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.

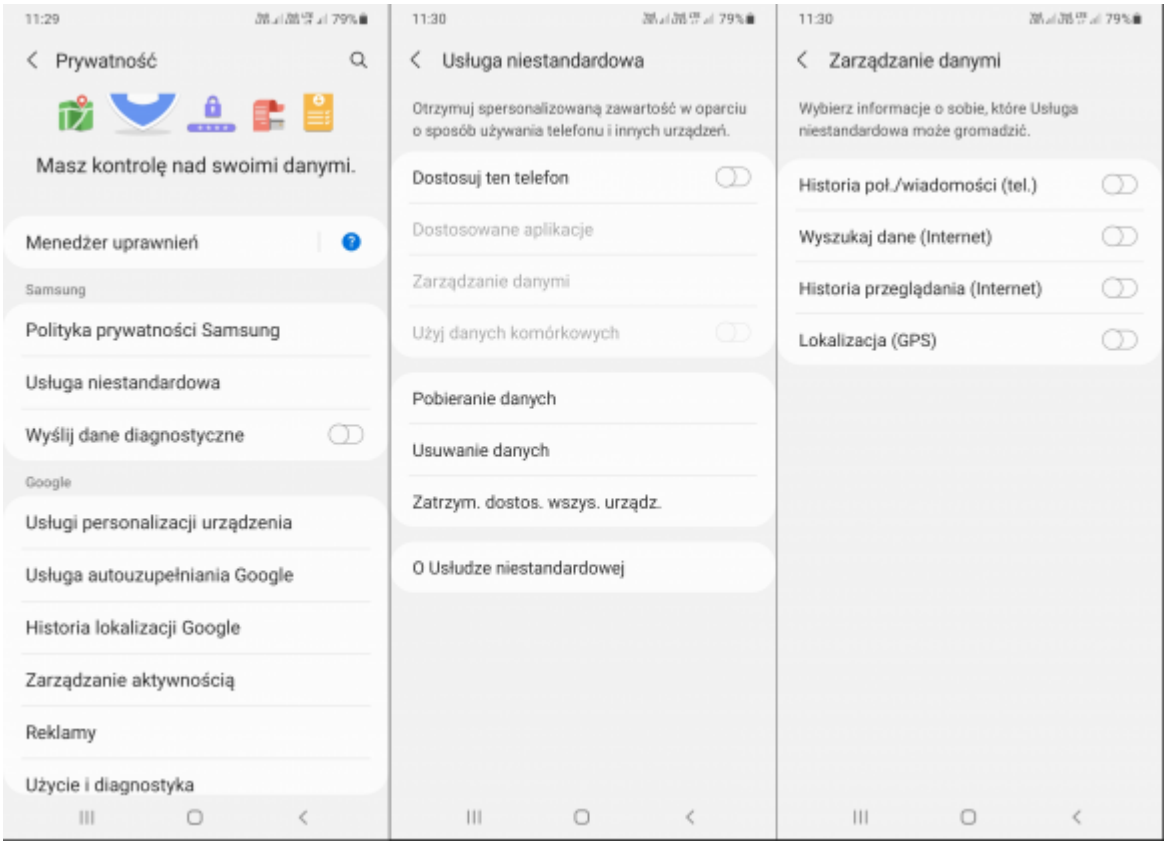
Jakie dane zbiera Samsung i co z tym zrobić

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.

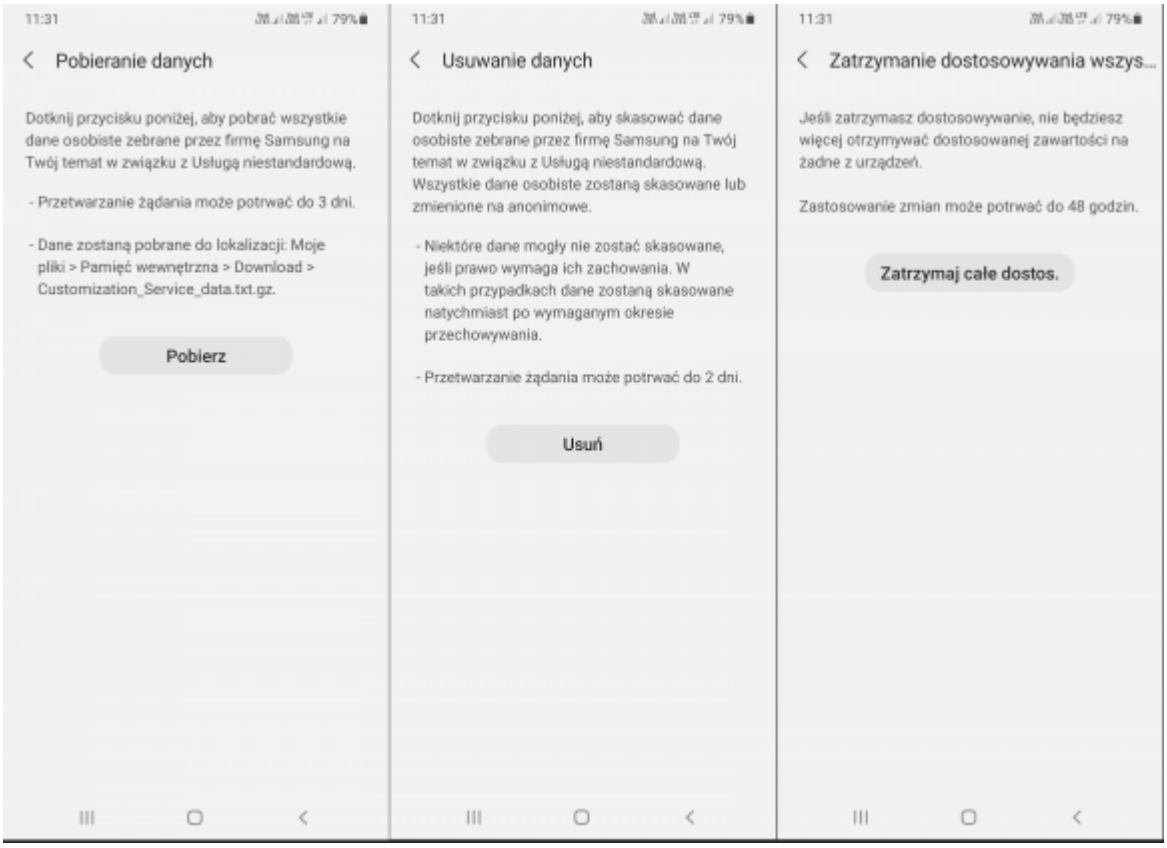
Zgromadzone dane mogą być przekazywane licznym podmiotom, m.in. partnerom biznesowym Samsunga i współpracującym z nim usługodawcom, którzy dokonują napraw, przygotowują spersonalizowane reklamy itp. Informacje o konkretnych użytkownikach mogą być ujawniane „gdy wymaga tego prawo lub gdy jest to niezbędne 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.



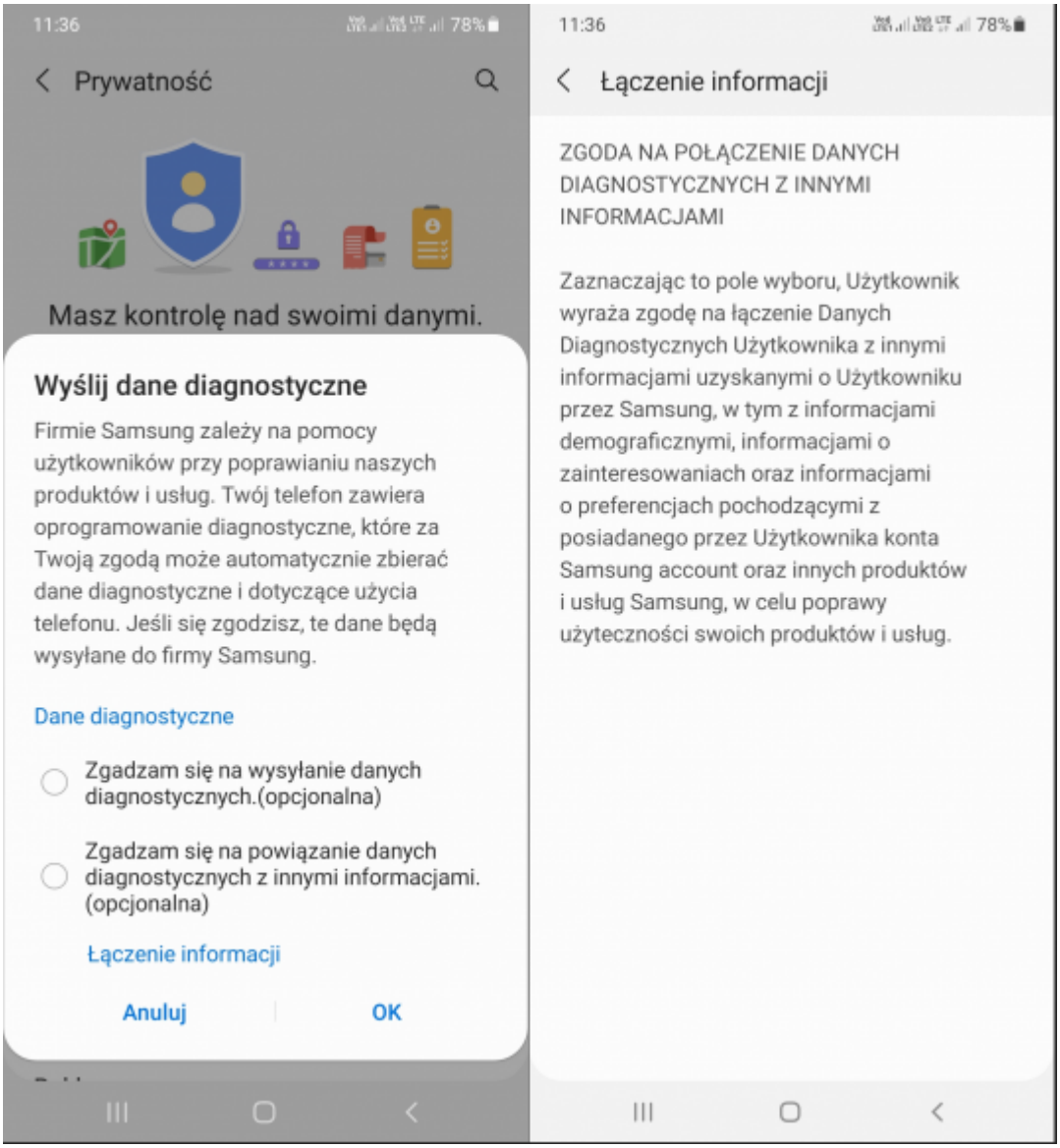
„Usługa niestandardowa” oferowana przez Samsunga

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

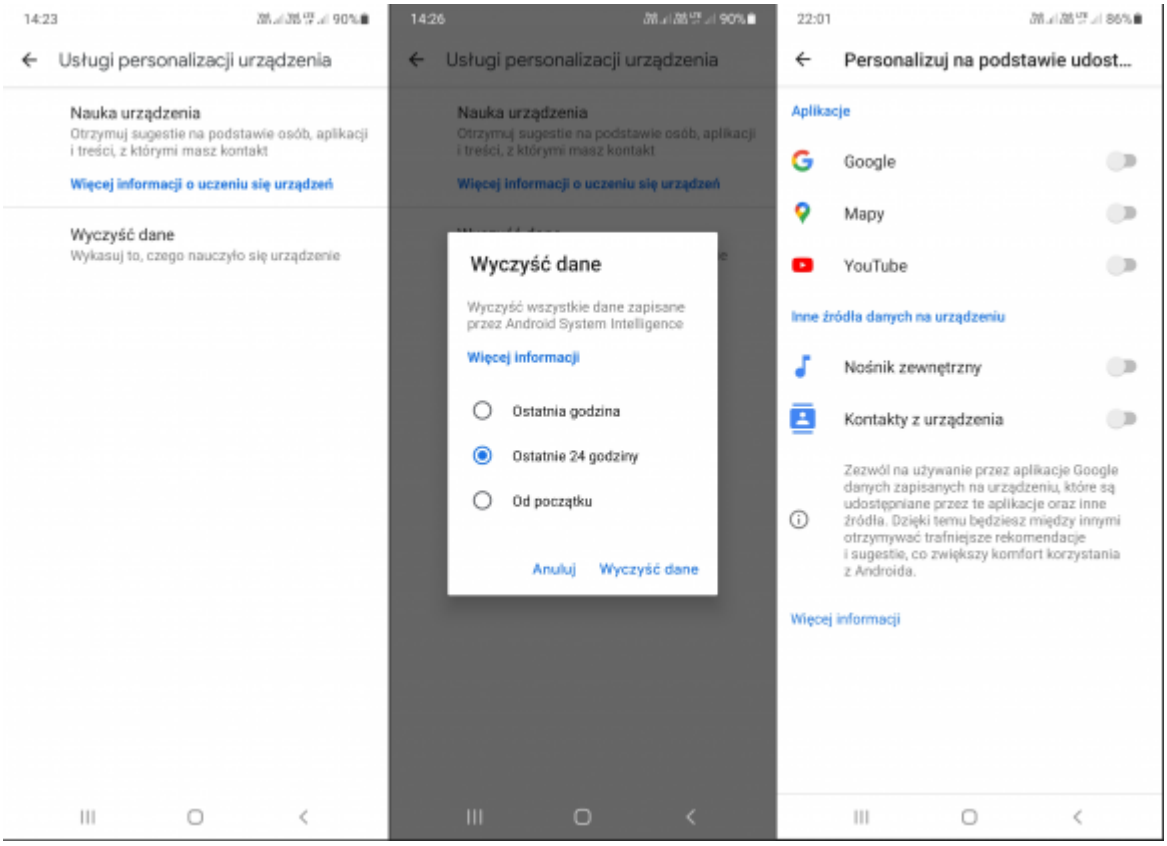
W zakładce „Prywatność” znajdziemy ponadto opcję wysyłania Samsungowi danych diagnostycznych, której również sugerujemy nie aktywować. Klikając w link „Dane diagnostyczne”, dowiemy się, że decyzja o nieprzekazywaniu firmie tego typu informacji nie wpłynie w żaden sposób na funkcjonalność telefonu. Producent 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

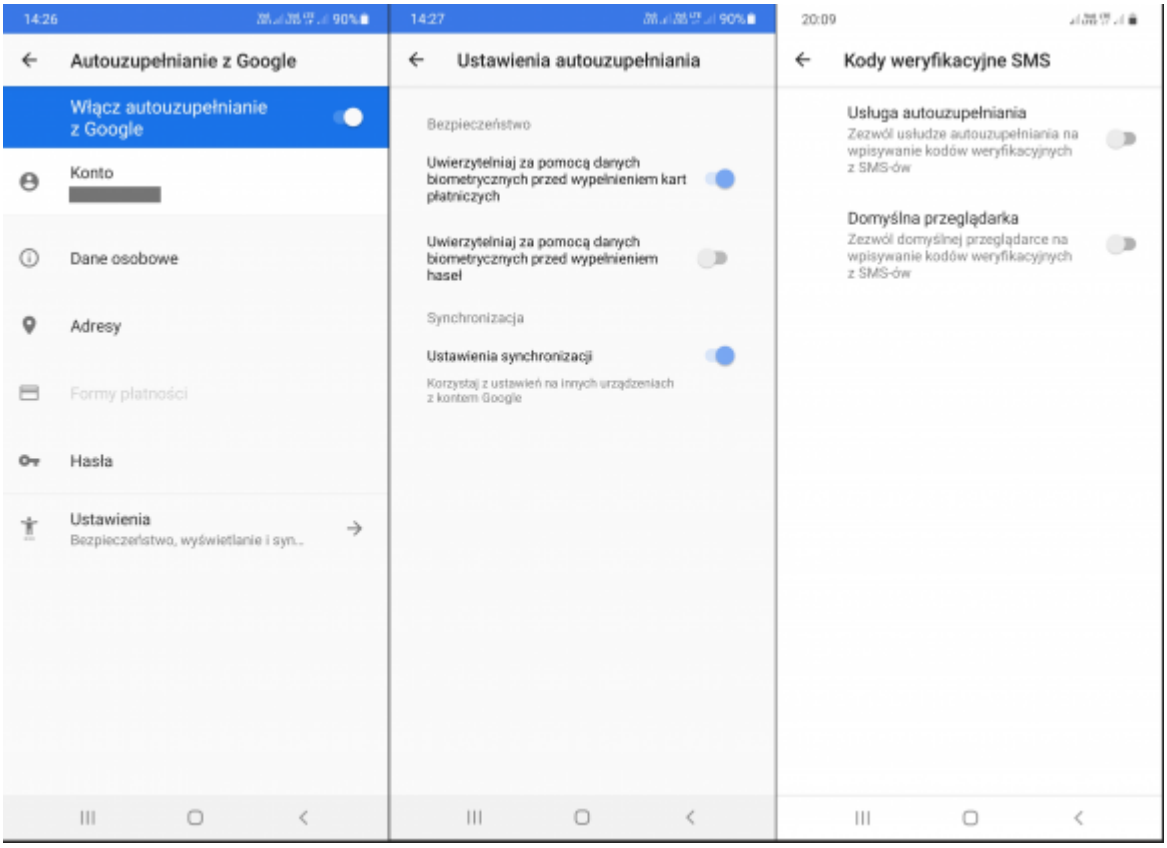
Przegląd ustawień prywatności związanych z usługami Google zaczynamy od możliwości personalizacji urządzenia i akurat w tym przypadku nie chodzi o wyświetlanie reklam, tylko o podpowiadanie użytkownikowi na podstawie jego wcześniejszych działań, co może w danej chwili zrobić. Jeśli np. zaznaczymy jakiś 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.

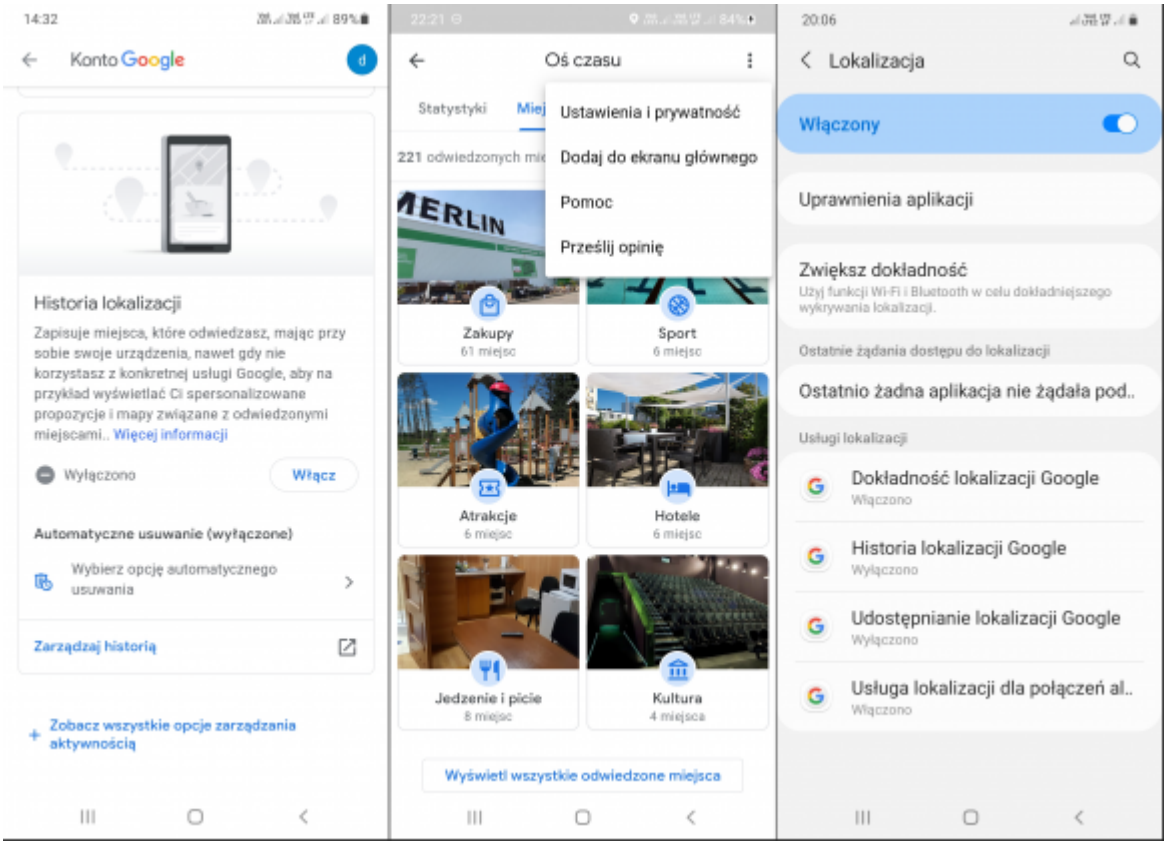


Ustawienia autouzupełniania

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".

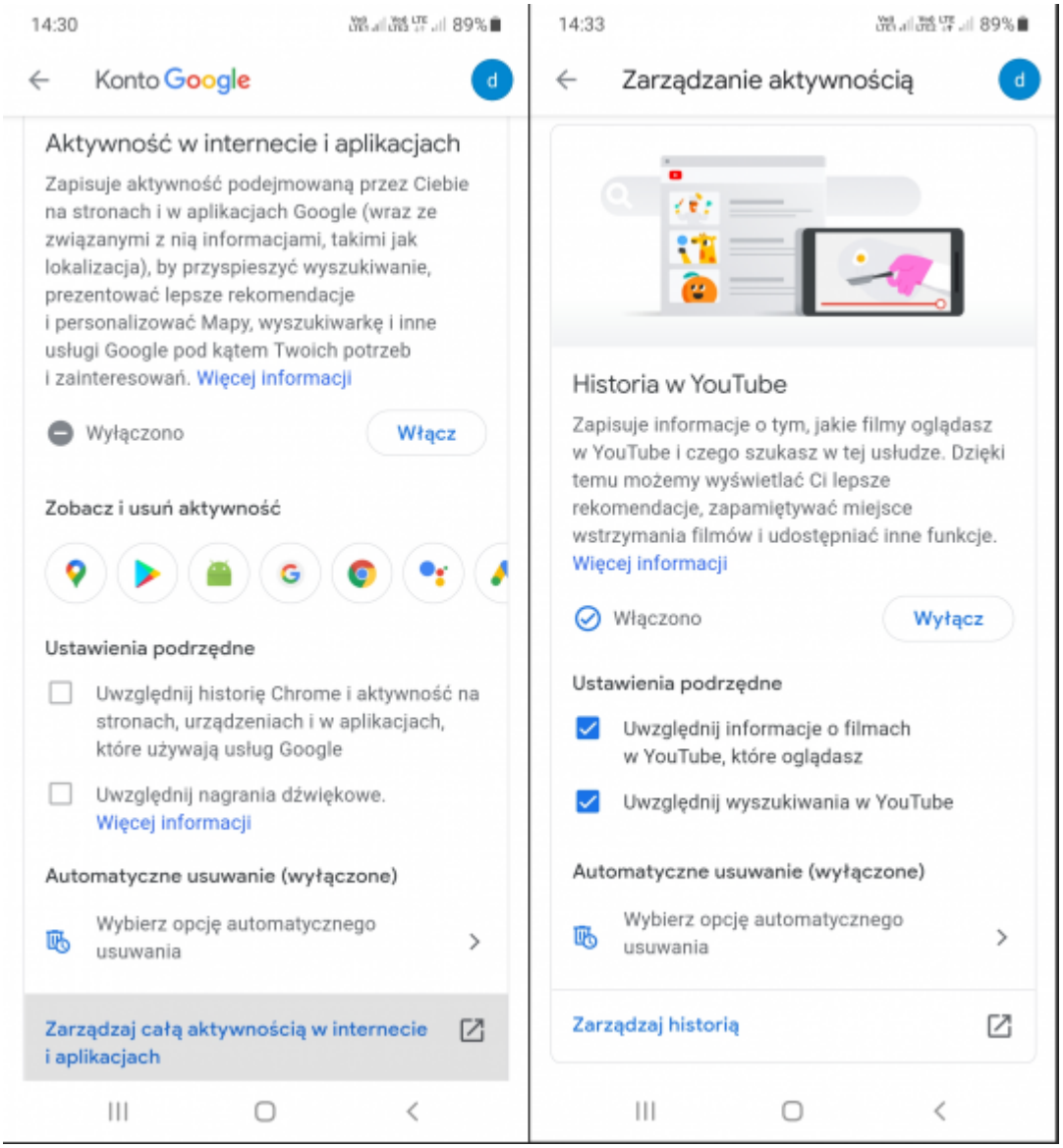


Zarządzanie lokalizacją

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.

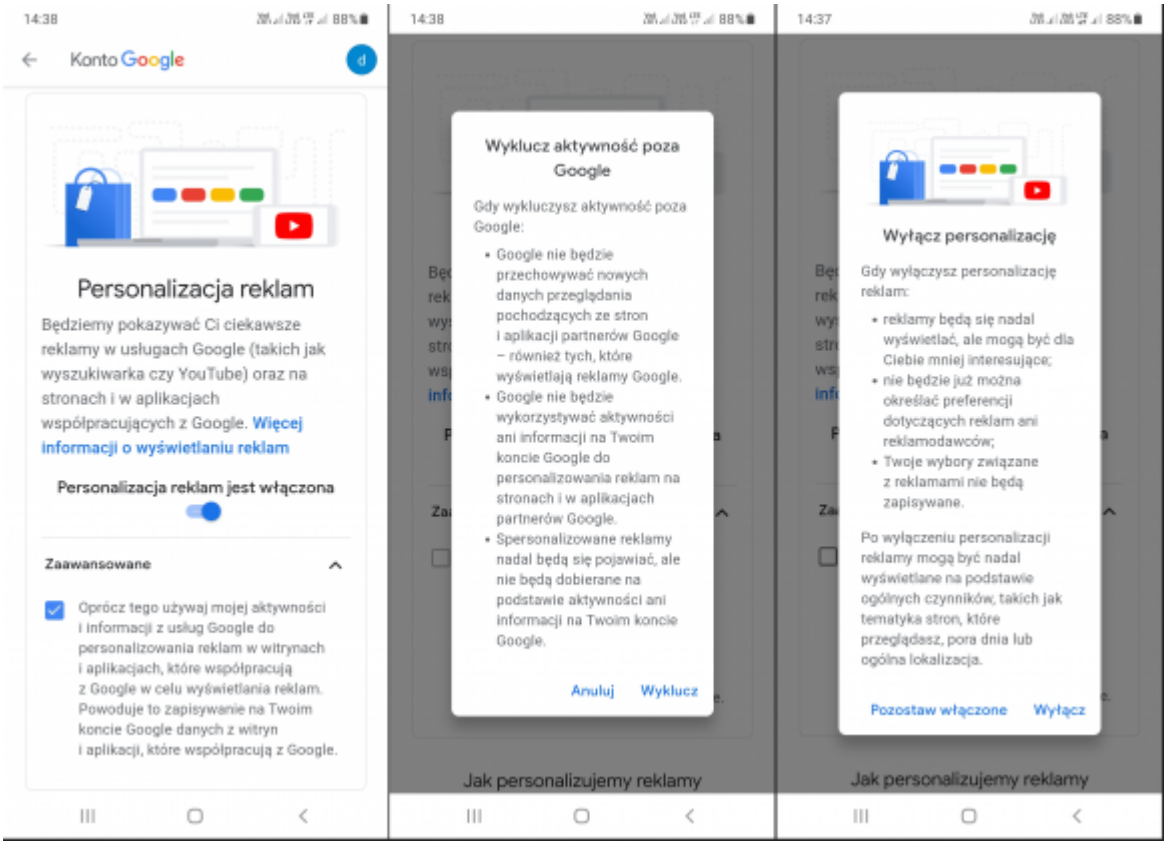


Zarządzanie aktywnością

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).

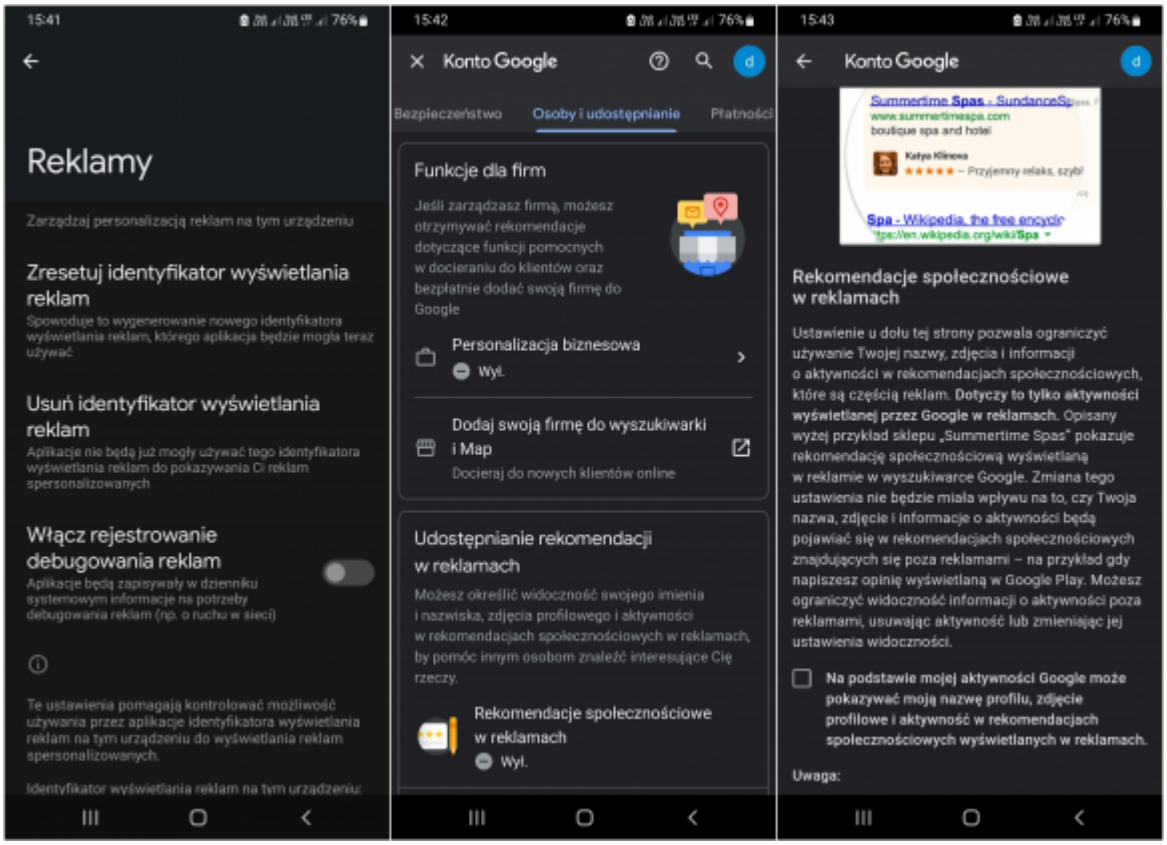


Personalizacja reklam

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.

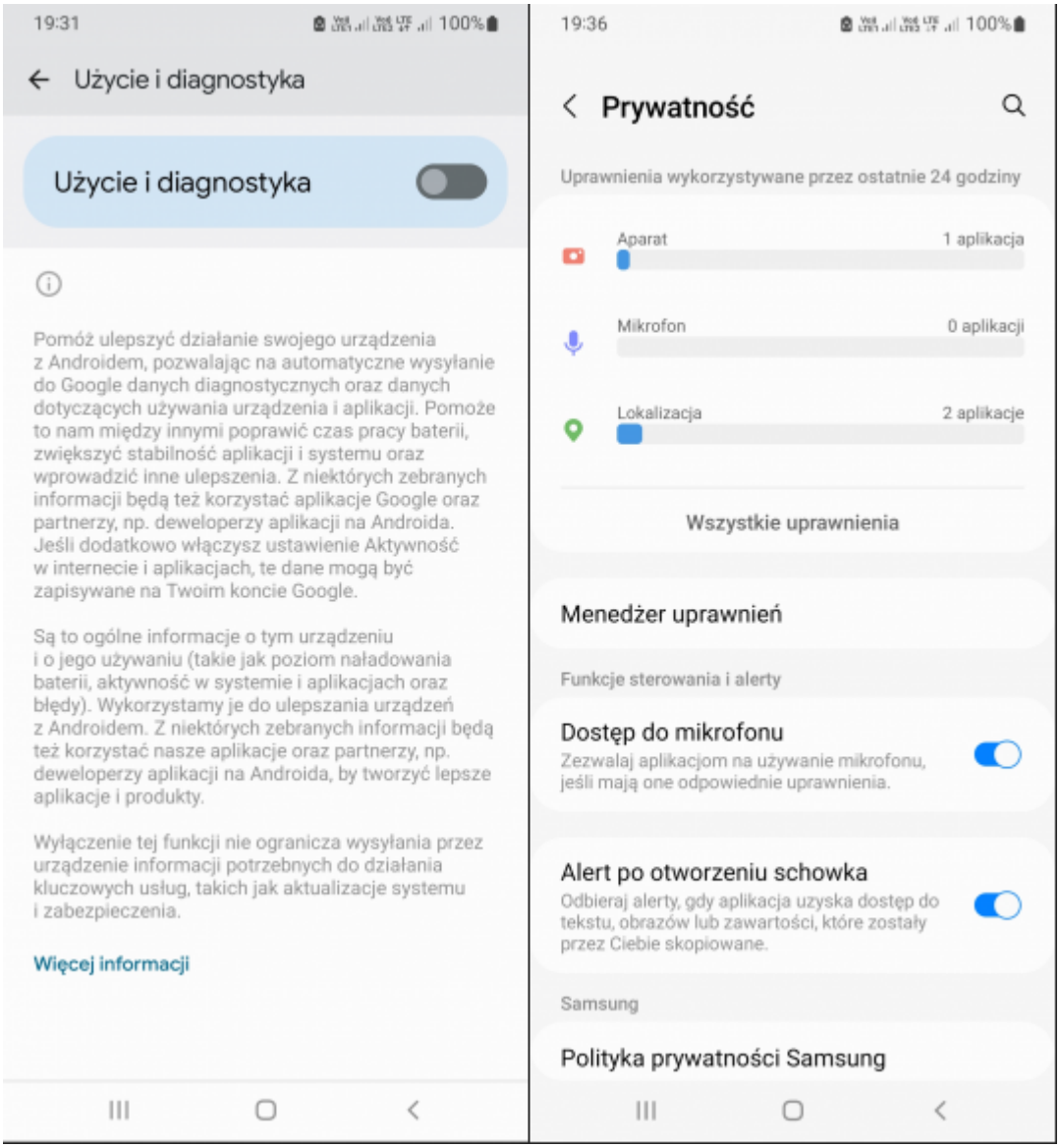


Reklamy i rekomendacje społecznościowe

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

Google śledzi użytkowników Chrome nawet w trybie „incognito”

Jeśli używasz przeglądarki Google Chrome do surfowania po sieci i robisz to „incognito”, co ma oznaczać przeglądanie prywatne, powinieneś wiedzieć, że gigant z Doliny Krzemowej nadal potajemnie śledzi twoją aktywność w sieci.

Firma Alphabet Inc. twierdzi, że aktywacja trybu „stealth” w Chrome oznacza po prostu, że firma nie „zapamięta Twojej aktywności”. Nie oznacza to, że Google nie jest w stanie zobaczyć, które strony odwiedzasz i jak często je odwiedzasz, co dla niektórych może być zaskoczeniem.

Sędzia okręgowy USA Lucy Koh, znana z tego, że wzięła się za Big Tech, które jest winne zbrodni przeciwko ludzkości, odpowiedziała na pozew zbiorowy przeciwko Google, mówiąc, że jest „zaniepokojona” praktykami gromadzenia danych przez międzynarodową korporację, które w najlepszym przypadku są

zwodnicze.

Pozew domaga się 5000 dolarów odszkodowania za każdego z milionów użytkowników Chrome, których prywatność została naruszona od czerwca 2016 roku. Koh mówi, że uważa za „niezwykłe” to, że Google dokłada „dodatkowego wysiłku” w celu zebrania takich danych, jeśli rzekomo tego nie robi aby profilować użytkowników i kierować do nich reklamy.

Firma Google jest i była uwikłana w liczne procesy sądowe dotyczące jej praktyk monopolistycznych, w tym naruszania prywatności w reklamach cyfrowych i wyszukiwaniu online. W jednym z nich Koh skutecznie zmusiła Google do ujawnienia skanowania prywatnych wiadomości e-mail w celu tworzenia profili i kierowania reklam.

W tym przypadku Google jest oskarżany o osadzanie kodu w witrynach internetowych, które wykorzystują jej usługi analityczne i reklamowe do pobierania danych z rzekomo prywatnej historii przeglądania użytkowników i przekazywania ich na serwery Google w celu przetworzenia.

Google sprawia wrażenie, jakby tryb przeglądania prywatnego zapewniał użytkownikom większą kontrolę nad ich danymi, mówi prawniczka Amanda Bonn, ale w rzeczywistości „Google twierdzi, że w zasadzie niewiele można zrobić, aby uniemożliwić nam gromadzenie Twoich danych, i właśnie to powinieneś założyć”

Google to zło; przestań używać ich produkty

Andrew Shapiro, prawnik Google, twierdzi, że polityka prywatności jego klienta „wyraźnie ujawnia” fakt, że podczas korzystania z produktu Google prawie nic nie jest prywatne.

„Gromadzenie danych, o którym mowa, zostało ujawnione” – mówi.

Stephen Broome, inny prawnik Google, mówi, że strony internetowe, które zawierają umowę z Google na korzystanie z jej narzędzi analitycznych lub innych usług, doskonale znają

praktyki gromadzenia danych jego klientów i nie jest to tajemnicą.

Broome próbował bagatelizować obawy powodów, a także sądu dotyczące prywatności, wskazując, że własna strona internetowa federalnego sądu korzysta z usług Google. Ta taktyka przyniosła jednak odwrotny skutek, gdy sędzia zażądał wyjaśnienia „co dokładnie robi Google", wyrażając jednocześnie obawy, że osoby odwiedzające witrynę sądu nieświadomie ujawniają Google prywatne informacje.

„Chcę oświadczenia od Google na temat tego, jakie informacje gromadzą o użytkownikach witryny sądu i do czego są one wykorzystywane" – powiedziała Koh prawnikom Google.

Wniosek z tego wszystkiego jest taki, że Google nie można i nie powinno się ufać. Wszystko, co robi, ma na celu zarabianie pieniędzy, przejęcie władzy, eliminację praw ludzi i ostatecznie osiągnięcie dominacji nad światem.

„Ponadto Google i Alphabet ukradły kod Oracle, więc cała ich działalność opiera się na tej kradzieży" – zauważył jeden z naszych komentatorów o kolejnej króliczej dziurze Google.

„Sprawa jest w tej chwili w Sądzie Najwyższym i wkrótce zostanie rozpatrzona. Naprawdę łatwo to udowodnić, Google jest skończone. Nawet przestępcy w Sądzie Najwyższym nie mogą pozwolić sobie na to. To zbyt oczywiste".

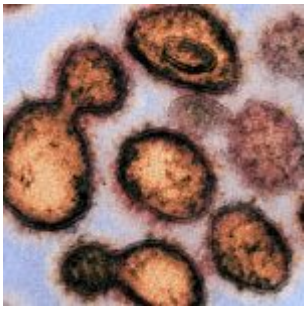
Inny komentator zgodził się z tym, dodając, że „dni Google są policzone", ponieważ „nigdy nie nauczą się, że wahadło może wychylać się tylko daleko w jednym kierunku, i musi wrócić".

Źródła tego artykułu obejmują:

BNNBloomberg.ca

NaturalNews.com

COVID19 – dowody globalnego oszustwa



COVID-19 i późniejsze reakcje rządu wydają się być częścią międzynarodowego spisku mającego na celu popełnienie oszustwa. Wydaje się, że nie ma dowodów na to, że wirus o nazwie SARS-CoV-2 wywołuje chorobę zwaną COVID-19.

Czasami musisz kierować się instynktem. Nie jestem ekspertem w dziedzinie genetyki i, jak zawsze, oczekuję poprawy. Jednak moją uwagę zwróciły niektóre badania opublikowane przez hiszpańskie czasopismo medyczne D-Salud-Discovery. Ich rada doradcza złożona z wybitnie wykwalifikowanych lekarzy i naukowców nadaje ich badaniom wiarygodność. Ich twierdzenie jest zdumiewające.

Genetyczne startery i sondy używane w testach RT-PCR do identyfikacji SARS-CoV-2 nie są ukierunkowane na nic konkretnego. Postępowałem zgodnie z technikami wyszukiwania przedstawionymi w tym angielskim tłumaczeniu ich raportu i mogę potwierdzić dokładność ich twierdzeń dotyczących sekwencji nukleotydów wymienionych w protokołach Światowej Organizacji Zdrowia. Możesz zrobić to samo.

D-Salud-Discovery oświadcza, że nie ma testów zdolnych do identyfikacji SARS-CoV-2. W związku z tym wszystkie twierdzenia dotyczące domniemanego wpływu COVID 19 na zdrowie

populacji są bezpodstawne.

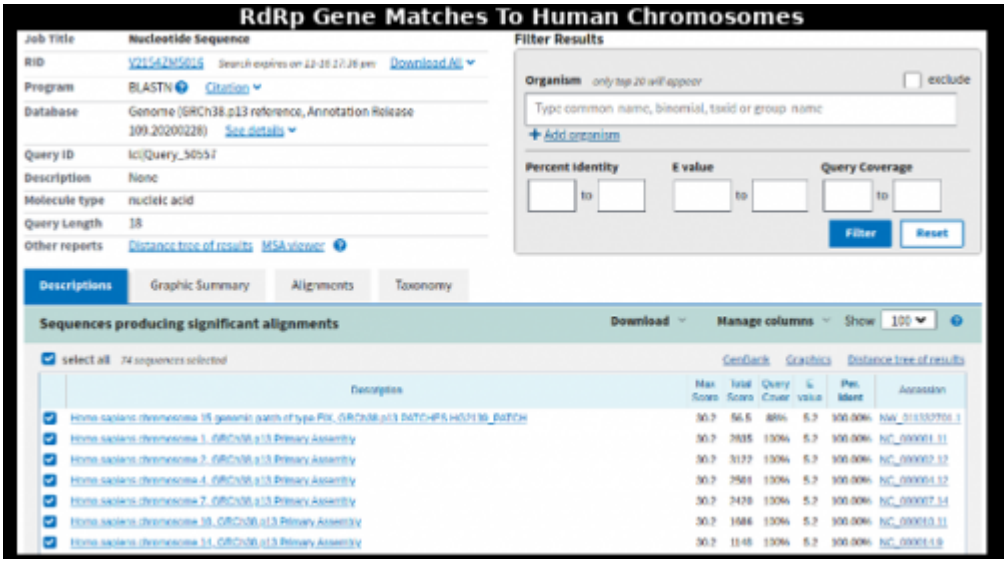
Cała oficjalna narracja COVID 19 jest oszustwem. Podobno nie ma naukowych podstaw dla jakiejkolwiek części tej narracji.

Jeśli te twierdzenia są trafne, możemy stwierdzić, że nie ma dowodów na pandemię, a jedynie jej złudzenie. Ponieśliśmy nieobliczalne straty bez wyraźnego powodu, poza ambicjami pozbawionych skrupułów despotów, którzy chcą przekształcić globalną gospodarkę i nasze społeczeństwo, aby odpowiadały ich celom.

Czyniąc to, ta *„klasa pasożytów”* potencjalnie popełniła niezliczone przestępstwa. Przestępstwa te mogą i powinny być przeanalizowane i rozpatrzone przed sądem.

Identyfikacja ale czego dokładnie?

Światowa Organizacja Zdrowia (WHO) sklasyfikowała COVID-19 (choroba COronaVIrus 2019). Ogłosili globalną pandemię COVID-19 11 marca 2019 roku.



[Wytyczne](#) WHO dotyczące [badań laboratoryjnych](#) stanowią:

> *Czynnik etiologiczny [przyczyna choroby] odpowiedzialny za skupisko przypadków zapalenia płuc w Wuhan został zidentyfikowany jako nowy betakoronawirus (z tej samej rodziny co SARS-CoV i MERS-CoV) poprzez sekwencjonowanie nowej generacji (NGS) z hodowanego wirusa lub bezpośrednio z próbek otrzymanych od kilku pacjentów z zapaleniem płuc."*

WHO twierdzi, że wirus SARS CoV-2 *jest powodem choroby* COVID-19. Twierdzą również, że ten wirus został wyraźnie zidentyfikowany przez naukowców z Wuhan.

W WHO'wskim [Novel Coronavirus 2019-nCov Situation Report 1](#) na temat [koronawirusa 2019-nCov 1](#) stwierdza się:

> *Chińskie władze zidentyfikowały nowy typ koronawirusa, który został wyizolowany 7 stycznia 2020 r. …… W dniu 12 stycznia 2020 r. Chiny udostępniły krajom sekwencję genetyczną nowego koronawirusa do wykorzystania przy opracowywaniu określonych zestawów diagnostycznych."*

Te dwa oświadczenia WHO jasno sugerują, że wirus SARS-CoV-2 został wyizolowany (co oznacza oczyszczony do badań), a następnie *zidentyfikowano* sekwencje genetyczne z wyizolowanej próbki. Na tej podstawie opracowano i rozprowadzono na całym

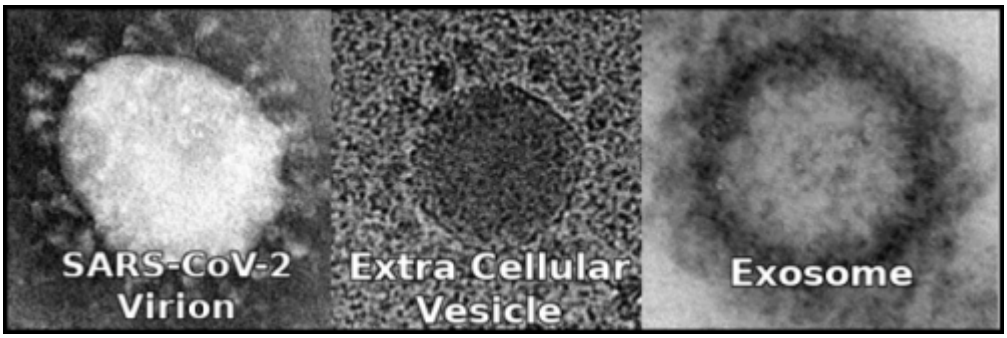
świecie zestawy diagnostyczne do testowania wirusa w miastach i społecznościach na całym świecie. Według WHO i chińskich naukowców testy te wykryją wirusa, który *powoduje* COVID 19.

Jednak WHO stwierdza również:

> *Pracując bezpośrednio na podstawie informacji o sekwencjach, zespół opracował serię testów amplifikacji genów (PCR) wykorzystywanych przez laboratoria."*

Naukowcy z Wuhan opracowali testy amplifikacji genów na podstawie *„informacji o sekwencji",* ponieważ nie było wyizolowanej, oczyszczonej próbki tak zwanego wirusa SARS-CoV-2. Pokazali również obrazy z mikroskopu elektronowego nowo odkrytych wirionów (kolczastej kulki białkowej zawierającej wirusowe RNA).

Jednak takie struktury białek nie są wyjątkowe. Wyglądają jak inne okrągłe pęcherzyki, takie jak pęcherzyki endocytarne i egzosomy.



Wirusolodzy twierdzą, że nie jest możliwe *„wyizolowanie"* wirusa, ponieważ replikuje się on tylko w komórkach gospodarza. Dodają, że Postulaty Kocha nie mają zastosowania, ponieważ dotyczą bakterii (czyli organizmów żywych). Zamiast tego wirusolodzy obserwują cytopatogenne skutki wirusa (CPE), powodujące mutację i degradację komórek w hodowlach komórkowych.

Kiedy chińscy naukowcy po raz pierwszy zsekwencjonowali pełny genom SARS-CoV-2, zaobserwowali CPE w komórkach Vero E6 i

Huh7. Vero E6 to unieśmiertelniona linia komórek małpich, a Huh7 to unieśmiertelnione komórki rakowe (rakotwórcze). Oznacza to, że były one utrzymywane in vitro (w hodowlach na płytkach Petriego) przez wiele lat.

Centralnym punktem oficjalnej historii SARS-CoV-2 jest idea, że jest to wirus odzwierzęcy, zdolny do pokonywania dystansu między zwierzętami a ludźmi. Kiedy naukowcy z amerykańskiego CDC *„zainfekowali”* różne komórki nowym wirusem, zauważyli, co następuje:

> *Zbadaliśmy zdolność SARS-CoV-2 do infekowania i replikacji w kilku popularnych liniach komórkowych naczelnych i ludzkich, w tym ludzkich komórkach gruczolakoraka (A549) [komórki płuc], ludzkich komórkach wątroby (HUH7.0) i ludzkich embrionalnych komórkach nerkowych (HEK-293T), oprócz Vero E6 i Vero CCL81 [komórki małpy]… Nie zaobserwowano efektu cytopatycznego w żadnej z linii komórkowych z wyjątkiem komórek Vero [komórki małpy]… Komórki HUH7.0 i 293T wykazały jedynie niewielką replikację wirusa i Komórki A549 [ludzkie komórki tkanki płucnej] były niezgodne z zakażeniem SARS-CoV-2”.*

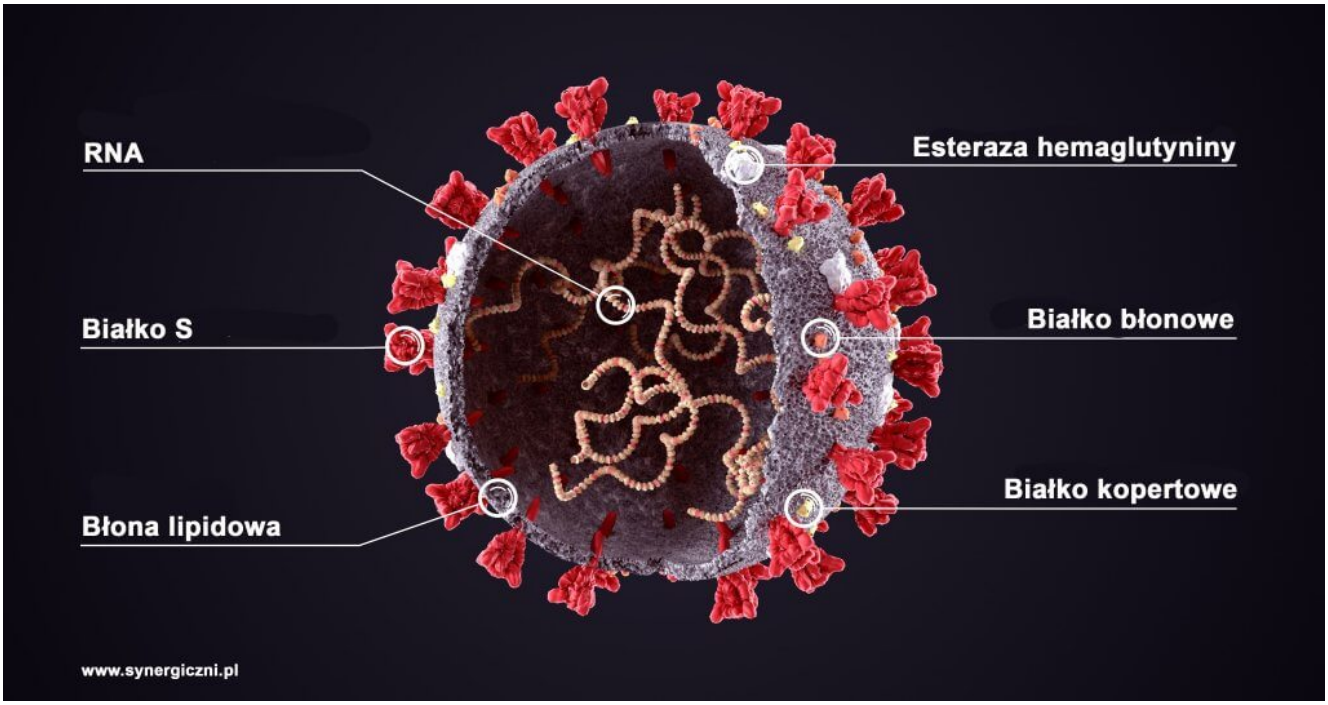
CDC nie zaobserwował żadnego CPE w ludzkich komórkach. Nie widzieli żadnych dowodów na to, że ten rzekomy wirus spowodował jakąkolwiek chorobę człowieka. Ten rzekomy ludzki wirus nie wykazywał też żadnej godnej uwagi replikacji w ludzkich komórkach, co sugeruje, że infekcja z człowieka na człowieka byłaby niemożliwa.

Dostrzegając ten problem, zespół polskich naukowców wprowadził tego sekwencjonowanego *„wirusa”* do komórek nabłonka ludzkiego (dróg oddechowych). Obserwowali wpływ na te kultury HAE przez 5 dni. Zauważyli znacznie większą replikację niż naukowcy z CDC, ale ostatecznie stwierdzili:

„Nie zaobserwowaliśmy żadnego uwolnienia wirusa z podstawno-bocznej strony hodowli HAE”.

Oznacza to, że nie widzieli żadnych dowodów rzekomych wirionów naruszających błonę ściany komórkowej. Ponownie sugerujemy, że ten tak zwany wirus nie jest zaraźliwy dla ludzi.

Nie jest jasne, czy SARS-CoV-2 jest ludzkim wirusem zdolnym do wywoływania choroby. Może nawet nie istnieć fizycznie. Czy to nic innego jak koncepcja oparta na *predykcyjnych* sekwencjach genetycznych?



Podróż odkrywcza

Wuhan Center for Disease Control and Prevention oraz Shanghai Public Health Clinical Center opublikowały pierwszy pełny genom SARS-CoV-2 (MN908947.1). To było wielokrotnie aktualizowane. Jednak MN908947.1 był pierwszą sekwencją genetyczną opisującą rzekomy czynnik *etiologiczny* COVID-19 (SARS-CoV-2).

Wszystkie kolejne roszczenia, testy, terapie, statystyki, opracowywanie szczepionek i wynikające z nich zasady są oparte na tej sekwencji. Jeśli testy tego *nowego* wirusa nie zidentyfikują niczego, co mogłoby wywołać chorobę u ludzi, cała narracja COVID-19 jest niczym innym jak farsą.

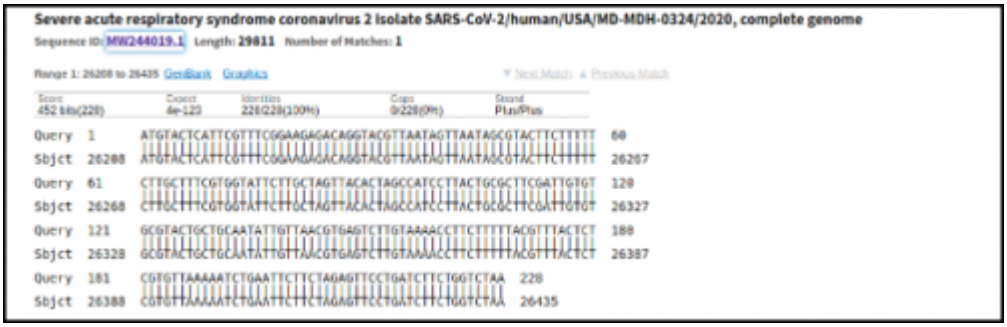
Badacze z Wuhan, stwierdzili, że już skutecznie poskładali sekwencję genetyczną SARS CoV-2, przez dopasowwanie fragmentów znajdujących się w próbkach zawierających inne, uprzednio odkryte, sekwencje genetyczne. Z zebranych materiałów stwierdzili, że 87,1% pasuje do koronawirusa SARS (SARS-Cov). Zastosowali de novo assembly i ukierunkowaną reakcję PCR i znaleźli 29 891 par zasad, które w 79,6% są zgodne z SARS-CoV.

Musieli użyć *de novo assembly,* ponieważ nie mieli wiedzy *a priori* o prawidłowej kolejności lub kolejności tych fragmentów. Po prostu stwierdzenie WHO, że chińscy naukowcy *wyizolowali* wirusa 7 stycznia, jest fałszywe.

Zespół z Wuhan wykorzystał 40 rund amplifikacji RT-qPCR, aby dopasować fragmenty cDNA (uzupełniające się DNA zbudowane z fragmentów RNA z próbek) z opublikowanym genomem koronawirusa SARS (SARS-CoV). Niestety nie jest jasne, jak dokładny jest oryginalny genom SARS-CoV.

W 2003 roku zespół naukowców z Hongkongu przebadał 50 pacjentów z ciężkim ostrym zespołem oddechowym (SARS). Pobrali próbki od 2 z tych pacjentów i opracowali hodowlę w komórkach wątroby płodu małpy.

Stworzyli 30 klonów znalezionego materiału genetycznego. Nie mogąc znaleźć dowodów na istnienie żadnego innego znanego wirusa, tylko w jednej z tych sklonowanych próbek znaleźli sekwencje genetyczne *„nieznanego pochodzenia”.*



Badając te nieznane sekwencje RNA, stwierdzili, że 57% pasują do bydlęcego koronawirusa i mysiego wirusa zapalenia wątroby i

wywnioskowali, że należy do rodziny Coronaviridae. Biorąc pod uwagę te sekwencje, aby sugerować nowo odkryty wirus SARS-CoV (nowe odkrycie to ambrozja dla naukowców), zaprojektowali startery RT-PCR do testowania tego nowego wirusa. Naukowcy stwierdzili:

> *Startery do wykrywania nowego wirusa zaprojektowano do wykrywania RT-PCR tego genomu koronawirusa związanego z zapaleniem płuc u ludzi w próbkach klinicznych. Spośród 44 próbek z jamy nosowo-gardłowej dostępnych od 50 pacjentów z SARS, 22 miało dowody na obecność RNA koronawirusa związanego z zapaleniem płuc u ludzi."*

Połowa badanych pacjentów, którzy mieli te same objawy, uzyskała wynik pozytywny dla tego nowego rzekomego wirusa. Nikt nie wie, dlaczego druga połowa uzyskała wynik negatywny na obecność tego *nowego* wirusa SARS-CoV. Takie pytanie nie padło.

Ten rzekomy wirus miał tylko 57% dopasowanie sekwencji do rzekomo znanego koronawirusa. Pozostałe 43% *„tam"* po prostu było. Zsekwencjonowane dane zostały wyprodukowane i zapisane jako nowy genom GenBank Accession No. AY274119.

Naukowcy z Wuhan następnie znaleźli 79,6% dopasowania sekwencji do AY274119 i dlatego nazwali go nowym szczepem SARS-CoV (2019-nCoV – ostatecznie przemianowanym na SARS-CoV-2). Nikt na żadnym etapie tego procesu nie wyprodukował żadnej wyizolowanej, oczyszczonej próbki żadnego wirusa. Jedyne, co mieli, to dopasowania sekwencji procentowej do innych dopasowań sekwencji procentowej.

Nic nie wyizolowano

Naukowcy są bardzo zirytowani, ponieważ wciąż mówią, że wirus został wyizolowany, ale nikt im nie wierzy. Dzieje się tak, ponieważ jak dotąd nikt nie dostarczył ani jednej oczyszczonej próbki wirusa SARS-CoV-2. Zamiast tego mamy kompletny genom i,

jak za chwilę odkryjemy, nie jest to szczególnie przekonujące.

Dziennikarze śledczy Torsten Engelbrecht i Konstantin Demeter poprosili niektórych naukowców, którzy twierdzili, że mają zdjęcia wirionów SARS-C0V-2, aby potwierdzili, że są to obrazy izolowanego, oczyszczonego wirusa. Żaden z nich tego nie zrobił.

W Australii naukowcy z Instytutu Doherty ogłosili, że *wyizolowali wirusa SARS-CoV-2*. Poproszeni o wyjaśnienie naukowcy powiedzieli:

> *„Mamy krótkie (RNA) sekwencje z testu diagnostycznego, które można wykorzystać w testach diagnostycznych"*

To wyjaśnia, dlaczego rząd Australii oświadczył:

> *Wiarygodność testów COVID-19 jest niepewna ze względu na ograniczoną bazę dowodów… Dostępne są ograniczone dowody pozwalające ocenić dokładność i użyteczność kliniczną dostępnych testów COVID-19".*

W Wielkiej Brytanii w lipcu grupa zaniepokojonych naukowców napisała list do premiera Wielkiej Brytanii Borisa Johnsona, w którym poprosili go o aby:

> *Przedstawić niezależnie recenzowane dowody naukowe potwierdzające, że wirus Covid-19 został wyizolowany."*

Do tej pory nie otrzymali odpowiedzi.

Podobnie brytyjski badacz Andrew Johnson złożył wniosek o wolność informacji do Public Health England (PHE). Poprosił ich o dostarczenie mu swoich danych opisujących izolację wirusa SARS-COV-2. Na co odpowiedzieli:

> *PHE może potwierdzić, że nie zawiera informacji w sposób sugerowany w Twojej prośbie".*

Kanadyjska badaczka Christine Massey wystąpiła z podobną prośbą o ujawnienie informacji, prosząc o to samo kanadyjski rząd. Na co odpowiedział rząd Kanady:

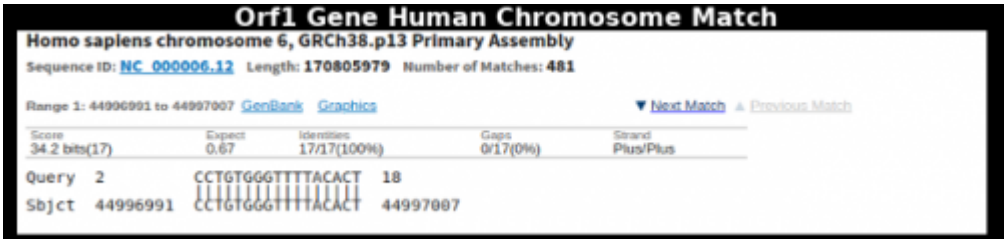
> *Po dokładnym wyszukiwaniu z przykrością informujemy, że nie mogliśmy znaleźć żadnych danych odpowiadających na Państwa żądanie".*

CDC w USA oświadczyło w RT-PCR Diagnostic Panel:

> *… Obecnie nie są dostępne ilościowo określone izolaty wirusa 2019-nCoV …… ..Wykrycie wirusowego RNA może nie wskazywać na obecność zakaźnego wirusa lub że 2019-nCoV jest czynnikiem wywołującym objawy kliniczne."*

Ostatnia aktualizacja 13 lipca 2020 r., CDC jeszcze nie pozyskała czystej próbki wirusa od jakiegokolwiek pacjenta, u którego stwierdzono chorobę COVID-19. Otwarcie przyznają, że ich testy niekoniecznie pokazują, czy SARS-CoV-2 jest obecny lub powoduje COVID 19.

Powiedziano nam, że nic z tego nie ma znaczenia. Że jesteśmy ignorantami i po prostu nie rozumiemy wirusologii. Dlatego musimy przyjąć obrazy rzeczy, o których wiemy, że mogą być czymś innym, a sekwencje genetyczne (które mogą być czymś innym) jako ostateczny dowód, że ten wirus i choroba, którą ma wywoływać, są prawdziwe.



Testowanie po nic

WHO i każdy rząd, think tank, komitet sterujący polityką, rządowy doradca naukowy, instytucje ponadnarodowe i inne

osoby, które promują oficjalną narrację o COVID-19, zapewniają, że SARS-CoV-2 powoduje COVID-19.

Chociaż nikt nigdy nie wyprodukował próbki tego rzekomego wirusa, rzekomy genom SARS-CoV-2 został opublikowany. Jest w domenie publicznej.

Mówi się, że kluczowe sekwencje genetyczne w genomie SARS-CoV-2 mają określone funkcje. Są to białka docelowe, które naukowcy badają, aby *zidentyfikować* obecność *„wirusa”*. Obejmują one:

- Gen polimerazy RNA (Rd-Rp) – umożliwia replikację RNA SARS-CoV-2 w cytoplazmie komórek nabłonka chorych na COVID-19.
- Gen S (Orf2) – ta glikoproteina tworzy kolec na powierzchni wirionu SARS-CoV-2, który rzekomo ułatwia wiązanie SARS-CoV-2 z receptorami ACE2 na komórkach, umożliwiając RNA wewnątrz powłoki białka wirionu (kapsyd) przejście do teraz *zainfekowanej* komórki.
- Gen E (Orf1ab) – małe białko błonowe używane w składaniu wirusa
- Gen N (Orf9a) – gen nukleokapsydu, który wiąże RNA podczas tworzenia kapsydu

WHO prowadzi publicznie dostępny rejestr starterów RT-PCR i sond używanych do testowania SARS-CoV-2. Startery to specyficzne sekwencje nukleotydowe, które wiążą się (łączą) z nicią antysensowną i sensowną zsyntetyzowanego cDNA (nazywane odpowiednio starterami do przodu i do tyłu).

Nici cDNA rozdzielają się po podgrzaniu i przekształcają po schłodzeniu. Przed schłodzeniem sekwencje nukleotydowe zwane sondami są wprowadzane do hybrydyzacji z określonymi regionami docelowymi podejrzanego genomu wirusa. Podczas amplifikacji, gdy obszary między starterami wydłużają się, gdy starter uderza w sondę, sonda rozpada się, uwalniając fluorescent lub barwnik, który następnie może zostać odczytany przez

naukowców.

Naukowcy twierdzą, że to identyfikacja tych markerów dowodzi obecności SARS-CoV-2 w próbce.

Coś innego, co jest publicznie dostępne, to podstawowe narzędzie wyszukiwania lokalnego dopasowania (BLAST). Dzięki temu każdy może porównać opublikowane sekwencje nukleotydów ze wszystkimi zapisanymi w genetycznej bazie danych National Institutes of Health (NIH) Stanów Zjednoczonych o nazwie GenBank. Dlatego możemy BLASTOWAĆ zastrzegane startery SARS-CoV-2, sondy i sekwencje genów docelowych.

Protokoły WHO do przodu i do tyłu oraz protokoły sondy dla rzekomego genomu wirusa SARS-CoV-2 opierają się na profilach genów RdRp, Orf1, N i E. Każdy może przeprowadzić je przez BLAST, aby zobaczyć, co znajdzie.

Istotną sekwencją nukleotydową RdRP, używaną jako starter do przodu, jest – ATGAGCTTAGTCCTGTTG. Jeśli przeprowadzimy nukleotydowy BLAST, jest to rejestrowane jako kompletny *izolat* SARS-CoV-2 ze 100% dopasowaną identycznością sekwencji. Podobnie, odwrotna sekwencja startera genu E – ATATTGCAGCAGTACGCACACA – ujawnia obecność sekwencji Orf1ab, która również *identyfikuje* SARS-CoV-2.

Jednak BLAST umożliwia także przeszukiwanie sekwencji nukleotydów genomów drobnoustrojów i człowieka. Jeśli szukamy sekwencji RdRp SARS-CoV-2, ujawnia ona 99 ludzkich chromosomów ze 100% zgodnością sekwencji. Orf1ab (gen E) zwraca 90 ze 100% identycznością sekwencji z ludzkimi chromosomami.

Robiąc to samo dla tych sekwencji, wyszukując mikroorganizmy, znajdziemy 92 drobnoustroje w 100% zgodne z genem SARS-CoV-2 E i 100 dopasowanych drobnoustrojów o 100% identyczności sekwencji z istotnym genem SARS-CoV-2 RdRp.

Ilekroć sprawdzamy tak zwane unikalne markery genetyczne dla SARS-CoV-2, zapisane w protokołach WHO, znajdujemy pełne lub

wysokoprocentowe dopasowania z różnymi fragmentami ludzkiego genomu. Sugeruje to, że sekwencje genetyczne, które mają identyfikować SARS-CoV-2, nie są unikalne. Może to być wszystko, od sekwencji drobnoustrojów po fragmenty ludzkich chromosomów.

Tak zwane osoby weryfikujące fakty, takie jak projekt *Health Feedback firmy* Reuters, szybko odrzuciły twierdzenia tych, którzy zauważyli widoczny brak specyficzności w rzekomym genomie SARS-CoV-2.

Używając mnóstwa słomianych argumentów, takich jak: *„to twierdzenie sugeruje, że każdy test powinien być pozytywny”* (a tak nie jest), ich próba *obalenia* wygląda *mniej więcej* tak:

> *Startery są zaprojektowane tak, aby wiązały się z określonymi sekwencjami nukleotydów, które są unikalne dla wirusa. Starter do przodu może wiązać się z określonym chromosomem, ale starter do tyłu nie wiąże się z tym samym chromosomem, więc chromosom nie jest obecny w wirusie SARS-CoV-2. Ponadto, ponieważ startery w przód i w tył otaczają sekwencję, która ma być amplifikowana, sekwencja cDMA między starterami jest unikalna dla wirusa.*

Wydaje się to celowo przeinaczać znaczenie tych ustaleń, przedstawiając argument, którego nie wysuwa nikt oprócz samych weryfikatorów faktów. Przeszukiwania BLAST pokazują, że te sekwencje docelowe nie są unikalne dla SARS-CoV-2. Nie trzeba też znajdować wszystkich celów, aby wynik był pozytywny.

Marokańscy naukowcy zbadali epidemiologię rzekomych marokańskich *przypadków* SARS-CoV-2. Dziewięć procent było pozytywnych dla trzech genów, osiemnaście procent było pozytywnych dla dwóch genów, a siedemdziesiąt trzy procent dla jednego. Jak przed chwilą omówiliśmy, wiele mogło być pozytywnych dla żadnego.

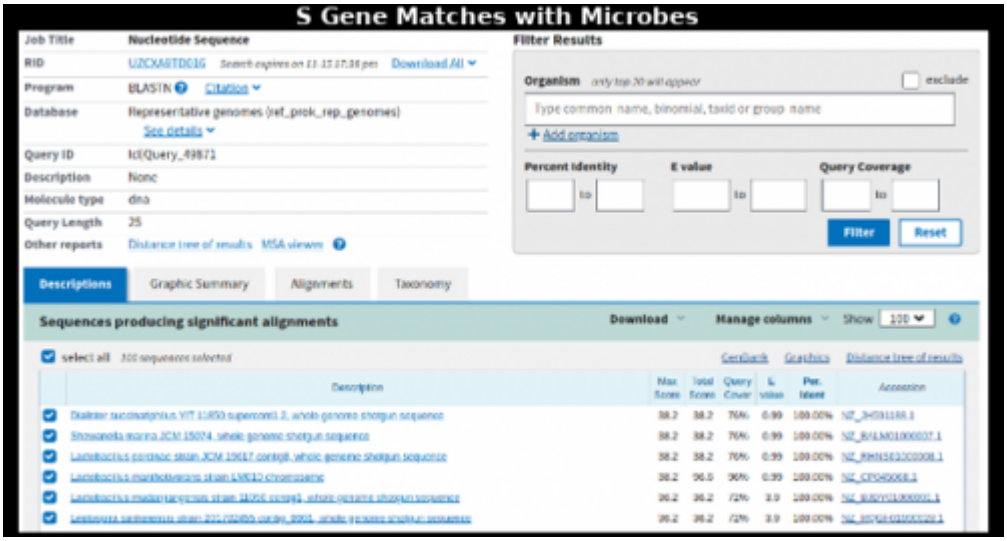
Jest to całkowicie zgodne z wytycznymi dotyczącymi testów WHO.

Stwierdzają:

„Optymalna diagnoza obejmuje NAAT [test amplifikacji kwasu nukleinowego] z co najmniej dwoma niezależnymi od genomu celami SARS-CoV-2; jednakże na obszarach, gdzie transmisja jest powszechna, można zastosować prosty algorytm pojedynczego celu… Jeden lub więcej negatywnych wyników niekoniecznie wyklucza zakażenie SARS-CoV-2.”

Bez względu na fałszywe argumenty dobrze finansowanych *weryfikatorów faktów,* jeśli startery do przodu i do tyłu identyfikują śmieci, być może jeden jest fragmentem chromosomu, a drugi sekwencją drobnoustrojów, wówczas wzmocniony region między nimi jest prawdopodobnie również śmieciami.

Argument, że RT-PCR znajduje tylko RNA, jest zwodniczy. Naturalna transkrypcja (oddzielenie nici DNA) zachodzi podczas ekspresji genów. Nikt nie mówi, że całe chromosomy lub mikroby są sekwencjonowane w rzekomym genomie SARS-CoV-2. Choć mogą, z tego, co wiemy. Mówią, że rzekome markery używane do testowania tego rzekomego wirusa nie nadają są odpowiednie.



Testy RT-PCR nie sekwencjonują całego genomu. Poszukują przypadków specyficznej fluorescencji sondy, aby wskazać obecność sekwencji, o których mówi się, że istnieją. Sekwencje te są zdefiniowane w MN908947.1 i kolejnych aktualizacjach. Te

startery i sondy nie mogą ujawnić niczego poza dopasowaniami RNA wyekstrahowanymi z niekodującego, czasami nazywanego *„śmieciowym”* DNA (cDNA).

Na przykład gen SARS-CoV-2 S ma być wysoce specyficzny dla genomu wirusa SARS-CoV-2. Sekwencja docelowa to – TTGGCAAAATTCAAGACTCACTTTC. Wyszukiwanie mikrobiologiczne BLAST zwraca 97 dopasowań drobnoustrojów ze 100% zgodnością sekwencji. Najniższe dopasowanie procentowe tożsamości, w pierwszej setce, to 95%. Ludzki genom BLAST również znajduje 100% dopasowanie sekwencji do 86 fragmentów ludzkich chromosomów.

Bez względu na to, gdzie spojrzysz w rzekomym genomie SARS-CoV-2, w protokołach testowych WHO nie ma nic, co jasno identyfikuje, co to jest. Cały genom może być fałszywy. Testy nie dowodzą istnienia SARS-CoV-2. Odsłaniają jedynie zupę nieokreślonego materiału genetycznego.

Jeśli tak, ponieważ nie ma wyizolowanych ani oczyszczonych próbek wirusa bez wykonalnego testu, nie ma dowodów na istnienie SARS-CoV-2. Dlatego nie ma żadnych dowodów na istnienie choroby zwanej COVID-19.

Oznacza to, że nie ma podstaw naukowych do jakichkolwiek twierdzeń dotyczących liczby przypadków COVID-19, przyjęć do szpitali lub wskaźników śmiertelności. Wszystkie środki podjęte w celu *zwalczania* tego *śmiercionośnego wirusa* są prawdopodobnie oparte na niczym.

Ostateczne oszustwo

Oszustwo to przestępstwo. Prawną definicją oszustwa jest:

„Jakaś podstępna praktyka lub umyślna sztuczka, której celem jest odebranie komuś prawa lub wyrządzenie mu krzywdy”.

Prawna definicja spisku to:

„Połączenie lub konfederacja między dwiema lub więcej osobami

utworzonymi w celu popełnienia, wspólnym wysiłkiem, jakiegoś czynu niezgodnego z prawem lub przestępstwa"

Wydaje się, że ci, którzy twierdzą, że mamy do czynienia z pandemią, nie dostarczyli żadnych dowodów na to, że wirus o nazwie SARS-CoV-2 wywołuje chorobę zwaną COVID-19. Wszystkie informacje silnie sugerujące taką możliwość są łatwo dostępne w domenie publicznej. Każdy może to przeczytać.

Aby nastąpiło oszustwo, oszustwo musi być umyślne. Intencją musi być celowe pozbawienie innych ich praw lub zranienie ich w inny sposób. Jeśli istnieją dowody zmowy między osobami i organizacjami w celu popełnienia oszustwa, jest to spisek (w jurysdykcjach prawa zwyczajowego) lub wspólne przedsiębiorstwo przestępcze (JCE) na mocy prawa międzynarodowego.

Wygląda na to, że COVID-19 był celowo wykorzystywany jako *casus belli* do prowadzenia wojny z ludzkością. Zostaliśmy uwięzieni we własnych domach, nasza wolność przemieszczania się została ograniczona, wolność słowa i wypowiedzi została ograniczona, prawa do protestowania zostały ograniczone, oddzieloni od bliskich, firmy zniszczone, zbombardowani psychicznie, w kagańcach i terroryzowani.

Co gorsza, chociaż nie ma dowodów na *bezprecedensową* śmiertelność ze wszystkich przyczyn, odnotowano *bezprecedensowy* wzrost liczby zgonów. Są one ściśle powiązane z lockdownami, które doprowadziły do wycofania świadczeń zdrowotnych, za które płacimy, i zmiany orientacji publicznych usług zdrowotnych na leczenie jednej domniemanej choroby z wyłączeniem wszystkich innych.

Ponadto ci, którzy przekazali historię COVID-19, sugerują, że ta domniemana choroba stanowi uzasadnienie dla całkowitej restrukturyzacji światowej gospodarki, naszych systemów politycznych, społeczeństw, kultur i samej ludzkości.

Dopuszczenie do udziału w ich tzw. *„nowej normalności",* która jest hurtowym przekształceniem całego naszego społeczeństwa

bez naszej zgody, nalegają, abyśmy podporządkowali się ich warunkom.

Obejmują one między innymi biometryczny nadzór nad wszystkimi, scentralizowaną kontrolę i monitorowanie wszystkich naszych transakcji, opresyjne ograniczenia biznesowe i społeczne oraz skuteczne żądanie, abyśmy nie mieli prawa do suwerenności nad naszymi własnymi ciałami. Stanowi to warunek niewolnictwa.

Nie ma wątpliwości, że zostaliśmy pozbawieni naszych praw i zranieni. Dowody na to, że szkoda została celowo spowodowana przez międzynarodową konspirację, są przytłaczające. Niszczycielska polityka, prowadzona przez rządy na całym świecie, najwyraźniej wywodzi się z globalistycznych think tanków i ponadnarodowych instytucji na długo przed pojawieniem się tej nieistniejącej pandemii.

W jurysdykcjach Kodeksu Napoleona domniemywa się winy. Aby oskarżeni spiskowcy udowodnili swoją niewinność, muszą wykazać, że pomimo swoich niezmierzonych zasobów zbiorowo nie byli w stanie uzyskać dostępu ani zrozumieć żadnego z ogólnie dostępnych dowodów sugerujących, że COVID-19 jest mitem.

Osoby odpowiedzialne za przestępstwo spisku w celu popełnienia globalnego oszustwa powinny być sądzone. Jeśli zostaną uznani za winnych, powinni zostać uwięzieni, podczas gdy reszta z nas będzie próbowała naprawić szkody, które już wyrządzili.

Pekin wykorzystuje pandemię koronawirusa do rozbudowy

aparatu nadzoru internetowego

Według raportu Freedom House, Pekin wykorzystuje pandemię koronawirusa w Wuhan (COVID-19) jako uzasadnienie rozszerzenia i zintensyfikowania i tak już gigantycznych systemów nadzoru internetowego.

W swoim corocznym raporcie Freedom of the Net, w którym szczegółowo opisano stan nadzoru cyfrowego w ponad 60 krajach, organizacja non-profit umieściła Chiny na ostatnim miejscu z wynikiem 10 na 100. To szósty rok z rzędu, w którym kraj ten został ukoronowany jako „najgorszy gwałciciel wolności w internecie" na świecie.

> *„Ta pandemia normalizuje rodzaj cyfrowego autorytaryzmu, który Komunistyczna Partia Chin (KPCh) od dawna stara się wprowadzić do głównego nurtu" – napisał Freedom House w oświadczeniu.*

Według raportu, chińskie władze wdrożyły zarówno niską, jak i zaawansowaną technologię, aby kontrolować swobodny przepływ informacji w Internecie na temat stanu tzw. pandemii koronawirusa w tym kraju. Wykorzystały również te technologie, aby uniemożliwić użytkownikom Internetu przeglądanie niezależnych źródeł wiadomości, które kwestionują oficjalną narrację KPCh.

Freedom House zauważył również, że na początku tzw. pandemii Chiny próbowały bagatelizować i ignorować ostrzeżenia lekarzy dotyczące pierwotnego wybuchu koronawirusa w Wuhan. Odkryli również, że mniej użytkowników internetu w Chinach z

powodzeniem omija krajową Wielką Zaporę Sieciową, zwłaszcza po zaostrzeniu przez Pekin ograniczeń dotyczących osób korzystających z wirtualnych sieci prywatnych w celu uzyskania dostępu do zablokowanych witryn.

W raporcie stwierdza się ponadto, że tylko w pierwszym kwartale 2020 r. Chińska Administracja Cyberprzestrzeni, główny regulator internetowy w kraju, zamknęła 816 stron internetowych i usunęła ponad 33000 kont i grup na zatwierdzonych witrynach społecznościowych, takich jak Renren, Weibo i WeChat.

Masowa ekspansja wysiłków w zakresie inwigilacji Internetu w tym kraju spowodowała również wzrost liczby „fabryk cenzury". W tych miejscach pracy znajdują się tysiące cenzorów internetowych, którzy zamiatają przestrzenie internetowe kraju za pomocą technologii sztucznej inteligencji.

Chiny nie są jedynym krajem wykorzystującym COVID-19 do uzasadnienia ekspansji możliwości nadzoru internetowego. Zarówno podmioty państwowe, jak i niepaństwowe wdrażają nowe technologie, które w dowolnym momencie przed globalną pandemią byłyby uważane za zbyt inwazyjne.

Pozostałe kraje, które dołączają do Chin w pierwszej piątce, to Iran, Syria, Kuba i Wietnam. Pięć najlepszych krajów to Islandia, Estonia, Kanada, Niemcy i Wielka Brytania. Tajwan nie został uwzględniony w rankingu pomimo tego, że był znany jako drugi najbardziej wolny kraj w Azji.

Technologia nadzoru przeciw dysydentom jest wdrażana jako instrumenty „zdrowia publicznego"

Sarah Cook, starszy badacz w Freedom House, twierdzi, że wiele nowych chińskich technologii inwigilacji zostało po raz pierwszy opracowanych w celu ochrony kraju przed dysydentami. W szczególności Cook zauważa, że technologia opracowana przeciwko Ujgurom i innym mniejszościom muzułmańskim w Xinjiangu rośnie obecnie w innych częściach

kraju.

Jedną z takich technologii przeciwdziałania dysydentom jest urządzenie przenośne, którego władze mogą używać do skanowania smartfonów ludzi i pobierania z nich danych bez zgody właściciela.

> *„Rząd Chin już teraz korzysta z najbardziej wyrafinowanego i wielowarstwowego aparatu cenzurującego i kontrolującego Internet na całym świecie" – powiedziała Cook.*

Istniejąca technologia nadzoru przeciwko dysydentom jest również udoskonalana na potrzeby epoki pandemii. W marcu, kiedy koronawirus dopiero zaczynał rozprzestrzeniać się po całym świecie, Chiny były już bliskie ulepszenia swojej technologii rozpoznawania twarzy w celu identyfikacji osób noszących maski.

Inne technologie, zarówno stare, jak i nowe, są również wykorzystywane do naruszania prywatności obywateli Chin, na przykład zmuszając ludzi do korzystania z aplikacji, która śledzi infekcje i zmuszając ludzi do umieszczania kamer internetowych w ich domach i poza ich drzwiami, aby śledzić ich ruchy. Cook twierdzi, że te systemy mają tylne drzwi, które pozwalają policji nadzorować ludzi, kiedy tylko zechcą.

Według Cooka rozprzestrzenianie się pandemii jest bezpośrednio związane z ekspansją kontroli KPCh nad mową w Internecie.

Warto zadać sobie pytanie: jak się ma sytuacja w Polsce, jeżeli chodzi o aplikacje nadzorujące osoby objęte kwarantanną…?

Źródła:

TheEpochTimes.com

VOANews.com

TaiwanNews.com.tw 1

FreedomHouse.org

TaiwanNews.com.tw 2

FT.com

Australijska policja może porywać ludzi z powodów medycznych i pozbywać się wszystkiego „łącznie z bielizną”, aby na siłę podawać szczepionki

Artykuł został zarchiwizowany. Znajdziesz go w poniższym linku.

Archiwum

California zakazuje stosowania technologii rozpoznawania twarzy w nagraniach z kamer policjantów

California może mieć wiele wątpliwych praw, ale jest takie, które zasługuje na aplauz. Zabrania stosowania technologii rozpoznawania twarzy w nagraniach wykonanych przez kamery funkcjonariuszy policji.

Rozpoznawanie twarzy to technologia, która polega na dopasowywaniu w czasie rzeczywistym obrazu osoby do jej poprzedniego zdjęcia. Opiera się na fakcie, że twarz każdej osoby ma około 80 unikalnych punktów węzłowych w obszarach nosa, ust, policzków i oczu, które można wykorzystać do odróżnienia ludzi od siebie.

Cyfrowa kamera wideo służy do pomiaru odległości między tymi punktami na twarzy osoby. Obejmuje między innymi pomiary głębokości oczodołów, odległości między oczami, kształtem linii żuchwy i szerokości nosa. Informacje te służą do tworzenia unikalnego kodu numerycznego, który można dopasować do kodu pobranego z poprzedniego zdjęcia.

W marcu Waszyngton stał się pierwszym stanem w kraju, który zalegalizował używanie rozpoznawania twarzy przez organy ścigania i inne agencje stanowe. Oprogramowanie było już

używane na poziomie hrabstwa i miasta przed wprowadzeniem tam nowego prawa. Jednak rozpoznawanie twarzy może być używane tylko w niektórych przypadkach, takich jak poszukiwanie zaginionych osób lub identyfikacja zwłok. Agencje będą zobowiązane do złożenia zawiadomienia o zamiarze użycia systemu zanim go użyją, a także raportu dotyczącego odpowiedzialności.

Jeśli chodzi o ruch Waszyngtonu, American Civil Liberties Union stwierdziła, że zamiast zabezpieczyć wykorzystanie rozpoznawania twarzy, grozi legitymizacją jego rozszerzenia. Kierownik projektu ACLU Jennifer Lee powiedziała, że prawo zawiera język, który pozwala agencjom na używanie rozpoznawania twarzy do odmawiania ludziom podstawowych potrzeb i innych niezbędnych rzeczy, takich jak mieszkanie, jedzenie, woda i opieka zdrowotna.

Zwolennicy prywatności chwalą ustawę CA.

Zwolennicy prywatności wyrazili ulgę, że ustawa kalifornijska została podpisana przez gubernatora Gavina Newsoma. Dotyczy to nie tylko rozpoznawania twarzy, ale także ogólnie nadzoru biometrycznego, takiego jak analiza chodu z wykorzystaniem materiału filmowego, który można zebrać z materiału wideo z kamery policyjnej.

W projekcie ustawy stwierdza się: „Korzystanie z rozpoznawania twarzy i innego nadzoru biometrycznego jest funkcjonalnym odpowiednikiem wymagania od każdej osoby, aby zawsze okazywała dowód tożsamości ze zdjęciem, co stanowi naruszenie uznanych praw konstytucyjnych. Ta technologia umożliwia również śledzenie osób bez pozwolenia”.

Posunięcie to nastąpiło niedługo po tym, jak ACLU przeprowadziło badanie rozpoznawania twarzy, które wykazało, że program Amazon błędnie zidentyfikował ponad dwa tuziny kalifornijskich prawodawców jako przestępców.

Podobny zakaz został wprowadzony kilka miesięcy wcześniej

przez San Francisco w związku z wykorzystywaniem przez rząd funkcji rozpoznawania twarzy do nadzoru, kilka innych amerykańskich miast zrobiło to samo.

Chiny mają przeciwny pogląd na technologię rozpoznawania twarzy, w pełni ją wykorzystując do śledzenia swoich obywateli. Służy również do tworzenia wyników społecznych, które dają tym, którzy są posłuszni KPCh, pewne korzyści w ich codziennym życiu i ograniczają ruch i wolności tych, których wyniki są niższe.

Niestety nowe prawo Kalifornii dotyczy tylko korzystania z tej technologii przez organy ścigania, a nie sektor prywatny. Niemniej jednak jest to krok we właściwym kierunku, o wiele więcej, niż możemy powiedzieć o wielu innych prawach pochodzących z Kalifornii .

Źródła:

DailyMail.co.uk

Mashable.com

NaturalNews.com

Armia USA rozpoczyna testy latających balonów obserwacyjnych w całym kraju, aby śledzić ruchy ludzi

Wojsko USA testowało balony, które mogą szpiegować ludzi i śledzić ich ruchy. Zgodnie z dokumentami złożonymi w FCC balony mogą unosić się na wysokości 65 000 stóp. W zeszłym roku zostały przetestowane w stanach takich jak Iowa, Missouri, Illinois, Wisconsin, Minnesota i Południowa Dakota.

Testy zostały przeprowadzone przez US Southern Command, czyli Southcom, które jest częścią Departamentu Obrony i odpowiada za operacje wywiadowcze, współpracę w zakresie bezpieczeństwa i reagowanie na katastrofy w Ameryce Środkowej i Południowej. Jest to wspólny wysiłek US Air Force, US Navy, US Army i innych sił, których głównym zadaniem jest znalezienie i przechwycenie transportów narkotyków, które są przeznaczone dla USA. Według the Guardian, aż 25 bezzałogowych zasilanych energią słoneczną balonów rozpoczęto lot od obszarów wiejskich w Dakocie Południowej i pokonaó 250 mil przez sąsiednie stany.

Zgodnie z dokumentami FCC, balony mają na celu zapewnienie stałego nadzoru, który może wykryć i powstrzymać handel narkotykami oraz zagrożenia dla bezpieczeństwa wewnętrznego. Balony są wyposażone w czułą technologię radarową, która może śledzić pojazdy przy każdej pogodzie, w dzień i w nocy. Tylko jedno z urządzeń radarowych w tych balonach może uchwycić ruch wszystkich samochodów podróżujących w promieniu 25 mil.

Oznacza to, że wojsko może śledzić ruch pojazdów a co za tym idzie także ruch ludzi. Technologię tę porównuje się do „walki TiVo”, ponieważ kiedy coś się wydarzy na obserwowanym obszarze, kontrolujący go mogą cofnąć się w czasie i zobaczyć, co się stało, kto był zaangażowany w incydent i jaka była przyczyna.

Sieć MESH jest również wykorzystywana, aby umożliwić balonom komunikację między sobą oraz z ludźmi na ziemi. Raport wskazuje również, że balony mogą być w stanie nagrywać lub transmitować wideo.

Balony budzą wiele obaw dotyczących prywatności

Oczywiście ten rodzaj nadzoru jest niezwykle niepokojący dla obrońców praw obywatelskich. Starszy analityk American Civil Liberties Union, Jay Stanley, powiedział w the*Guardian* : „Nawet podczas testów wciąż zbierają wiele danych na temat Amerykanów [jadących] do domu związkowego, kościoła, meczetu, kliniki… Nie powinniśmy iść w kierunku dopuszczenia tego do użytku w Stanach Zjednoczonych, niepokojące jest też to, że testy te są przeprowadzane przez wojsko”.

Southcom już używa lekkich samolotów wyposażonych w czujniki do przelotów nad częściami Panamy, Kolumbii, Meksyku i Morza Karaibskiego. Jednak samoloty te mogą latać tylko przez kilka godzin i wymagają kosztownych załóg. Nowe balony są tańszą opcją, mogą podążać za wieloma łodziami i samochodami przez dłuższy czas i łatwiej im zawisnąć na jakiś czas nad określonym obszarem.

Wojsko nie jest jedyną grupą testującą tego typu nadzór; Prywatne firmy, takie jak World View, również pracują nad podobnymi balonami. Stratollites to systemy nadzoru zamontowane w balonach, którymi można zdalnie sterować i regulować. Balon World View wykonał w zeszłym roku 16-dniową misję w zachodnich Stanach Zjednoczonych – o czym wielu na ziemi nie wiedziało.

World View twierdzi, że jego Stratollites mogą być wykorzystywane do zastosowań, takich jak pomoc w nadzorze żołnierzy, prognozowanie pogody, komunikacja i 'pierwszej odpowiedzi’, a także mogą być używane przez organy ścigania.

Chociaż nikt nie chce widzieć narkotyków przedostających się do kraju, wielu Amerykanów czuje się niekomfortowo, na myśl o

byciu śledzonym, rejestrowaniu i potencjalnym przechowywaniu każdego ich ruchu, dostęp do tych danych jest narażony na ataki hakerów. Większość ludzi nawet nie zdaje sobie sprawy ze wszystkich sposobów, na jakie każdego dnia tracimy coraz więcej naszej prywatności dzięki nowoczesnej technologii, która ma poprawiać jakość naszego życia.

Źródła:

DailyMail.co.uk

TheGuardian.com