeczeństwo do śledzenia i informacji o Grypie Fauciego. Przyjrzeli się wykorzystaniu plików cookie w każdej witrynie i doszli do wniosku, że ponad 90 procent witryn rządowych „tworzy pliki cookie zewnętrznych modułów śledzących bez zgody użytkowników".

„Ciasteczka internetowe były wykorzystywane do zbierania informacji o aktywnościach i zainteresowaniach użytkowników w Internecie" – wyjaśnia gazeta.

„Niesesyjne pliki cookie, które są tworzone przez moduły śledzące i mogą trwać przez kilka dni lub miesięcy, są powszechnie obecne nawet w krajach, w których obowiązują

surowe przepisy dotyczące prywatności użytkowników. Pokazujemy również, że powyższe jest problemem dla oficjalnych stron internetowych organizacji międzynarodowych oraz popularnych serwisów, które informują opinię publiczną o pandemii COVID-19”.

Oto wskazówka: w pierwszej kolejności nie odwiedzaj żadnych rządowych witryn COVID, a nie będziesz śledzony

Innymi słowy, największe gospodarki świata angażują się w nieujawnione i potencjalnie nielegalne programy szpiegowskie i inwigilacyjne za pośrednictwem oficjalnych rządowych stron internetowych, z których społeczeństwo korzysta, aby dowiedzieć się o COVID i angażować się w inne formy konsumpcji propagandy.

Spośród 5550 rządowych witryn internetowych i ponad 118 000 adresów URL administrowanych przez rządy ponad 50 procent ich plików cookie należy do stron trzecich, podczas gdy od 10 do 90 procent pochodzi od znanych trackerów.

„Większość z tych ciasteczek ma żywotność dłużej niż jeden dzień, a wiele z nich wygasa rok lub dłużej” – ujawnia badanie.

Około 60 procent witryn rządowych używa co najmniej jednego pliku cookie stron trzecich, a 95 procent lub prawie *wszystkie* tworzy pliki cookie bez zgody użytkownika. Nawiasem mówiąc, pliki cookie stron trzecich są „znane z tego, że śledzą użytkowników w celu gromadzenia danych”, wyjaśnia badanie.

Rządowe strony internetowe dotyczące chińskiego wirusa są najgorszymi przestępcami, ponieważ 99 procent zawiera ukryte

pliki cookie, które zostały tam umieszczone bez zgody użytkownika.

„Na przykład bardzo popularna strona internetowa z globalnymi mapami dotyczącymi przypadków COVID-19, prowadzona przez *Johns Hopkins University*, dodaje pliki cookie z 7 trackerów" – czytamy dalej.

„Wszystkie pozostałe witryny Top 10 to oficjalne krajowe witryny informacyjne w krajach europejskich, które mają co najmniej trzy trackery. Amerykańskie Centra Kontroli i Zapobiegania Chorobom (CDC) również znajdują się w pierwszej dziesiątce, z plikami cookie powiązanymi z trzema trackerami".

Kiedyś tego typu rzeczy miały miejsce tylko w krajach jawnie komunistycznych, takich jak Chiny, które przodują w totalitaryzmie. Jednak ostatnio Stany Zjednoczone i inne mocarstwa zachodnie wydają się naśladować model Komunistycznej Partii Chin, narzucając w swoich krajach systemy typu „społecznej oceny kredytowej".

Grypa Fauciego szybko stała się powszechnym pretekstem do naruszania prywatności ludzi, wymuszania pewnych restrykcyjnych zachowań, a nawet popełniania gwałtu medycznego w formie obowiązkowego maskowania i „szczepienia".

Okazuje się, że nawet w sieci rząd łamie prawa ludzi i śledzi ich zachowanie bez pozwolenia. Pełny zakres powodów, dla których rząd chce śledzić zachowanie ludzi w Internecie, jeszcze nie został ujawniony.

Jak zadbać o swoją prywatność, używając Androida

Jak bardzo trzeba się postarać, by ograniczyć ilość danych zbieranych przez producentów urządzeń z Androidem i firmę Google, która regularnie wydaje nowe wersje systemu? Pokazujemy krok po kroku, co trzeba zrobić, by zapewnić sobie więcej prywatności.

Twórcy Androida umieścili „Menedżera uprawnień” wśród ustawień mających wpływ na prywatność i rzeczywiście, szafując uprawnieniami na prawo i lewo, możemy nieopatrznie dać aplikacjom zbyt szeroki dostęp do naszych danych, tracąc tym samym część prywatności. Jak temu zaradzić, opisywaliśmy w jednym z wcześniejszych artykułów, w tym skupimy się więc na innych opcjach, które warto wziąć pod uwagę. Jak je skonfigurować, omówimy na przykładzie Galaxy M21 od Samsunga, działającego pod kontrolą Androida 11 z interfejsem One UI 3.1. Sprawdzimy też, co dodano w Androidzie 12 z One UI 4.1. Układ ustawień w telefonach z inną wersją systemu bądź nakładką innego producenta może odbiegać od tego, który pokazujemy, wiele opcji będzie jednak podobnych.

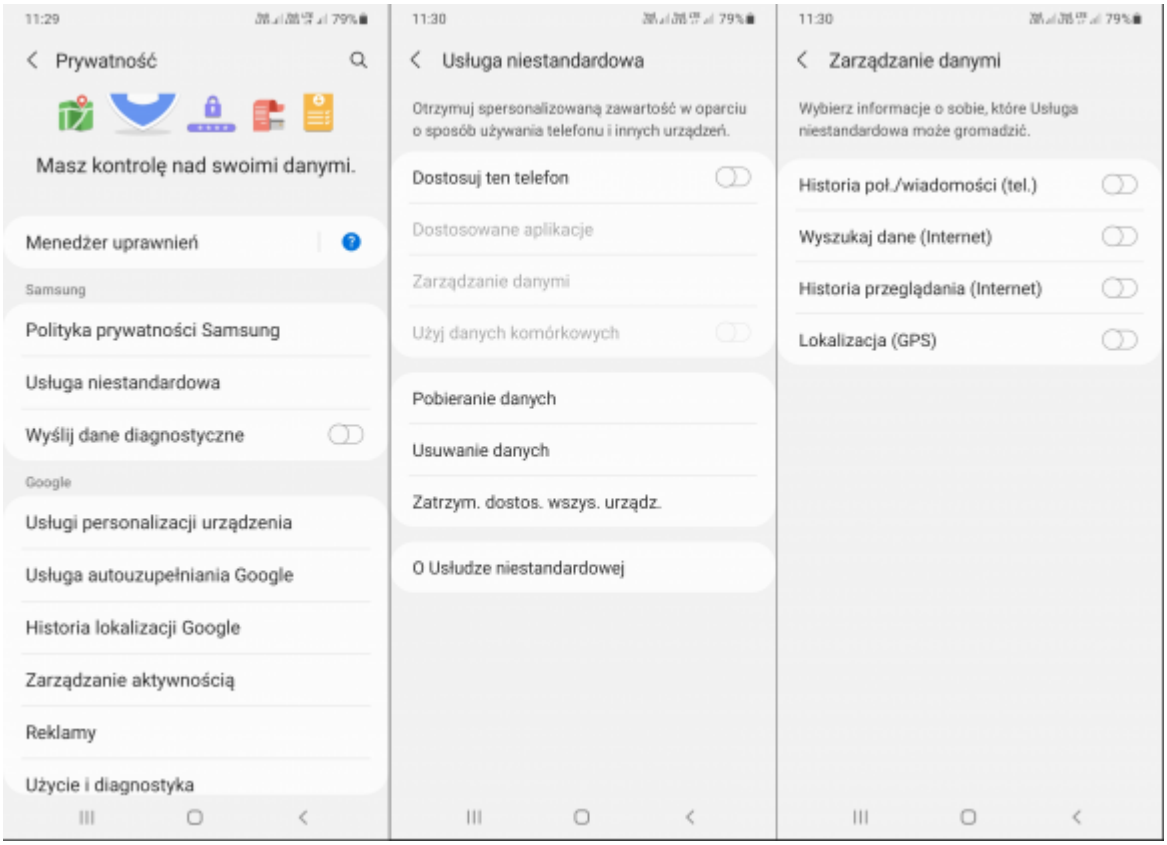
Jakie dane zbiera Samsung i co z tym zrobić

W polityce prywatności Samsung przyznaje, że „gromadzi informacje osobiste Użytkownika różnymi sposobami”. Interesują go zarówno dane przekazywane bezpośrednio, np. podczas

zakładania konta, zakupu którejś z płatnych usług czy kontaktu z obsługą klienta, jak i zbierane przez firmowe aplikacje, gdy korzystamy z naszego telefonu. W tym drugim przypadku chodzi nie tylko o podstawowe informacje o urządzeniu (jak model, IMEI, MAC, wersja systemu operacyjnego, numer telefonu czy adres IP), ale też o pliki cookie, dane pochodzące z logów, historię obejrzanych treści, nagrania naszego głosu (jeśli stosujemy polecenia głosowe), słowa wpisywane za pomocą klawiatury (gdy włączymy funkcję podpowiadania tekstu), informacje o lokalizacji itp. Jakby tego było mało, Samsung zbiera dane „dostępne publicznie lub za opłatą", np. pochodzące z mediów społecznościowych – są one następnie łączone z innymi informacjami o użytkowniku danego smartfona. Firma nie stroni też od usług analitycznych zewnętrznych dostawców, jak Google Analytics.

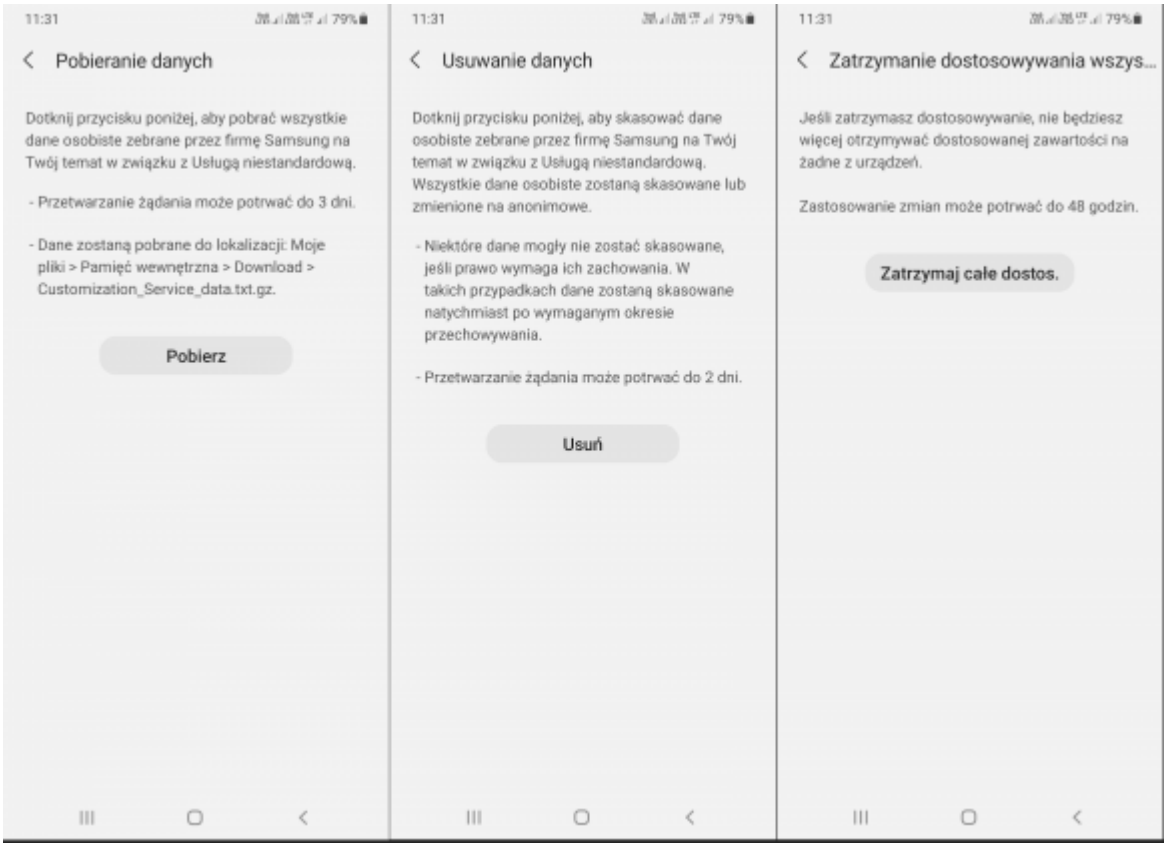
Zgromadzone dane mogą być przekazywane licznym podmiotom, m.in. partnerom biznesowym Samsunga i współpracującym z nim usługodawcom, którzy dokonują napraw, przygotowują spersonalizowane reklamy itp. Informacje o konkretnych użytkownikach mogą być ujawniane „gdy wymaga tego prawo lub gdy jest to niezbędne do ochrony usług firmy Samsung", jak również „na potrzeby organów ścigania, bezpieczeństwa narodowego, walki z terroryzmem lub innych kwestii związanych z bezpieczeństwem publicznym". W polityce prywatności możemy przeczytać, że firma przechowuje dane użytkowników „Wyłącznie przez czas wymagany w celu, w jakim takie informacje zostały zgromadzone lub są przetwarzane, lub dłużej, jeśli wymaga tego jakakolwiek umowa, obowiązujące prawo, bądź w celach statystycznych, z zachowaniem odpowiednich zabezpieczeń". Innymi słowy – nie wiadomo, jak długo i choćby z tego względu warto ograniczyć ilość przekazywanych Samsungowi danych. Dlatego sugerujemy np. nie używać dostarczanej wraz systemem przeglądarki, sugestywnie podpisanej jako „Internet" – lepszy będzie nawet Google Chrome (po włączeniu w ustawieniach „Piaskownicy prywatności"), ale można też pokusić się o zainstalowanie mobilnej wersji Firefoksa albo DuckDuckGo. Nie

zaszkodzi też poszukać alternatywnych rozwiązań dla pozostałych narzędzi oferowanych przez producenta.



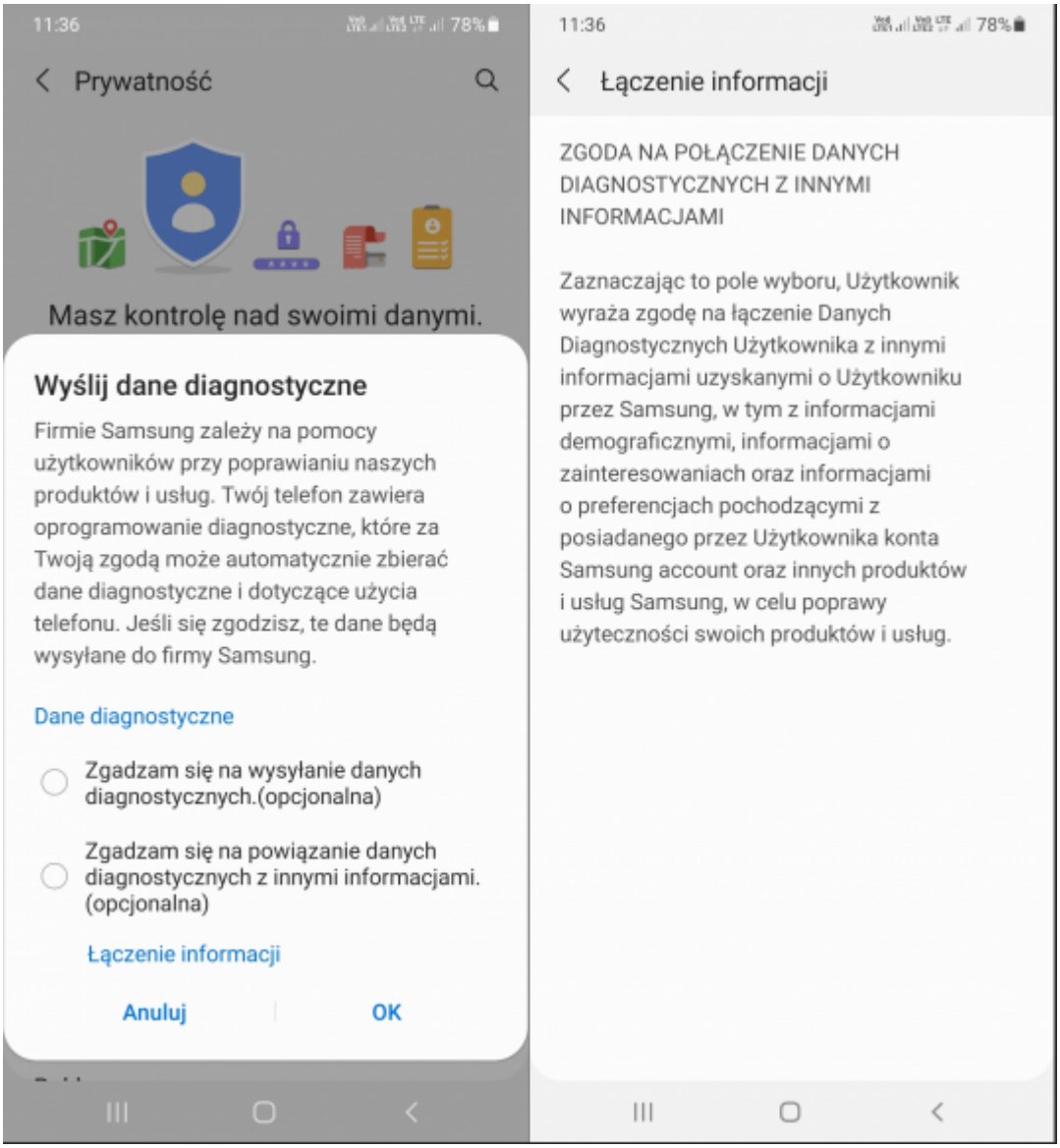
„Usługa niestandardowa” oferowana przez Samsunga

Po wejściu do ustawień telefonu w zakładce „Prywatność” znajdziemy ponadto pozycję „Usługa niestandardowa”, która odpowiada za dostarczanie reklam i innych treści w oparciu o nasze (rzekome) zainteresowania i odwiedzane przez nas miejsca w świecie rzeczywistym. Można ją skonfigurować po zalogowaniu się na założone wcześniej konto w usługach Samsunga. Jeśli opcja „Dostosuj ten telefon” zostanie aktywowana, to w sekcji „Zarządzanie danymi” będziemy mogli określić, czy usługa ma mieć dostęp do naszych połączeń i wiadomości, historii wyszukiwania i przeglądania oraz lokalizacji (ale nie są to jedyne zbierane przez nią informacje, o czym się przekonamy, zaglądając do odrębnej polityki prywatności). W sekcji „Dostosowane aplikacje” możemy z kolei wskazać, które z systemowych aplikacji będą z gromadzonych danych korzystać. Nasza rada? W ogóle tej usługi nie włączać.



Ujarzmianie „Usługi niestandardowej”

Jeśli nieopatrznie zrobiliśmy to wcześniej, możemy skorzystać z opcji „Pobieranie danych” i sprawdzić, czego dowiedział się o nas Samsung. Firma uprzedza, że przetwarzanie żądania może jej zająć nawet 3 dni, a interesujące nas informacje zostaną zapisane w folderze „Download” pod postacią pliku *Customization_Service_data.txt.gz*. Za pomocą opcji „Zatrzym. dostos. wszys. urządz.” możemy zrezygnować z otrzymywania spersonalizowanych treści, nie nastąpi to jednak od razu – zastosowanie zmian może potrwać do 2 dni. Podobnie mają się sprawy z usuwaniem gromadzonych przez usługę danych. Co gorsza, nie wszystkie zostaną skasowane z uwagi na bliżej nieokreślone wymogi prawne, o czym zostaniemy poinformowani przed naciśnięciem przycisku „Usuń”.



Zgoda na wysyłanie do Samsunga danych diagnostycznych

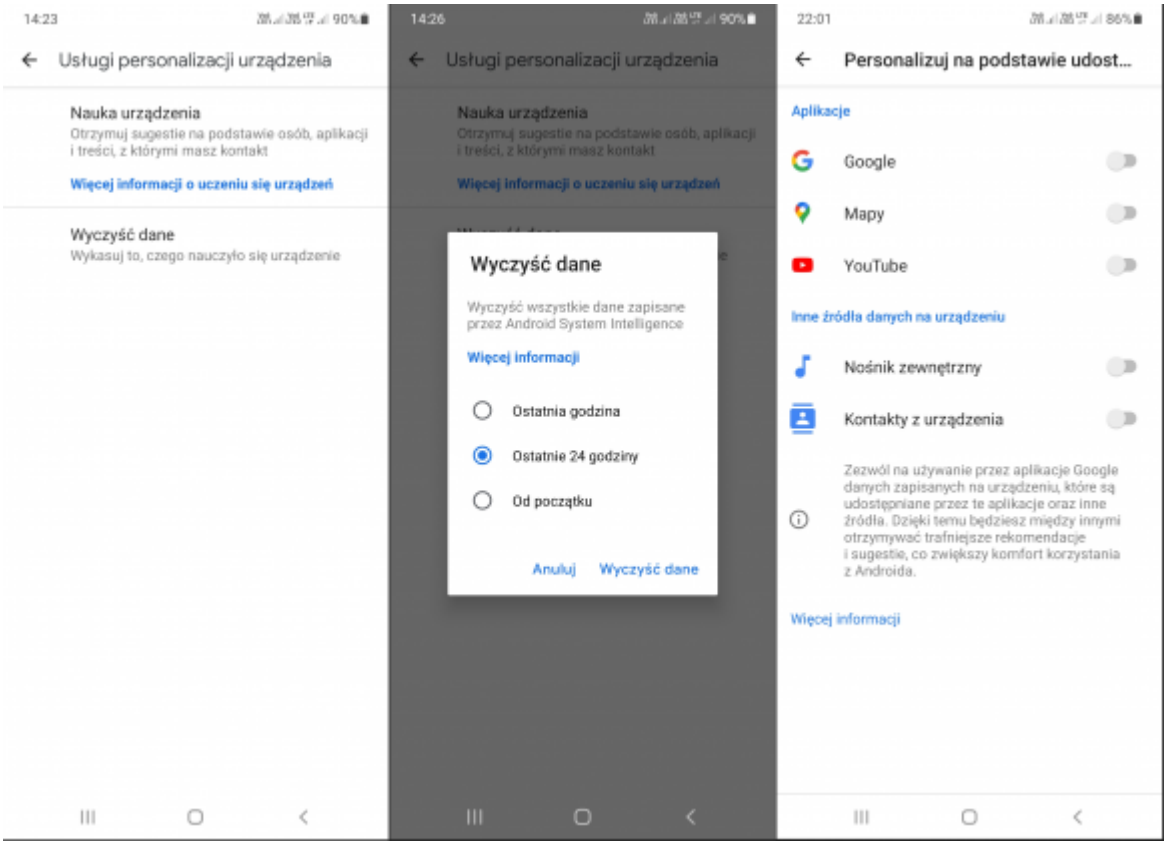
W zakładce „Prywatność” znajdziemy ponadto opcję wysyłania Samsungowi danych diagnostycznych, której również sugerujemy nie aktywować. Klikając w link „Dane diagnostyczne”, dowiemy się, że decyzja o nieprzekazywaniu firmie tego typu informacji nie wpłynie w żaden sposób na funkcjonalność telefonu. Producent zbiera je „w celu doskonalenia jakości produktów i usług oraz monitorowania przypadków i reagowania na przypadki niespodziewanych wyłączeń lub błędów systemu”. Jak widać na powyższym zrzucie ekranu, dane te za zgodą użytkownika mogą zostać powiązane z innymi informacjami o nim, które firma pozyskuje z różnych źródeł. Samsung zakłada, że cykl życia urządzeń przenośnych wynosi dwa lata i zapewnia, że po tym czasie informacje osobiste będą automatycznie usuwane (ale jak wiemy z polityki prywatności, nie brakuje od tej reguły

wyjątków).

Jeśli się zastanawiacie, czy inne firmy produkujące smartfony z Androidem gromadzą mniej danych albo obchodzą się z nimi lepiej, to odpowiedź brzmi „raczej nie”, o czym możecie się przekonać, zaglądając do ich polityk prywatności. Oto kilka przykładowych: Xiaomi, Huawei, Alcatel, Sony.

Ujarzmianie usług Google

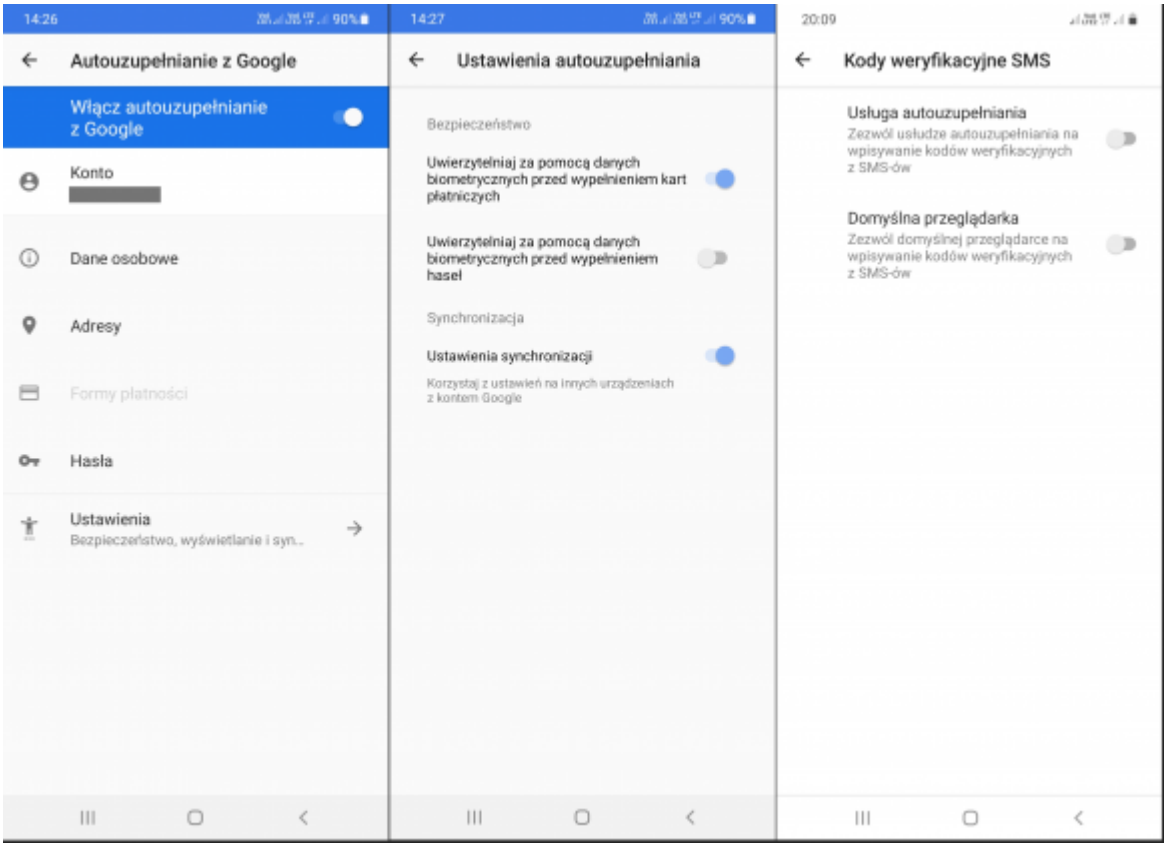
Przegląd ustawień prywatności związanych z usługami Google zaczynamy od możliwości personalizacji urządzenia i akurat w tym przypadku nie chodzi o wyświetlanie reklam, tylko o podpowiadanie użytkownikowi na podstawie jego wcześniejszych działań, co może w danej chwili zrobić. Jeśli np. zaznaczymy jakiś tekst, a Google rozpozna, że jest to nazwa restauracji, to możemy otrzymać sugestię otwarcia aplikacji Mapy i wyznaczenia trasy dojazdu. W zakładce „Prywatność” po wybraniu „Usług personalizacji urządzenia” możemy uzyskać więcej informacji na temat tej funkcji, a także usunąć zgromadzone dotychczas dane. W Androidzie 12 omawiana funkcja kryje się pod nazwą „Android System Intelligence” i pozwala dodatkowo włączyć inteligentne podpowiedzi w pasku sugestii klawiatury. W obu przypadkach, jeśli chcemy coś skonfigurować (czyli wskazać lub wykluczyć jakieś źródła danych), musimy się udać do zakładki „Google” i wybrać opcję „Personalizuj na podstawie udostępnionych danych”.



Usługi personalizacji urządzenia

Kolejna warta uwagi pozycja w zakładce „Prywatność” to „Usługa autouzupełniania Google” umożliwiająca automatyczne wpisywanie danych do formularzy, co jest – i owszem – wygodne, ale dostarcza producentowi Androida sporo wrażliwych informacji o użytkowniku. Jeśli włączymy tę funkcję, to po kliknięciu w „Dane osobowe” przeniesiemy się do sekcji zarządzania osobistymi informacjami na koncie Google, „Adresy” pozwolą nam ustawić adres domowy i służbowy w aplikacji Mapy, „Formy płatności” będą aktywne tylko po ich wcześniejszym skonfigurowaniu (w sekcji „Google” » „Ustawienia aplikacji Google” » „Google Pay”), a „Hasła” dadzą dostęp do wbudowanego menedżera haseł. Wybierając „Ustawienia”, będziemy mogli określić, czy chcemy uwierzytelniać się za pomocą biometrii przed wypełnieniem danych kart płatniczych i/lub haseł, a także zezwolić na synchronizację ustawień tej usługi na innych urządzeniach. Jeśli natomiast przejdziemy do sekcji „Autouzupełnianie” w zakładce „Google”, to znajdziemy tam m.in. opcję „Kody weryfikacyjne SMS”. Ze względów bezpieczeństwa nie powinniśmy zezwalać na wpisywanie kodów weryfikacyjnych z SMS-ów ani usłudze autouzupełniania, ani

domyślnej przeglądarce.

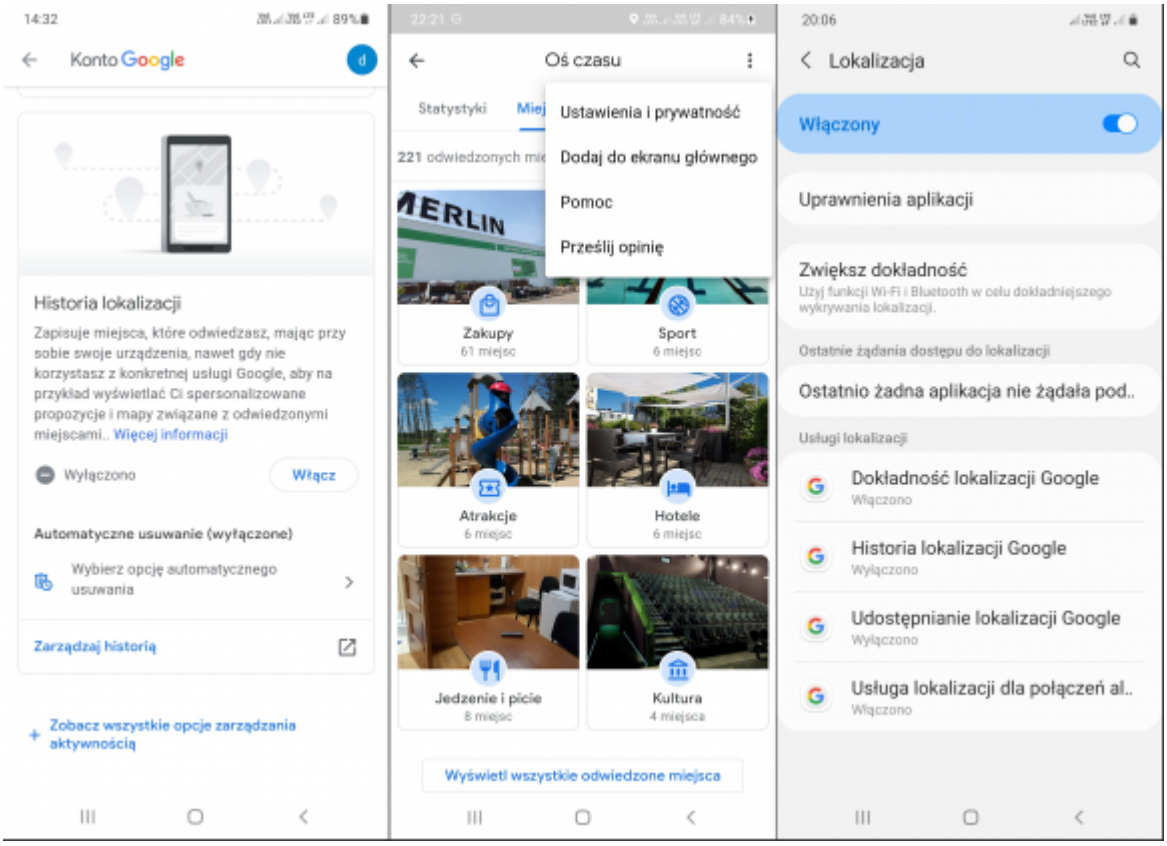


Ustawienia autouzupełniania

Przejdźmy teraz w zakładce „Prywatność” do sekcji „Historia lokalizacji Google”. Możemy ją od razu wyłączyć, lepszym pomysłem będzie jednak skorzystanie z opcji „Zarządzaj historią” i przejrzenie zapisanych przez firmę informacji o naszym przemieszczaniu się w świecie rzeczywistym. Klikając w trzy kropki widoczne po prawej stronie ekranu i wybierając „Ustawienia i prywatność”, uzyskamy m.in. możliwość usunięcia całej historii lokalizacji lub pewnego jej zakresu, a także skonfigurowania automatycznego usuwania gromadzonych danych – możemy w ten sposób na bieżąco kasować aktywność starszą niż 3, 18 lub 36 miesięcy.

Dodatkowe opcje znajdziemy w odrębnej zakładce „Lokalizacja”, dostępnej bezpośrednio z głównego menu ustawień smartfona. W sekcji „Uprawnienia aplikacji” możemy zobaczyć, jakim aplikacjom przyznaliśmy ciągły dostęp do danych lokalizacyjnych, jakie mają do nich dostęp tylko podczas używania i jakim nie daliśmy dostępu, choć o niego prosiły. W

przypadku pomyłki istnieje oczywiście możliwość skorygowania wcześniejszych wyborów. Standardowo lokalizacja urządzenia jest wykrywana za pomocą GPS, możemy jednak aplikacjom zezwolić na korzystanie z Wi-Fi i Bluetootha w celu dokładniejszego jej określania (co może się przydać, jeśli na fali sentymentu nadal gramy w Pokemon Go albo skonfigurowaliśmy zaufane miejsca w funkcji Smart Lock – zob. *Biometria i inne sposoby ochrony Androida przed niepowołanym dostępem*). Udostępniając swoją lokalizację innym osobom, powinniśmy pamiętać, że mogą się one dowiedzieć nie tylko, gdzie jesteśmy obecnie, ale również gdzie byliśmy przedtem, w jaki sposób się przemieszczamy (jedziemy czy idziemy), jaki jest stan naszego urządzenia, w tym np. stopień naładowania baterii i parę innych rzeczy – dlatego sugerujemy korzystać z tej opcji z rozwagą. Warto natomiast aktywować „Usługę lokalizacji dla połączeń alarmowych (ELS)". Jak tłumaczy producent systemu: „Gdy zadzwonisz lub napiszesz SMS-a na numer alarmowy, może zostać wysłana również lokalizacja Twojego telefonu, aby ratownicy mogli szybko Cię odnaleźć. Numer alarmowy w Stanach Zjednoczonych to 911, a w Europie 112".

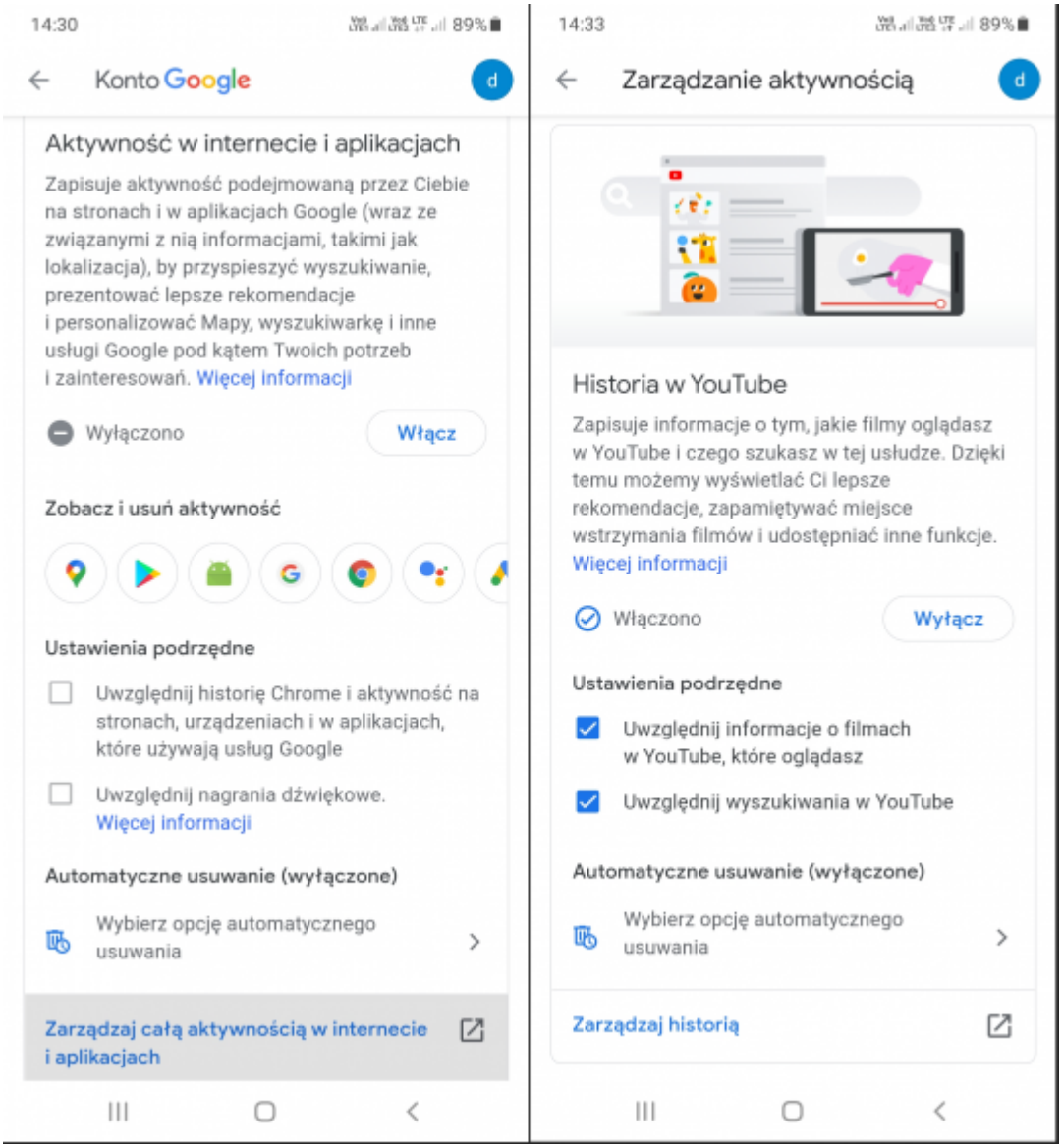


Zarządzanie lokalizacją

Wróćmy jednak do zakładki „Prywatność” i wybierzmy „Zarządzanie aktywnością”. Zobaczymy cztery sekcje: „Aktywność w internecie i aplikacjach”, ponownie (omówioną już) „Historię lokalizacji”, „Historię w YouTube” i „Personalizację reklam”.

Decydując się na zapisywanie naszej aktywności w internecie i aplikacjach, dowiemy się, że gromadzone dane „pomagają personalizować usługi Google, np. pozwalają szybciej wyszukiwać informacje oraz zwiększają trafność rekomendacji i reklam – zarówno w usługach Google, jak i innych firm”. Wniosek? Nic złego się nie stanie, jeśli wyłączymy tę funkcję. Jeśli tego nie zrobimy, możemy ograniczyć ilość zapisywanych informacji poprzez nieuwzględnianie historii przeglądarki Chrome i nagrań dźwiękowych generowanych podczas interakcji z wyszukiwarką Google, Asystentem i Mapami. Klikając w link „Więcej informacji”, przeczytamy, że ustawienie to „nie ma wpływu na dane dźwiękowe zapisane na Twoim urządzeniu i w innych usługach Google ani na sposób, w jaki Google przetwarza, transkrybuje i wykorzystuje do nauki Twoje dane w czasie rzeczywistym”. Tak jak w przypadku historii

lokalizacji, możemy skonfigurować automatyczne usuwanie zebranych danych. Wybierając „Zarządzaj całą aktywnością w internecie i aplikacjach”, otrzymamy także możliwość wyszukiwania i filtrowania zapisanych treści według dat i usług. Podobnie wygląda zarządzanie historią serwisu YouTube.

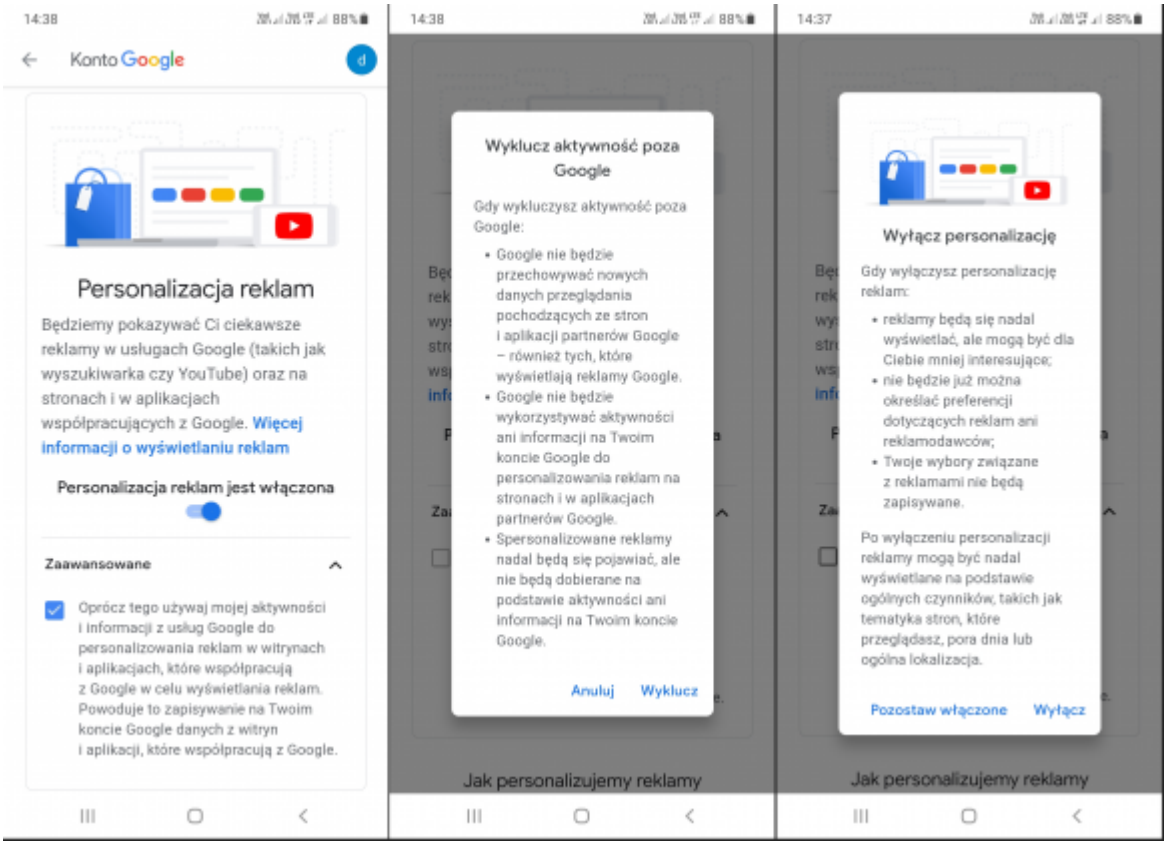


Zarządzanie aktywnością

Inaczej mają się sprawy z funkcją „Personalizacja reklam”. Jeśli jest ona włączona, to w sekcji „Jak personalizujemy reklamy” zobaczymy, na podstawie jakich danych osobowych Google dopasowuje do nas przekaz reklamodawców (przykładowe pozycje: „45-54 lata”, „Mężczyzna”, „Język: polski i jeszcze 1”). Każdą z uwzględnionych informacji możemy zaktualizować, a w przypadku profilowania na podstawie naszych zainteresowań – wyłączać te, z którymi się nie utożsamiamy i przywracać

wyłączone przez pomyłkę. W sekcji „Reklamy o charakterze kontrowersyjnym w YouTube” możemy ograniczyć wyświetlanie reklam dotyczących alkoholu i hazardu, a od pewnego czasu także randek, ciąży i rodzicielstwa czy nawet odchudzania. Na dole widnieje link „Twoje dane i reklamy”, pod którym znajduje się zapewnienie Google, że nigdy nie sprzedaje danych osobowych i nie używa informacji poufnych do personalizowania reklam. Sami musicie zadecydować, czy w to wierzycie. Bloomberg donosi, że z 68 mld dolarów całkowitych przychodów firmy w kwartale zakończonym 31 marca br. około 54 mld pochodziło z usług reklamowych.

Aby zapewnić sobie więcej prywatności, możemy usunąć zaznaczenie jedynej, niezbyt jasno opisanej opcji w zakładce „Zaawansowane” – dzięki temu Google nie będzie używać naszych danych do personalizowania reklam wyświetlanych na stronach i w aplikacjach firm trzecich, które z nim współpracują. Nie będzie też zapisywać informacji o naszych działaniach na stronach i w aplikacjach należących do zewnętrznych usługodawców. Jeszcze lepszym pomysłem jest całkowite wyłączenie personalizacji. Twórcy Androida uprzedzają, że reklamy nadal będą się nam wyświetlać, ale mogą być mniej interesujące – niewielka strata. Potwierdzając swój wybór, zobaczymy komunikat o możliwości wyłączenia personalizacji reklam Google wyświetlanych bez logowania oraz reklam z ponad 100 innych internetowych sieci reklamowych – da się tego dokonać w serwisie Your Online Choices (chociaż nie jest to rozwiązanie bez wad, bo opiera się na ciasteczkach).

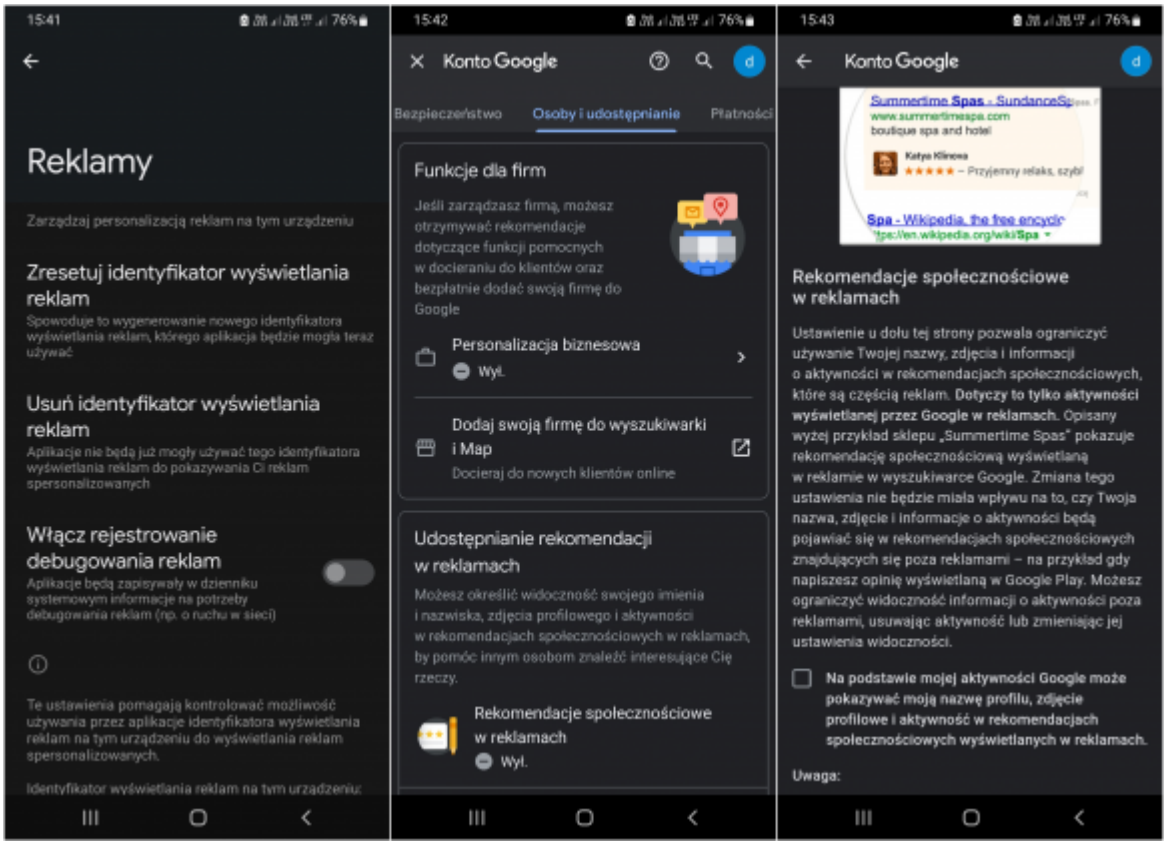


Personalizacja reklam

W zakładce „Prywatność” znajdziemy też odrębną sekcję „Reklamy”. W to samo miejsce trafimy, wybierając opcję o identycznej nazwie po wejściu z głównego menu ustawień do zakładki „Google” (czemu służy takie dublowanie ścieżek, nie wiadomo – może zamotaniu niedoświadczonego użytkownika, który dzięki temu coś przeoczy). W sekcji tej możemy zresetować unikalny identyfikator, który pozwala usługodawcom śledzić nasze zwyczaje i zainteresowania w celu lepszego dopasowania prezentowanych nam reklam. Identyfikator ten możemy również usunąć bez zastępowania go nowym. W Androidzie 12 stosowną opcję znajdziemy bez większych problemów, w starszych wersjach systemu kryje się ona natomiast pod nieco mylącą nazwą „Rezygnacja z personalizacji reklam”, którą dla odmiany trzeba włączyć.

Innej ukrytej funkcji musimy poszukać, wciskając w zakładce „Google” przycisk „Zarządzaj kontem Google”. Z górnego menu wybieramy „Osoby i udostępnianie”, przechodzimy do sekcji „Udostępnianie rekomendacji w reklamach” i klikamy w link „Zarządzaj rekomendacjami społecznościowymi”. Zobaczymy ścianę

tekstu wyjaśniającą, czym są wspomniane rekomendacje – w skrócie chodzi o możliwość wykorzystania w celach reklamowych naszej nazwy użytkownika, zdjęcia i informacji o aktywności (np. dodanej przez nas opinii o jakiejś restauracji). Aby temu zapobiec, trzeba zjechać na dół strony i usunąć zaznaczenie znajdującego się tam pola wyboru.

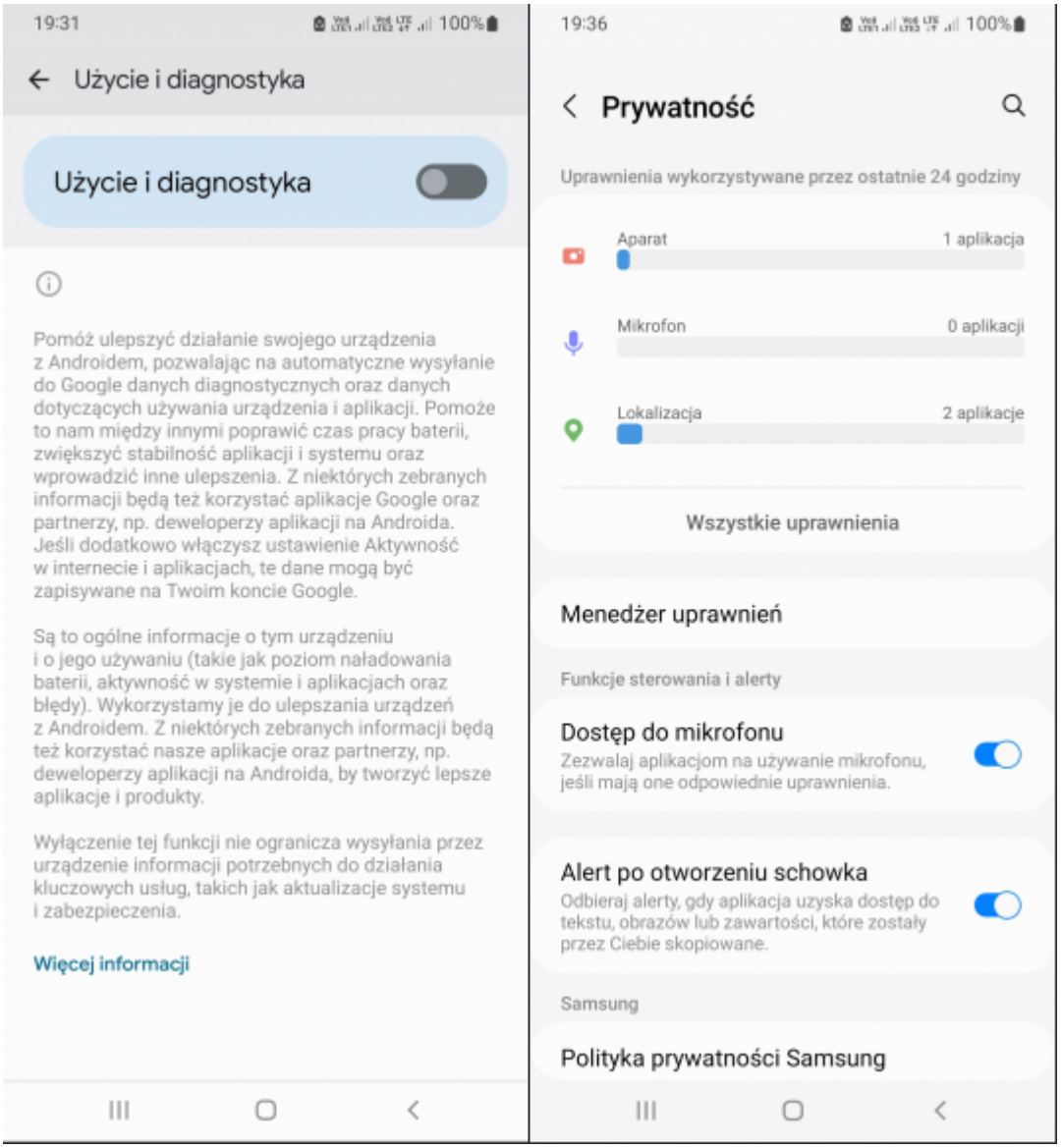


Reklamy i rekomendacje społecznościowe

Więcej sugestii dotyczących zarządzania kontem Google można znaleźć w naszych wcześniejszych artykułach z cyklu Podstawy Bezpieczeństwa: *Jak zadbać o swoją prywatność w usługach Google* oraz *Jak zadbać o swoje bezpieczeństwo w usługach Google*.

Ostatnią wartą uwagi sekcją w zakładce „Prywatność" jest „Użycie i diagnostyka", która po włączeniu przesyła producentowi systemu informacje o jego działaniu i ewentualnych problemach. Ze strony pomocy technicznej Google możemy się dowiedzieć, że firmę interesują również takie dane, jak częstotliwość używania aplikacji, poziom naładowania baterii oraz jakość i czas trwania połączeń sieciowych. Są one

zapisywane na koncie użytkownika, co oznacza, że da się je przejrzeć i usunąć za pośrednictwem strony Moja aktywność. Przesyłanie tych informacji nie jest konieczne do poprawnego funkcjonowania Androida, możemy więc tę funkcję zdezaktywować.



Wysyłanie danych diagnostycznych i inne opcje

Spośród nowych opcji, które dodano w Androidzie 12, warto wymienić możliwość cofnięcia wszystkim aplikacjom dostępu do mikrofonu (wystarczy posłużyć się jednym suwakiem) oraz alerty po otworzeniu schowka. W kolejnej wersji Androida ma się pojawić także automatyczne usuwanie historii schowka, dzięki czemu aplikacje zostaną prewencyjnie odcięte od wcześniej skopiowanych, nieprzeznaczonych dla nich informacji. Wchodząc do zakładki „Prywatność”, możemy teraz zobaczyć statystyki wykorzystania aparatu, mikrofonu i lokalizacji w ciągu

ostatnich 24 godzin. Kliknięcie w którąkolwiek z tych funkcji umożliwia zapoznanie się z dokładną historią jej użycia. W Androidzie 13 liczba aplikacji wymagających dostępu do lokalizacji może ulec zmniejszeniu – nie trzeba będzie np. przyznawać tego uprawnienia, aby włączyć skanowanie Wi-Fi.

Na konferencji Google I/O, która odbyła się w maju, firma poinformowała o dostępności „trzynastki" w wersji beta 2, którą wyposażono w wymienione wyżej i sporo innych nowości. Można ją przetestować na smartfonach kilku różnych producentów, ale Samsung się do nich nie zalicza. Cóż, poczekamy… zwłaszcza że Android 12 ledwo zaczął zdobywać popularność. Według statystyk dostępnych na stronie StatCounter na razie używa go tylko 11,77% posiadaczy telefonów z tym systemem, a w Polsce jeszcze mniej, bo 9,78%. Niekwestionowanym liderem pozostaje „jedenastka", która na szczęście przykłada do prywatności użytkowników większą wagę niż poprzedniczki.

Dla zachowania pełnej przejrzystości: Patronem cyklu jest Aruba Cloud. Za opracowanie i opublikowanie tego artykułu pobieramy wynagrodzenie.

Źródło

Amerykańskie szpitale dzielą się danymi pacjentów z Facebookiem

Artykuł zatytułowany *„Facebook Is Receiving Sensitive Medical Information from Hospital Websites”* („Facebook otrzymuje wrażliwe informacje medyczne ze stron internetowych szpitali”) jest jednym z bardziej szokujących artykułów śledczych tego tygodnia, który jednak nie trafił do mainstreamowych mediów korporacyjnych – donosi strona LifesiteNews, powołując się na wpis dr. Roberta Malone.

Autorzy dokumentują, że na prywatnych, wewnętrznych stronach internetowych (intranetowych) wielu szpitali zainstalowano narzędzie śledzące, które zbiera informacje o stanie zdrowia pacjentów. Obejmują one schorzenia, recepty i wizyty lekarskie. Narzędzie to następnie wysyła wszystkie te dane do Facebooka (i jego firmy macierzystej Meta).

Mamy tu do czynienia z najjaskrawszym przypadkiem złamania nie tylko etyki lekarskiej, ale przepisów – znanych w Stanach Zjednoczonych jako HIPAA – które powinno chronić dane prywatne pacjenta. Przepisami HIPAA zasłaniają się szpitale, odmawiając nawet współmałżonkowi czy rodzicom, dostępu do informacji o stanie zdrowia. Jak widać, dzielenie się tymi wrażliymi danymi z korporacyjnymi podmiotami, których jednym z największych zadań jest śledzenie użytkowników, nie stanowi jednak najmniejszego problemu dla administratorów szpitali.

Autorzy, którzy pierwotnie opublikowali wyniki śledztwa w *The Markup*, wskazują, że narzędzie szpiegujące było zainstalowane w 33 ze 100 najlepszych szpitali w USA i w siedmiu głównych systemach medycznych, w tym w systemie „My Chart”. Oznacza to, że duży odsetek szpitali bezpośrednio wysyłał dane pacjentów do Facebooka (lub Mety).

„Aby było jasne, chodzi tu tylko o 33 szpitale, które zostały przetestowane przez *The Markup*, a nie o systemy szpitalne czy zdecydowaną większość szpitali i gabinetów lekarskich, które korzystają z tych dużych systemów oprogramowania opartych na chmurze lub sieci w USA." – piszą dziennikarze śledczy.

Gdyby wyniki te ekstrapolować na całość systemu szpitalnego w USA, to oznaczałoby to, że ponad 1/3 wszystkich placówek dzieli się danymi pacjentów z największą korporacją, w gruncie rzeczy powołaną do zbierania danych użytkowników.

„Jeszcze w 2017 r. rząd rzeczywiście martwił się, że systemy medyczne mogą zostać zhakowane." – pisze dr Malone, nieco naiwnie uważając, że rząd kiedykolwiek „martwił się" o ochronę praw pacjenta. „Najwyraźniej 'my', ludzie, nie możemy polegać na rządzie USA. … Dlatego musimy chronić się sami." – kończy jednak trzeźwo.

Jak pisaliśmy wiele lat temu o historiach powstawania takich firm jak Facebook czy Google: niech nikt nie powtarza idiotycznych bajek jakoby kilku studentów, ot tak, samorzutnie utworzyło największe firmy na świecie. Co prawda nie znamy (jeszcze oficjalnie) pikantnych szczegółów powstania Facebooka, ale jeśli chodzi o Google, to wiemy już – ze zdeklasyfikowanych dokumentów – że powstał on przy pomocy finansowej i przy wsparciu DARPA (*Defense Advanced Research Projects Agency* – Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności), czyli Agencji Departamentu Obrony USA, odpowiedzialnej m.in. za sfinansowanie pierwszych badań nad stworzeniem Internetu, najnowocześniejszych broni, czy broni biologicznej. Z takimi firmami jak Google czy Facebook jest właśnie tak jak można było sobie przeczytać w niejednym „konspiracyjnym" opowiadaniu science-fiction: **rządowe inwigilacyjne agencje typu NSA uznały, że łatwiej będzie zebrać dane ludzi przy użyciu popularnych narzędzi zabawowo-komunikacyjnych niż przy pomocy „klasycznej" acz**

technologicznie zaawansowanej metody wywiadowczej. Sfinansowano więc projekty Google'a (i Facebooka) i rozpostarto parasol ochronny nad przydatnymi dla wywiadu firmami.

A propos: czy nie powinno dać nieco do myślenia, że dzisiejsze giganty wywiadowcze założone zostały przez Żydów? Larry Page (matka żydówka), Sergey Brin (rodzice – rosyjscy żydzi, żona – żydówka polskiego pochodzenia), Mark Zuckerberg, Eduardo Saverin czy Dustin Moskovitz… można wymieniać. Ale przecież to tylko przypadek, wszak jedynie żydowscy studenci są tacy zdolni…

> ***Pamiętaj: używając Facebooka sam instalujesz sobie Spyware i Malware.***
>
> ***Używając Facebooka czy Google nie miej złudzeń co do zachowania prywatności. Firmy te istnieją głównie CELEM zbierania danych.***
>
> *Za Twoją „darmową" skrzynkę pocztową – i inne „damowe" usługi – płacisz danymi o sobie.*

Źródło

Cena naszej prywatności

Polacy są skłonni płacić po 14-17 złotych miesięcznie, aby

uniknąć reklam i ograniczyć platformom internetowym dostęp do swoich osobistych danych.

4,025 miliardów złotych warte były dla Google'a dane polskich użytkowników w 2020 r., a 2,196 mld zł – wynosiła wartość danych z Polski dla Facebooka. My jednak raczej nie chcemy, aby te obie globalne firmy miały wiedzę na nasz temat. Polacy są skłonni nawet płacić po kilkanaście złotych miesięcznie, aby ograniczyć przedsiębiorstwom dostęp do swoich prywatnych danych – mówi badanie przeprowadzone przez Polski Instytut Ekonomiczny. Ciekawe, czy Polacy byliby też skłonni zapłacić za to, aby mniej na ich temat wiedziały różne dzisiejsze instytucje rządowe?

Ponadto, aż 87 proc. uczestników badania PIE twierdzi, że firmy technologiczne wiedzą o nas za dużo, a 84 proc. uważa, że działalność tych firm powinna podlegać większej kontroli. Inny model funkcjonowania platform cyfrowych byłby zatem społecznie pożądany – wynika z raportu Polskiego Instytutu Ekonomicznego „Ile warte są nasze dane?".
Polacy są więc generalnie niechętni temu, aby platformy cyfrowe na szeroką skalę wykorzystywały ich dane, a zwłaszcza za darmo. Lubimy zarobić, więc za obecną sytuację, w której platformy cyfrowe mają dostęp do niemal wszystkich naszych danych oraz wyświetlają spersonalizowane reklamy, przeciętny użytkownik internetu oczekiwałby pieniężnej rekompensaty.

Jak wskazuje PIE, ponad połowa pytanych internautów (63 proc.) zgadza się z postulatem zakazu pokazywania reklam na podstawie danych osób prywatnych. Z drugiej strony, zaledwie 38 proc. ankietowanych jest gotowych płacić za lepszą ochronę prywatności tym serwisom, z których korzystają.

„Może to być związane z nieufnością wobec takich firm. 76 proc. nie wierzy, że płatna wersja Facebooka lepiej chroniłaby ich prawa. W przypadku Google'a jest to 73 proc." – mówi Ignacy Święcicki, kierownik zespołu gospodarki cyfrowej w Polskim Instytucie Ekonomicznym.

Zdaniem PIE, przychody Google'a i Facebooka z danych polskich użytkowników są znacznie wyższe od raportowanych przez polskie oddziały tych koncernów na potrzeby statystyki i dla organów podatkowych.

„Miesięczny przychód z danych pojedynczego polskiego użytkownika dla Google wynosi 10,16 PLN. Szacujemy, że łącznie w 2020 r. przychód z danych wszystkich polskich użytkowników wyniósł więc nawet 4,025 mld PLN. Miesięczny przychód z danych polskiego użytkownika dla Facebooka wynosi 8,52 PLN. Czyli – według naszych szacunków – łącznie w 2020 r. przychód z danych wszystkich polskich użytkowników mógł sięgać 2,196 mld PLN" – ocenia PIE.

W ostatnich latach mieliśmy do czynienia z ogromnym wzrostem skali i zasięgu działania oraz skokiem przychodów i zysków platform cyfrowych. W trzecim kwartale 2021 r. platformy miały aż 42 proc. udział w pierwszej 10 firm o najwyższej na świecie wycenie giełdowej. Dla porównania, jeszcze 10 lat wcześniej ten udział był zerowy, co poniekąd zrozumiałe, bo one dopiero wtedy rozwijały skrzydła. W przypadku Facebooka przychody z reklam stanowią 98 proc. przychodów firmy – 84 miliardów dolarów globalnie w 2020 r., w przypadku Google'a, udział przychodów z reklamy w przychodach firmy to 80 proc. – około 147 mld dol.

Sposób funkcjonowania platform cyfrowych wiąże się z pozyskiwaniem i przetwarzaniem ogromnych ilości danych użytkowników. Jak pokazało badanie Polskiego Instytutu Ekonomicznego, fakt ten nie umyka świadomości internautów. Aż 77 proc. respondentów zdaje sobie sprawę, że za bezpłatny dostęp do usług w sieci płaci swoimi danymi.

PIE w swym sondażu zapytał też o możliwość korzystania ze zmodyfikowanych wersji głównych serwisów, w których w zamian za płatność platformy zbierają mniej danych.

„Okazało się, że przeciętny badany jest skłonny płacić 17,07

zł miesięcznie, aby Facebook nie miał dostępu ani do danych agregowanych na platformie, ani pochodzących z innych źródeł. Za brak dostępu Google'a do prywatnych danych – w tym aktywności na innych portalach – Polki i Polacy byliby skłonni płacić 14,10 zł miesięcznie" – twierdzi Jacek Grzeszak, starszy analityk z zespołu strategii w PIE.

Jakakolwiek zmiana dzisiejszego, nadzwyczaj opłacalnego modelu biznesowego funkcjonowania platform cyfrowych będzie trudna do przeprowadzenia, ale wydaje się być społecznie oczekiwana. Aż 69 proc. respondentów w badaniu PIE uważa, że żadna strona internetowa ani aplikacja nie powinny pobierać opłat za dostęp.

Zdaniem PIE, twierdzenia dotyczące reklamy internetowej mogą jednak wydawać się paradoksalne. Z jednej strony bowiem 63 proc. internautów zgadza się z postulatem zakazu pokazywania reklam na podstawie danych osób prywatnych. Wprowadzenie w życie takiego kroku doprowadziłoby do zaprzestania tzw. targetowania reklam. W efekcie jedynym sposobem dopasowania reklam do potrzeb odbiorcy byłoby mało precyzyjne bazowanie na lokalizacji, z której dana osoba loguje się do internetu (czyli, czy z miasta, czy wsi) lub tzw. reklama kontekstowa, która zakłada dopasowanie treści reklam do zawartości stron, na których są one umieszczone. Z drugiej strony aż 43 proc. badanych wyraża przekonanie o tym, że obecne, kierowane do nich reklamy, odpowiadają na ich potrzeby.

Według PIE, te wyniki wskazują na pewną niekonsekwencję w odpowiedziach respondentów. W rzeczywistości chodzi jednak o to, że wbrew rozpowszechnionemu przekonaniu, reklama internetowa ma dość znikomy wpływ na zachowania zakupowe konsumentów, więc jest im raczej obojętne, czy odpowiada ona na ich potrzeby, czy nie.

Nie zmienia to faktu, że Polacy chętnie mogliby zaakceptować zmieniony model zarządzania usługami oferowanymi przez platformy. Chodziłoby w nim przede wszystkim o ochronę

prywatności i ograniczenie lub nawet całkowite pozbycie się targetowanych reklam wyświetlanych użytkownikom.

Jak ocenia Krystian Łukasik, analityk z zespołu gospodarki cyfrowej w PIE, już przy opłacie rzędu około 10 zł miesięcznie, obie strony odczułyby korzyść – i nadawcy internetowi, i odbiorcy ich treści. Jest to bowiem kwota niższa niż deklarowana przez respondentów jako możliwa do zapłaty za wyeliminowanie dostępu do swych danych. Z drugiej zaś strony, jest wyższa niż średni miesięczny przychód platform z obecności jednego użytkownika.

Nie wiadomo jednak, czy inkasując te 10 zł miesięcznie, platformy cyfrowe rzeczywiście zrezygnowałyby z reklam, czy tylko jakoś zakamuflowały ich obecność? Szefowie tych koncernów najchętniej pragnęliby przecież mieć i dochody z reklam, i comiesięczne wpływy od użytkowników.

Trybuna.info

Aplikacje należące do Facebooka mogą śledzić i zbierać Twoje dane, nawet jeśli nie używasz ich aktywnie

Wiele aplikacji na smartfony śledzi dane osób, w tym ich bieżącą lokalizację, nawet jeśli nie korzystają z nich aktywnie. Eksperci twierdzą, że jednym z najgorszych przestępców jest Facebook Messenger, dedykowana aplikacja do przesyłania wiadomości firmy mediów społecznościowych.

Eksperci zachęcają teraz ludzi do przeprowadzenia badań i zastanowienia się, jakie dane osobowe mogą rozdawać, pobierając i rejestrując się w aplikacjach takich jak Facebook Messenger.

„Jestem świadomy tego, kogo zaprosić do mojego domu, więc myślałem tak samo o tym, co mam na telefonie, i zachowałem ostrożność przy pobieranych aplikacjach" – powiedział Michael Huth, dyrektor ds. Badań i współzałożyciel firmy zajmującej się prywatnością i zorientowaną przeglądarką z własną wyszukiwarką i aplikacją.

Huth poradził ludziom, aby obniżyli poziom tego, do czego Facebook Messenger może uzyskać dostęp ze swoich smartfonów. Aplikacja Facebook może zbierać wszelkiego rodzaju dane od swoich użytkowników, jeśli tego nie robią, zwłaszcza jeśli nie są świadomi, do czego aplikacja ma dostęp.

„Firmy takie jak Google i Facebook próbują ukryć to, co robią z danymi i sprawić, by brzmiały pozytywnie", powiedział współzałożyciel i dyrektor generalny Xayn Leif-Nissen Lundbaek. „Zawierają język, który brzmi tak, jakby chroniły prywatność, chociaż tak nie jest".

Innym przykładem, który podał Lundbaek, jest WhatsApp, rzekomo prywatna usługa przesyłania wiadomości należąca do Facebooka z

szyfrowaniem typu end-to-end.

Lundbaek powiedział, że WhatsApp oferuje niewiele funkcji, które według Facebooka poprawiają jego prywatność. W rzeczywistości te funkcje w niewielkim stopniu chronią dane osób.

„Istnieje szereg aplikacji, takich jak przeglądarka Google i TiKTok, które są gorsze niż WhatsApp, ale nadal nie jest to dobry przykład" – powiedział. „To nie jest obrońca prywatności".

„Śledzą wszystko, od interakcji po inne używane aplikacje, lokalizacje i ruch" – dodał Lundbaek.

Inne aplikacje należące do Facebooka przekazujące dane użytkownika firmie macierzystej

Facebook Messenger, WhatsApp i Instagram są własnością Facebooka. Wszystkie są znane z udostępniania wielu prywatnych danych firmie macierzystej.

Obecne zasady WhatsApp chronią zawartość czatów danej osoby, w tym zdjęcia, filmy i połączenia, przed przechwyceniem przez Facebook. Nie wiadomo, czy niniejsza polityka prywatności jest przestrzegana co do joty.

To, co usługa szyfrowanych wiadomości typu end-to-end może udostępniać, to numer telefonu i nazwa profilu użytkownika. Może również udostępniać, gdy użytkownik wysyła wiadomość do innych osób. Adres IP użytkownika może być również gromadzony i udostępniany innym markom należącym do Facebooka.

Polityka prywatności WhatsApp jest celowo niejasna. Mówi, że może udostępniać dane osobowe Facebookowi wyraźnie wyróżnione

w polityce „lub uzyskane po powiadomieniu lub na podstawie Twojej zgody”.

Niedawna zmiana w polityce prywatności WhatsApp umożliwiła również firmom reklamującym się za pośrednictwem Facebooka przechowywanie czatów użytkowników na serwerach należących do Facebooka. Zak Doffman, dyrektor generalny firmy Digital Barriers zajmującej się technologią monitoringu, powiedział, że podważa to wiarygodność WhatsApp jako rzekomo kompleksowej usługi szyfrowanej wiadomości.

„WhatsApp twierdzi, że Facebook nie może wykorzystywać tych danych, ale firma może wyszukiwać czaty w celach reklamowych” – powiedział Doffman.

Instagram jest o wiele bardziej bezpośredni dzięki zbieranym danym. Jego polityka prywatności stwierdza, że Facebook „łączy informacje o twoich działaniach w różnych produktach i urządzeniach Facebooka”. Aplikacja podobno robi to, aby zapewnić użytkownikom „bardziej dostosowane i spójne wrażenia”.

Ponadto Instagram swobodnie gromadzi lokalizacje użytkowników, miejsca zamieszkania, miejsca, które odwiedzają, oraz szczegóły dotyczące firm i osób, z którymi są blisko i z którymi wchodzą w interakcje, aby „dostarczać, personalizować i ulepszać produkty Facebooka”.

Innymi słowy, Instagram udostępnia te dane Facebookowi w celu reklamy ukierunkowanej.

Jake Moore, specjalista ds. cyberbezpieczeństwa, ostrzegł osoby, które chcą korzystać z Instagrama, że ma on mniej kontroli prywatności niż sam Facebook.

„Instagram ma mniej kontroli prywatności niż Facebook” – powiedział. „I nie można powstrzymać większości swoich danych między platformami”.

Źródło:

The-Sun.com

Wired.co.uk