Droga do cyfrowych mandatów identyfikacyjnych: Jak regulacja mediów społecznościowych może zmienić prywatność online

W szybko zmieniającym się krajobrazie cyfrowym, dążenie do zaostrzenia przepisów dotyczących mediów społecznościowych zyskuje na popularności w całych Stanach Zjednoczonych. Connecticut, Nebraska i Utah znajdują się w czołówce tego ruchu, z proponowanymi przepisami, które mają na celu ograniczenie wpływu mediów społecznościowych na nieletnich. Chociaż środki te są określane jako niezbędne kroki w celu ochrony dzieci, stanowią one również znaczącą zmianę w kierunku obowiązkowych cyfrowych systemów identyfikacji. Zmiana ta może mieć daleko idące konsekwencje dla prywatności w Internecie i wolności osobistej, rodząc krytyczne pytania o przyszłość Internetu.

Connecticut: Ukierunkowanie algorytmów i nakładanie ograniczeń czasowych

Connecticut’s House Bill 6857, zatytułowany „An Act Concerning the Attorney General’s Recommendations Regarding Social Media

and Minors”, jest jednym z najbardziej ambitnych projektów regulacji treści w mediach społecznościowych dla młodych użytkowników. Prokurator generalny William Tong, głośny zwolennik ustawy, argumentuje, że platformy mediów społecznościowych celowo wykorzystują algorytmy uczenia maszynowego, aby utrzymać zaangażowanie użytkowników, zwłaszcza dzieci. „Algorytmy te analizują zachowanie użytkowników, aby dostarczać im coraz bardziej atrakcyjne treści, co moim zdaniem jest szczególnie szkodliwe dla dzieci” – twierdzi Tong.

Jeśli ustawa HB6857 zostanie przyjęta, nałoży ona kilka rygorystycznych środków:

Rekomendacje algorytmiczne: Zakaz rekomendacji treści opartych na algorytmach dla nieletnich, chyba że rodzic wyraźnie wyrazi na to zgodę.
Ograniczenia czasowe: Zablokowanie dostępu do mediów społecznościowych dla dzieci między północą a 6 rano i nałożenie dziennego limitu użytkowania wynoszącego jedną godzinę.
Zgoda rodziców: Wymaganie od rodziców podjęcia aktywnej decyzji dotyczącej dostępu ich dziecka do algorytmów, upewniając się, że wiąże się to z czymś więcej niż zwykłą zgodą na kliknięcie.
Tong podkreśla znaczenie zaangażowania rodziców: „Jeśli pojedynczy rodzic zdecyduje, że chce, aby jego dziecko miało dostęp do algorytmów, że może sobie z tym poradzić, może to zrobić, ale musi podjąć taką decyzję”.

Pomimo tych intencji, ustawa uznaje również wyzwania związane ze skuteczną weryfikacją wieku. Tong odrzuca pogląd, że gigantom mediów społecznościowych brakuje zasobów, aby wdrożyć solidne środki weryfikacji wieku: „To do tych firm, które każdego roku zarabiają biliony dolarów na nas wszystkich, należy wymyślenie, jak skutecznie blokować wiek, weryfikować wiek młodych ludzi i weryfikować zgodę rodziców. Wiemy, że samo umieszczenie strony z napisem „Masz 18 lat czy nie?” i

kliknięcie „Tak” lub „Nie” nie wystarczy. To nie wystarczy”.

Nebraska: Rozszerzenie wymagań dotyczących cyfrowego dokumentu tożsamości

Nebraska LB383, ustawa o prawach rodzicielskich w mediach społecznościowych, przyjmuje podobne, ale odmienne podejście. Ustawa nakłada na firmy zajmujące się mediami społecznościowymi obowiązek wdrożenia „rozsądnej weryfikacji wieku” w celu zablokowania nieletnim dostępu do platform bez zgody rodziców. Według Unicameral Update, akceptowalne metody weryfikacji obejmują cyfrowe identyfikatory i zewnętrzne usługi uwierzytelniania wieku. Podmioty te byłyby zobowiązane do usunięcia danych osobowych po weryfikacji, ale ustawa nadal budzi obawy co do ilości danych osobowych, które użytkownicy muszą podać.

Prokurator generalny Mike Hilgers postrzega zaangażowanie w mediach społecznościowych jako skalkulowany model biznesowy: „To nie są przypadkowe algorytmy, które przypadkowo przyciągają dzieci. Są one zaprojektowane, ponieważ jednymi z najbardziej lukratywnych klientów, jakich można znaleźć w tym obszarze, są dzieci”. Pomimo zapewnień o usuwaniu danych, krytycy ostrzegają, że przepisy te mogą stanowić precedens dla szerszych wymagań dotyczących cyfrowej identyfikacji, potencjalnie zmniejszając anonimowość w Internecie.

Utah: Odpowiedzialność App Store i kontrola rodzicielska

Ustawa Senatu Utah nr 142 (SB142), czyli App Store Accountability Act, przenosi punkt ciężkości na sklepy z aplikacjami. Ustawa wymagałaby od sklepów z aplikacjami weryfikacji wieku użytkownika przed zezwoleniem na pobieranie.

Jeśli użytkownik jest niepełnoletni, jego konto musiałoby być powiązane z kontem rodzica, a rodzice weryfikowaliby jego tożsamość – potencjalnie za pomocą karty kredytowej – przed udzieleniem dostępu.

Mechanizm egzekwowania prawa w SB142 jest szczególnie agresywny. Nieprzestrzeganie przepisów byłoby klasyfikowane jako „zwodnicza praktyka handlowa” zgodnie z prawem stanu Utah, dając rodzicom prawo do podjęcia kroków prawnych przeciwko dostawcom sklepów z aplikacjami. Przepis ten podkreśla nacisk ustawy na kontrolę rodzicielską i odpowiedzialność.

Szersze implikacje ekspansji cyfrowego ID

Podczas gdy ustawy te są rzekomo ukierunkowane na ochronę dzieci, stanowią one również znaczący krok w kierunku bardziej monitorowanej i kontrolowanej przestrzeni cyfrowej. Cyfrowe systemy identyfikacji, niezależnie od tego, czy są to identyfikatory wydawane przez rząd, karty kredytowe czy usługi weryfikacji stron trzecich, mogą zasadniczo zmienić internet. Krytycy twierdzą, że gdy kontrole tożsamości staną się standardem, mogą one wykroczyć poza media społecznościowe, utrudniając anonimowy dostęp online.

Joel R. McConvey, pisząc dla jednego z serwisów technologicznych, podkreśla globalny trend w kierunku weryfikacji wieku. „W ciągu ostatnich dwunastu miesięcy weryfikacja wieku dla treści online zmieniła się ze stosunkowo niszowej kwestii w priorytetowy punkt programu dla rządów, aktywistów i największych nazwisk w branży technologicznej”. Tendencja ta jest widoczna w różnych działaniach legislacyjnych, od brytyjskich wytycznych Ofcom po trwające testy technologii weryfikacji wieku w Australii.

Google i Meta, dwie największe firmy technologiczne, już teraz

skłaniają się ku weryfikacji wieku. Google ogłosiło, że wykorzysta algorytmy uczenia maszynowego do oszacowania wieku użytkowników YouTube, mając na celu zapewnienie odpowiednich do wieku doświadczeń i zabezpieczeń. Meta podobno idzie w ich ślady, testując podobne technologie.

Jednak sytuacja prawna jest złożona. Sędzia federalny w Teksasie tymczasowo zablokował część stanowej ustawy SCOPE, powołując się na obawy dotyczące pierwszej poprawki. Główny radca prawny FIRE Bob Corn-Revere argumentuje: „Stany nie mogą blokować dorosłym możliwości angażowania się w legalne wypowiedzi w imię ochrony dzieci, ani nie mogą powstrzymywać nieletnich przed ideami, które rząd uważa za nieodpowiednie”.

Równoważenie bezpieczeństwa i wolności

Nacisk na regulację mediów społecznościowych w Connecticut, Nebrasce i Utah odzwierciedla rosnące obawy dotyczące wpływu platform cyfrowych na młodych użytkowników. Chociaż środki te mają na celu ochronę dzieci, podnoszą również ważne pytania dotyczące prywatności, wolności osobistej i przyszłości Internetu. W miarę postępu prac nad tymi ustawami debata prawdopodobnie będzie się nasilać, zmuszając decydentów, firmy technologiczne i społeczeństwo do zmagania się z kompromisami między bezpieczeństwem a wolnością w erze cyfrowej.

BEZPRZEWODOWY ŚWIAT: Nowa era inwazyjnego nadzoru

W świecie coraz bardziej połączonym przez technologię, nowe badanie ujawnia niepokojące zjawisko: możliwość wykorzystania Wi-Fi i wież komórkowych do inwigilacji bez wiedzy lub zgody osób fizycznych. Technologia ta, która wykorzystuje promieniowanie bezprzewodowe otoczenia, może zmienić sposób, w jaki myślimy o prywatności i bezpieczeństwie, podnosząc istotne kwestie etyczne i prawne.

Technologia stojąca za zagrożeniem

Badanie, przeprowadzone przez wydział inżynierii na Uniwersytecie w Porto w Portugalii, zostało opublikowane na otwartej stronie naukowej Cornell University, arXiv, 24 stycznia 2025 roku. Naukowcy zaprojektowali system, który wykorzystuje rekonfigurowalną inteligentną powierzchnię (RIS) do manipulowania i kierowania sygnałami Wi-Fi, umożliwiając wykrywanie i renderowanie wizualnych obrazów ludzkiej aktywności z ponad 90% dokładnością.

Fariha Husain, kierownik programu promieniowania elektromagnetycznego (EMR) i sieci bezprzewodowych Children’s Health Defense (CHD), wyjaśniła możliwości tej technologii: „Panele RIS mogą być strategicznie rozmieszczone, aby zoptymalizować odbicie i sterowanie sygnałem bezprzewodowym. W pomieszczeniach można je montować na ścianach, sufitach lub meblach. Na zewnątrz mogą być instalowane na budynkach, latarniach i billboardach reklamowych. Dodatkowo, panele RIS umożliwią inteligentny nadzór miejski poprzez śledzenie ruchu pieszych i pojazdów”.

Implikacje tej technologii są głębokie. Według badań, system

może wykrywać gesty dłoni i monitorować parametry życiowe, takie jak oddech, nawet gdy osoby znajdują się za przeszkodami lub nie współpracują. Naukowcy twierdzą, że ta zdolność stanowi postęp w dziedzinie rozpoznawania aktywności człowieka (HAR) w kontekście komunikacji szóstej generacji (6G).

Kwestie etyczne i dotyczące prywatności

Podczas gdy zwolennicy twierdzą, że technologia RIS może mieć korzystne zastosowania w opiece zdrowotnej i automatyzacji, obrońcy prywatności biją na alarm. W. Scott McCollough, główny prawnik zajmujący się sprawami EMR & Wireless w CHD, podkreślił niebezpieczne implikacje dla masowej inwigilacji: „Przyszłe sieci 6G będą miały wbudowaną funkcjonalność RIS i nie zdziwiłbym się, gdyby nie wdrożyli RIS w przyszłych aktualizacjach 5G. Kilka raportów branżowych i rządowych na temat 6G wprost mówi, że chcą wykorzystać te możliwości do inwigilacji”.

Obawy McCollougha nie są bezpodstawne. Technologia stojąca za badaniem jest podobna do Origin AI, komercyjnej technologii wykrywania Wi-Fi opracowanej przez Raya Liu, byłego wykonawcę Agencji Zaawansowanych Projektów Badawczych Obrony (DARPA). Origin AI może lokalizować ruch z ponad 90% dokładnością i rejestrować wzorce oddechowe, co czyni ją potężnym narzędziem do ochrony domu i automatyzacji. Jednak budzi to również poważne obawy dotyczące prywatności.

Husain zauważył: „Panele RIS mogą być zintegrowane z obiektami i środowiskami bez wiedzy lub zgody osób, co sprawia, że rezygnacja z tej formy nadzoru jest prawie niemożliwa”. Dodała, że „technologia ta stwarza niebezpieczne implikacje dla masowego nadzoru, prywatności i bezpieczeństwa danych”.

Kontekst historyczny i współczesne znaczenie

Rozwój technologii RIS jest częścią szerszego trendu w ewolucji nadzoru. Peter Krapp, profesor filmu i studiów medialnych na Uniwersytecie Kalifornijskim w Irvine, badał wszechobecną naturę nadzoru w erze cyfrowej. Według Krappa, Stany Zjednoczone mają największą liczbę kamer monitorujących na osobę na świecie, a nadzór ten nie ogranicza się do kamer wideo. Telefony komórkowe, GPS, Wi-Fi, Bluetooth i różne aplikacje przyczyniają się do kompleksowego systemu śledzenia.

Krapp wyjaśnił: „Bazy danych mogą korelować dane o lokalizacji ze smartfonów, prywatnych kamer, czytników tablic rejestracyjnych i technologii rozpoznawania twarzy. Organy ścigania mogą śledzić, gdzie jesteś i gdzie byłeś, często bez nakazu. Prywatni brokerzy danych również gromadzą i sprzedają te dane, tworząc w dużej mierze nieuregulowany rynek danych osobowych”.

Historyczny kontekst inwigilacji w Stanach Zjednoczonych jest kluczowy dla zrozumienia współczesnego znaczenia technologii RIS. Od wczesnych dni podsłuchów po współczesną erę cyfrowego śledzenia, równowaga między bezpieczeństwem a prywatnością była kwestią sporną. Środowisko prawne po wyroku w sprawie Roe przeciwko Wade dodało nowe warstwy złożoności, z obawami o to, w jaki sposób dane śledzenia mogą być wykorzystywane w kontekście praw reprodukcyjnych i innych wrażliwych kwestii.

Wnioski: Wezwanie do regulacji

W miarę jak technologia RIS rozwija się i staje się coraz bardziej zintegrowana z sieciami 6G, potrzeba solidnych regulacji i wytycznych etycznych jest bardziej krytyczna niż kiedykolwiek. Husain i McCollough opowiadają się za ściślejszym nadzorem i kampaniami uświadamiającymi

społeczeństwo, aby zapewnić, że technologia ta nie narusza prywatności i bezpieczeństwa danych osobowych.

McCollough podsumował: „Musimy przeprowadzić krajową rozmowę na temat etycznych implikacji technologii RIS. Nie chodzi tylko o techniczną wykonalność; chodzi o ramy moralne i prawne, które będą regulować jej użycie”.

W świecie, w którym technologia może przekształcić przedmioty codziennego użytku w narzędzia nadzoru, walka o prywatność jest daleka od zakończenia. Ponieważ technologia ta nadal ewoluuje, ważne jest, aby prawodawcy, technolodzy i obywatele współpracowali w celu ochrony podstawowego prawa do prywatności w erze cyfrowej.

Wielka Brytania żąda od Apple stworzenia globalnego backdoora, zagrażającego prywatności na całym świecie

W oszałamiającym posunięciu, które może na nowo zdefiniować granice prywatności i nadzoru rządowego, Wielka Brytania potajemnie nakazała Apple stworzenie backdoora do zaszyfrowanej pamięci masowej w chmurze, zapewniając brytyjskim władzom bezprecedensowy dostęp do danych

użytkowników na całym świecie. Żądanie to, wydane na mocy kontrowersyjnej brytyjskiej ustawy o uprawnieniach śledczych z 2016 roku – nazwanej „Kartą szpiega” – oznacza znaczącą eskalację w globalnej bitwie o szyfrowanie, prywatność i swobody obywatelskie.

Zamówienie, o którym po raz pierwszy poinformował Washington Post, wymaga od Apple zapewnienia ogólnego dostępu do wszystkich zaszyfrowanych danych użytkowników przechowywanych w chmurze, a nie tylko do kont docelowych. Pozwoliłoby to brytyjskim organom ścigania ominąć zabezpieczenia szyfrowania i uzyskać dostęp do poufnych informacji, w tym zdjęć, wiadomości i dokumentów, bez wiedzy lub zgody użytkowników.

Dla Apple, firmy, która od dawna broni prywatności użytkowników jako podstawowej wartości, żądanie to stanowi egzystencjalny dylemat: zastosować się do nakazu Wielkiej Brytanii i zdradzić zaufanie użytkowników lub całkowicie wycofać zaszyfrowane usługi przechowywania danych w Wielkiej Brytanii. Źródła zaznajomione ze sprawą sugerują, że Apple prawdopodobnie wybierze to drugie rozwiązanie, ale nie rozwiązałoby to żądania Wielkiej Brytanii dotyczącego dostępu do danych w innych krajach, w tym w Stanach Zjednoczonych.

Niebezpieczny precedens dla prywatności

Według Washington Post, żądanie Wielkiej Brytanii nie ma precedensu w największych demokracjach. W przeszłości firmy technologiczne, takie jak Apple, współpracowały z organami ścigania w indywidualnych przypadkach, na przykład pomagając FBI w uzyskaniu dostępu do iPhone’a terrorysty w 2016 roku. Jednak nakaz Wielkiej Brytanii wykracza daleko poza te ukierunkowane żądania, szukając szerokiego backdoora, który podważyłby szyfrowanie dla wszystkich użytkowników.

„Nie ma powodu, dla którego [rząd] Wielkiej Brytanii miałby

prawo decydować za obywateli całego świata, czy mogą oni korzystać ze sprawdzonych korzyści w zakresie bezpieczeństwa, które wynikają z szyfrowania typu end-to-end” – powiedział Apple brytyjskim prawodawcom w marcu 2024 r., przewidując taki ruch.

Obrońcy prywatności i eksperci ds. cyberbezpieczeństwa potępili działania Wielkiej Brytanii, ostrzegając, że stworzenie tylnych drzwi dla organów ścigania nieuchronnie osłabi szyfrowanie dla wszystkich. „Ważne jest, aby zrozumieć, że każdy rodzaj dostępu tylnymi drzwiami (lub frontowymi drzwiami) dla” dobrych »może być również wykorzystany przez« złych ”- stwierdziła Fundacja Technologii Informacyjnych i Innowacji w raporcie z 2020 roku.

Obawy te nie są hipotetyczne. W 2021 r. były dyrektor FBI Chris Wray argumentował przed Senacką Komisją Sądownictwa, że szyfrowanie utrudnia dochodzenia w sprawie krajowego ekstremizmu, wzywając firmy technologiczne do tworzenia backdoorów, które chronią prywatność, umożliwiając jednocześnie dostęp rządowi. Jednak eksperci wielokrotnie ostrzegali, że taka równowaga jest niemożliwa – każdy backdoor może zostać wykorzystany przez hakerów, autorytarne reżimy lub inne złośliwe podmioty.

Globalne konsekwencje

Jeśli Wielkiej Brytanii uda się zmusić Apple do przestrzegania przepisów, może to wywołać efekt domina, ośmielając inne narody do żądania podobnego dostępu. Kraje takie jak Chiny, które już zablokowały szyfrowane aplikacje do przesyłania wiadomości, takie jak Signal, mogłyby wykorzystać precedens Wielkiej Brytanii do uzasadnienia własnych żądań dotyczących backdoorów. Mogłoby to zmusić Apple do wycofania zaszyfrowanych usług w chmurze na całym świecie, zamiast ryzykować naruszenie prywatności użytkowników.

Brytyjska ustawa o uprawnieniach śledczych, która upoważnia

rząd do zmuszania firm do pomocy w dostępie do danych użytkowników, od dawna jest krytykowana za jej nadmierny zasięg. Krytycy twierdzą, że prawo, które czyni przestępstwem nawet ujawnienie takich żądań, przyznaje rządowi niekontrolowane uprawnienia do inwigilacji.

Apple ma możliwość odwołania się od nakazu Wielkiej Brytanii do tajnego panelu technicznego i sędziego, ale prawo nie zezwala firmie na opóźnienie wykonania nakazu podczas procesu odwoławczego. Pozostawia to Apple niewielkie pole manewru, rodząc pytania o przyszłość szyfrowania i prywatności w erze cyfrowej.

Historia oporu

Stanowisko Apple w kwestii prywatności jest od lat cechą charakterystyczną marki. W 2016 roku firma słynnie opierała się nakazowi rządu USA odblokowania iPhone'a zmarłego terrorysty w sprawie San Bernardino, argumentując, że stworzenie backdoora stworzy niebezpieczny precedens. Podczas gdy Apple ostatecznie poszło na kompromis, opracowując plan skanowania urządzeń użytkowników w poszukiwaniu nielegalnych materiałów, inicjatywa ta została odłożona na półkę po szerokiej reakcji ze strony obrońców prywatności.

Najnowsze żądanie Wielkiej Brytanii grozi wznowieniem tej bitwy, stawiając obawy o bezpieczeństwo narodowe przeciwko podstawowemu prawu do prywatności. Jak zauważył Washington Post, brytyjski nakaz stanowi znaczącą porażkę firm technologicznych w ich trwającej od dziesięcioleci walce o uniknięcie wykorzystania ich jako narzędzi nadzoru rządowego.

Dalsza droga

Domaganie się przez Wielką Brytanię globalnego backdoora do szyfrowanej pamięci masowej Apple w chmurze jest przełomowym momentem w toczącej się debacie na temat prywatności i

bezpieczeństwa. Podczas gdy organy ścigania twierdzą, że szyfrowanie umożliwia przestępcom i terrorystom uniknięcie wykrycia, firmy technologiczne i obrońcy prywatności utrzymują, że osłabienie szyfrowania miałoby daleko idące konsekwencje dla wolności osobistych i cyberbezpieczeństwa.

Podczas gdy Apple rozważa swoje opcje, świat bacznie się temu przygląda. Czy firma podtrzyma swoje zobowiązanie do ochrony prywatności, nawet jeśli oznacza to wycofanie usług z Wielkiej Brytanii? A może skapituluje pod presją rządu, ustanawiając precedens, który może osłabić szyfrowanie na całym świecie?

Jedno jest pewne: wynik tej bitwy ukształtuje przyszłość cyfrowej prywatności na nadchodzące lata. W erze, w której dane są cenniejsze niż kiedykolwiek, stawka nie może być wyższa.

„Dostęp, którego domaga się Wielka Brytania, nie ma precedensu w największych demokracjach" – donosi Washington Post. Jeśli Wielka Brytania odniesie sukces, może nie być ostatnia.

Rząd Wielkiej Brytanii podejmuje poważne kroki w kierunku cyfrowego identyfikatora

Rząd Wielkiej Brytanii uruchomił Office for Digital Identities and Attribute (OfDIA) – cyfrowy organ nadzorujący ID w ramach Departamentu Nauki, Innowacji i Technologii, którego zadaniem jest wspieranie rozwoju rynku cyfrowego ID pod kierownictwem dyrektora generalnego Hannah Rutter.

W ten sposób rząd Partii Pracy podjął działania tam, gdzie porzucił rząd konserwatywny, biorąc pod uwagę, że Biuro zostało po raz pierwszy ogłoszone przez poprzedni rząd w 2022 r., kiedy to miało być „tymczasowym" podmiotem wprowadzającym cyfrowy dowód tożsamości w Wielkiej Brytanii.

„Wygoda" po raz kolejny znajduje się w centrum sposobu, w jaki władze wyjaśniają potrzebę takiego nacisku: Rutter cytuje, że zamiast „mozaiki papierkowej roboty" – i ma na myśli papierkową robotę zarówno od rządu, jak i podmiotów prywatnych – potrzebną dziś jako dowód tożsamości, istnieje „lepszy sposób".

„Cyfrowa tożsamość może ułatwić ludziom życie i odblokować miliardy funtów wzrostu gospodarczego" – powiedziała Rutter, nie podając dalej liczb, które pomogły jej dojść do liczby »miliardów funtów«.

System, za który odpowiada OfDIA, nie obejmuje opracowania rządowego dowodu osobistego i może być używany na zasadzie dobrowolności, kontynuowała.

Rutter odniosła się do jednego z zarzutów dotyczących bezpieczeństwa takich systemów – centralizacji – mówiąc, że system, nad którym pracuje jej biuro, również nie ma scentralizowanej cyfrowej bazy danych.

Jest to pewne przynajmniej na razie – i to potencjalni użytkownicy zdecydują, czy wybrany przez OfDIA model wygląda na bardziej godny zaufania: „Będziesz mógł wybierać spośród szeregu dostawców tożsamości cyfrowej i atrybutów, w oparciu o sektor prywatny i charytatywny”, Rutter starał się ich uspokoić.

Obecnie OfDIA pracuje nad stworzeniem „zaufanego i bezpiecznego rynku tożsamości cyfrowej”, a prace te koncentrują się na pięciu obszarach, począwszy od opracowania i utrzymania tożsamości cyfrowej i ram, a następnie bycia odpowiedzialnym za rejestr akredytowanych organizacji, które spełniają wymagania ram.

Jurysdykcja Urzędu obejmuje jednocześnie wydawanie „znaków zaufania” firmom – obecnie istnieje podobno 49 spełniających jedno z trzech kryteriów. Do tego dochodzi współpraca międzynarodowa, której celem jest zapewnienie interoperacyjności, tj. ponadnarodowej rentowności systemu (systemów).

Izrael zatrudni amerykańską firmę biometryczną do kontroli Palestyńczyków w Strefie Gazy

Izrael zaprezentował w tym tygodniu nowy program „Uber dla stref wojny”, mający na celu rozpoczęcie kontroli, w stylu Holokaustu, każdego Palestyńczyka w Strefie Gazy.

Według doniesień, Izrael planuje wynająć prywatną firmę logistyczną i ochroniarską z siedzibą w USA, aby stworzyć „zamkniętą społeczność” w Strefie Gazy, w której wszyscy Palestyńczycy będą poddawani kontroli biometrycznej w celu zakwalifikowania się do otrzymania pomocy.

Izraelski gabinet wojenny omówił tę propozycję w weekend, planując zatwierdzenie programu „pilotażowego” w ciągu najbliższych dwóch miesięcy. Global Delivery Company (GDC), firma prowadzona przez izraelsko-amerykańskiego biznesmena Mordechaja Kahanę, prowadzi obecnie rozmowy z Izraelem w sprawie prowadzenia programu badań biometrycznych.

Od jakiegoś czasu Izrael rozważa utworzenie tak zwanych „baniek humanitarnych” w północnej Gazie, w tym w obozie dla uchodźców Jabalia i wokół niego, który od trzech tygodni znajduje się pod całkowitym oblężeniem. Izrael nie zezwala na dostarczanie żywności, czystej wody i środków medycznych do Jabalii, co powoduje kryzys humanitarny.

W styczniu Międzynarodowy Trybunał Sprawiedliwości (MTS) wydał tymczasowe orzeczenie, zgodnie z którym Izrael musi podjąć natychmiastowe środki w celu zapewnienia Palestyńczykom mieszkającym w Strefie Gazy podstawowych usług i pomocy humanitarnej. W odpowiedzi Izrael opracował system kontroli biometrycznej jako warunek wstępny otrzymania pomocy.

GDC czerpie zyski z wojny od 14 lat

To sam Kahana wymyślił wyrażenie „Uber dla stref wojennych”, aby opisać swoją działalność nastawioną na zysk. GDC prowadzi tę działalność przez ostatnie 14 lat, podczas których działała i czerpała zyski z pięciu wojen, w tym w Afganistanie, Iraku, Strefie Gazy, Syrii i na Ukrainie.

„Personel pracujący dla naszego podwykonawcy ochrony jest przeszkolony i wyposażony w nieśmiercionośne i śmiercionośne metody kontroli tłumu” – czytamy w komunikacie prasowym GDC z tego tygodnia. „Są przeszkoleni w używaniu śmiercionośnej siły tylko w ostateczności, gdy ich życie jest zagrożone”.

Jeden z byłych najwyższych urzędników GDC, Stuart Seldowitz, jest również byłym urzędnikiem rządu USA, który został oskarżony o przestępstwo z nienawiści po tym, jak znęcał się nad ulicznym sprzedawcą żywności. Chociaż Seldowitz nie pracuje już dla GDC, Kahana mówi, że nadal jest otwarty na współpracę z nim.

Sam Kahana powiedział również kilka niezbyt przyjemnych rzeczy o Palestyńczykach. W listopadzie ubiegłego roku nazwał palestyńsko-amerykańską parlamentarzystkę Rashidę Tlaib „ambasadorem Hamasu w USA”. Kahana żartował również na temat etnicznego oczyszczenia wszystkich Palestyńczyków ze Strefy Gazy i przeniesienia ich do Jordanii.

Inni pracownicy wysokiego szczebla w GDC to byli wysocy rangą izraelscy oficerowie wojskowi oraz byli amerykańscy wojskowi i agenci wywiadu, co oznacza, że operacja jest schematem kompleksu wojskowo-przemysłowego, który z pewnością nie będzie miły dla Palestyńczyków w Gazie.

W maju media donosiły, że Izrael prowadził rozmowy z amerykańskimi firmami ochroniarskimi w sprawie zarządzania przejściem granicznym Rafah na południowej granicy Strefy Gazy z Egiptem. Kilka dni po opublikowaniu tych doniesień, Kahana

napisał na X / Twitterze, że będzie „pomagał w dostawach humanitarnych” w Strefie Gazy, sugerując, że GDC jest jedną z zaangażowanych firm ochroniarskich.

„Przybyliśmy tu z jednym jasnym celem: celem jest zasiedlenie całej Strefy Gazy, nie tylko jej części, nie tylko kilku osiedli, całej Strefy Gazy od północy do południa” – powiedziała Daniella Weiss, liderka Nachali, ortodoksyjnego żydowskiego ruchu osadniczego, który twierdzi, że ma ponad 700 żydowskich rodzin, które chcą osiedlić się w Strefie Gazy.

Weiss zorganizowała niedawno konferencję, na której obiecała uczestnikom, że Palestyńczycy „znikną” ze Strefy Gazy w odpowiednim czasie, umożliwiając Izraelowi przyłączenie tych ziem do siebie.

Ustawa o przejrzystości korporacyjnej – najbardziej agresywny krajowy program szpiegowski od czasów Patriot Act

Na konferencji prasowej 12 sierpnia 1986 r. prezydent Ronald Reagan powiedział: „Dziewięć najbardziej przerażających słów w

języku angielskim brzmi: »Jestem z rządu i jestem tutaj, aby pomóc«".

Słowa te odzwierciedlały powszechną i rosnącą nieufność wobec rządu.

Dziś cytat ten można by zinterpretować w następujący sposób: „Jestem z rządu federalnego, podaj swoje dane osobowe, a dopóki nie przekroczysz linii, zapewnimy ci bezpieczeństwo". Nie jest to tak zwięzłe, ale bardziej prawdziwe niż kiedykolwiek wcześniej.

Do końca tego roku każdy obywatel w Stanach Zjednoczonych będzie musiał przekazać dane osobowe swojej małej firmy, S-corp, LLC, HoA, zarządu, powierników, posiadaczy nieruchomości itp. do bazy danych organów ścigania rządu federalnego, obsługiwanej przez Financial Crimes Enforcement Network (FinCen) w ramach Departamentu Skarbu. Witamy w ustawie o przejrzystości korporacyjnej (CTA).

Prezydent Trump postrzegał tę ustawę jako kolejny sposób, w jaki rząd federalny celuje w klasę średnią i swoich wrogów politycznych. Prezydent Trump zawetował tę niekonstytucyjną ustawę w 2019 r., ale ona powróciła.

W bezprecedensowym akcie nadmiernego zasięgu rząd federalny zmierza do agresywnego gromadzenia danych na temat wszystkich właścicieli małych firm, którzy stanowią trzon amerykańskiej gospodarki, z powodów, które wydają się w najlepszym razie „mętne".

Jedynym celem wydaje się być utworzenie kolejnej nowej bazy danych obywateli do monitorowania, obserwowania i karania. Federalni zmierzają do wdrożenia CTA z prędkością warp i w pozornej całkowitej tajemnicy, ponieważ większość milionów właścicieli małych firm w Stanach Zjednoczonych nie ma pojęcia o istnieniu tego prawa.

Nie informując opinii publicznej, wydaje się, że prawdziwym

zamiarem FinCEN jest „złapanie” milionów właścicieli małych firm na „niezgodności”, aby mogli zostać zbadani i skontrolowani przez Departament Skarbu i ukarani.

Obowiązkowa zgodność z przepisami jest wymagana do 1 stycznia 2025 r., w przeciwnym razie grożą ogromne grzywny i do 2 lat więzienia federalnego.

Po zawetowaniu ustawy przez prezydenta Trumpa, została ona po cichu wepchnięta z powrotem do ustawy o autoryzacji obrony w 2021 roku. I tak, bez słowa dla amerykańskiej opinii publicznej, największy i najbardziej agresywny, bezpodstawny krajowy program szpiegowski w historii Stanów Zjednoczonych został wprowadzony w życie.

Nigdy o tym nie słyszałeś? Dołącz do klubu! Miliony właścicieli małych firm w Stanach Zjednoczonych nie mają pojęcia o istnieniu tego prawa ani o tym, że muszą zapewnić pełną zgodność z nim do 1 stycznia 2025 r., w przeciwnym razie zostaną ukarani wysokimi grzywnami w wysokości 591 dolarów dziennie.

Za niezgłoszenie się do bazy danych organów ścigania FinCen grozi do 2 lat więzienia federalnego.

Jako Brytyjczyk nie jestem obcy rządowej tyranii, ale wciąż mam kilka pytań.

Moje pierwsze pytanie brzmi: dlaczego obywatele USA, którzy nie popełnili żadnego przestępstwa – i gdzie nie ma prawdopodobnego powodu, aby sądzić, że popełnili przestępstwo – są zobowiązani do samodzielnego zgłaszania się do bazy danych organów ścigania, wyłącznie na podstawie tego, że pewnego dnia mogą popełnić przestępstwo?

W 2002 roku był bardzo popularny film zatytułowany „Raport mniejszości”.

Założeniem, o ile pamiętam, jest to, że nie ma już

przestępstw, ponieważ organy ścigania polegają na wykorzystaniu „pre-cogs”, aby przewidzieć, kto popełni przestępstwo, a następnie biuro „pre-przestępczości” aresztuje tę osobę, zanim jeszcze popełni przestępstwo, aby upewnić się, że nie popełni przestępstwa, którego nigdy nie popełnił. Wydaje się to całkowicie rozsądne!

Tak więc oprócz „defundacji policji” i „policji myśli”, mamy teraz policję „przedprzestępczą” mieszczącą się w FinCEN w Departamencie Skarbu. Czy IRS Union, również podlegająca temu samemu Departamentowi Skarbu, nie poparła właśnie Kamali Harris na prezydenta? Co może pójść nie tak?

Czy ktoś pamięta skandal z Lois Lerner z IRS? IRS został zmuszony do przyznania, że w szczególności celował w konserwatywne grupy non-profit w celu dodatkowej kontroli, z zamiarem ukarania i / lub odmowy statusu non-profit w oparciu o kaprysy niewybranej partyjnej biurokracji działającej w Departamencie Skarbu.

IRS został ostatecznie zmuszony do przyznania, że wykorzystywał partyjność polityczną do atakowania Amerykanów i zawarł ugodę z grupami non-profit, które były jego celem.

Czy wspomniałem, że nikt nigdy nie został pociągnięty do odpowiedzialności ani nie odbył kary więzienia za bezprawne namierzanie amerykańskich obywateli przez agencję federalną na podstawie przynależności politycznej? Ale ty, jako właściciel małej firmy, z pewnością pójdziesz do więzienia, jeśli nie zastosujesz się do ustawy o przejrzystości korporacyjnej.

Ustawa o przejrzystości korporacyjnej jest „dla zysku” odpowiednikiem partyzanckiej kontroli Departamentu Skarbu. W tym czasie organizacje non-profit ze słowem „partia herbaciana” i „patriota” były politycznie namierzane przez IRS i poddawane dalszej kontroli i/lub całkowitej odmowie przyznania im statusu 501c3.

W ramach CTA, powiedzmy, że jawnie agresywny biurokrata

przeciwny drugiej poprawce zdecydował się wyszukać słowo „pistolet”, „broń palna”, „patriota”, „wolność” – masz pomysł – mieliby gotową listę właścicieli małych firm do namierzenia, potencjalnego zbadania i audytu, za coś tak prostego jak nazwa. Zdarzyło się to już wcześniej z konserwatywnymi organizacjami non-profit, myślisz, że nie może się to powtórzyć z firmami nastawionymi na zysk?

Zgodnie z CTA, podmioty gospodarcze nastawione na zysk, zatrudniające mniej niż 20 pracowników i osiągające mniej niż 5 milionów przychodu, znajdują się na celowniku. Tak, dobrze przeczytałeś, jeśli zarabiasz więcej niż 5 milionów dolarów rocznie lub zatrudniasz więcej niż 20 pełnoetatowych pracowników – jesteś ZWOLNIONY z tego inwazyjnego wymogu samodzielnego raportowania, który może doprowadzić cię do więzienia.

Oznacza to, że Blackrock, Amazon, Facebook, Pfizer Apple i ExxonMobil mogą prowadzić „biznes jak zwykle”, ale „sklep z pączkami babci” będzie musiał pokazać jej „papier proszę”, jeśli chce zarabiać na życie.

Rejestracja firm i tworzenie podmiotów jest i zawsze było obsługiwane na poziomie stanowym przez stanowe komisje ds. korporacji lub podobne organizacje.

Dlaczego rząd federalny nadmiernie wkracza w kwestię praw stanowych i tworzy ogromną federalną bazę danych z naruszeniem klauzuli handlowej?

Oznacza to, że nawet jeśli jesteś zarejestrowanym podmiotem na poziomie stanowym, jeśli nie zgłosisz się i nie zarejestrujesz na poziomie federalnym, nie będziesz mógł prowadzić swojej małej firmy.

Dlaczego stanowy prokurator generalny nie zajmuje się tą kwestią? Mam nadzieję, że nie jest to pytanie retoryczne.

CTA jest ostatnim gwoździem do trumny tego, co pozostało z

iluzji „wolnorynkowej” gospodarki w Stanach Zjednoczonych i jest to ogromny program nadzoru gospodarczego z niewielkim lub żadnym zauważalnym nadzorem.

Ludzie powoli zaczynają zwracać na to uwagę, więc jest jeszcze czas i nadzieja. Zaledwie kilka tygodni temu Community Associations Institute złożył pozew przeciwko Departamentowi Skarbu Stanów Zjednoczonych, kwestionując stosowanie ustawy o przejrzystości korporacyjnej.

Ale CAI i inni właściciele małych firm, którzy również złożyli pozew, nie mogą tego zrobić sami.

Sędzia federalny w Alabamie orzekł już, że ustawa ta jest „niezgodna z konstytucją”, a mimo to rząd federalny nadal działa pełną parą, nie zważając na konstytucyjność tego bezprecedensowego przekroczenia uprawnień.

Jeszcze bardziej interesujące jest to, że orzeczenie o „niekonstytucyjności” ma zastosowanie tylko do powodów w sprawie, ustanawiając bardzo niebezpieczny precedens prawny, zgodnie z którym jeśli złożysz skargę, zachowasz swoje prawa konstytucyjne, ale jeśli tego nie zrobisz, stracisz je.

Oba obozy – republikanie i demokraci – muszą wypowiedzieć się w tej sprawie przed listopadem. Jest to najbardziej niebezpieczny krok, jaki Stany Zjednoczone kiedykolwiek podjęły w kierunku nacjonalizacji własności małych prywatnych firm pod parasolem federalnym.

Jest to taktyka od dawna praktykowana i realizowana przez rządy marksistowskie. Musi to być główny temat kampanii, aby chronić ponad 33 miliony małych firm przed zniszczeniem przez rząd federalny.

Małe firmy zatrudniają 61,7 miliona Amerykanów, co stanowi 46,4% pracowników sektora prywatnego. Nadszedł czas, aby przeciwstawić się temu rażącemu atakowi na prawa stanowe, który ma na celu kontrolowanie i/lub zniszczenie ekonomicznej

siły napędowej Ameryki.

Każdy właściciel małej firmy w Ameryce musi zabrać głos w tej sprawie, w przeciwnym razie będzie za późno.

Źródło

Ciemna strona GEOLOKACJI: Jak nasze gadżety stały się cichymi prześladowcami dzięki pozycjonowaniu WiFi

W dzisiejszym cyfrowo połączonym świecie geolokalizacja odgrywa kluczową rolę w sposobie nawigacji, interakcji z usługami, a nawet zachowania bezpieczeństwa.

Geolokalizacja to proces identyfikacji dokładnego położenia geograficznego urządzenia lub osoby przy użyciu technologii takich jak systemy pozycjonowania WiFi i globalne systemy nawigacji satelitarnej (GNSS). Chociaż technologie te oferują ogromne korzyści, wiążą się również z poważnymi zagrożeniami i lukami w zabezpieczeniach, budząc obawy o prywatność i bezpieczeństwo.

Korzyści z geolokalizacji

Wprowadzenie technologii geolokalizacji do szerszego społeczeństwa zasadniczo zmieniło sposób, w jaki ludzie nawigują i wchodzą w interakcje z otoczeniem. Ułatwia znalezienie najszybszej drogi do domu, a także innych miejsc docelowych i pomaga firmom usprawnić operacje dostawy – zwiększając ogólną wydajność i wygodę. Co więcej, precyzyjne dane lokalizacyjne mają kluczowe znaczenie dla służb ratunkowych – umożliwiając szybki czas reakcji, który może uratować życie w krytycznych sytuacjach.

Systemy pozycjonowania wewnątrz budynków, określane również jako śledzenie lokalizacji wewnątrz budynków, są niezbędne w dużych zamkniętych przestrzeniach, takich jak szpitale, centra handlowe i stacje kolejowe. Systemy te umożliwiają dokładne śledzenie lokalizacji za pomocą urządzeń mobilnych, takich jak smartfony lub tablety, poprawiając nawigację i wydajność operacyjną w budynkach.

Dla profesjonalistów pracujących w środowiskach odizolowanych lub wysokiego ryzyka, geolokalizacja wewnątrz budynków jest nieoceniona dla zapewnienia bezpieczeństwa. Śledzenie pozycji pracowników w czasie rzeczywistym może mieć kluczowe znaczenie w sytuacjach awaryjnych, umożliwiając szybką interwencję w razie potrzeby. W scenariuszach takich jak pożary lub incydenty terrorystyczne w miejscach publicznych, geolokalizacja wewnątrz budynków pomaga służbom ratowniczym w szybkim zlokalizowaniu osób znajdujących się w niebezpieczeństwie.

Zewnętrzne usługi geolokalizacyjne, zasilane przez GNSS – takie jak Galileo w Unii Europejskiej i GPS w Stanach Zjednoczonych – stały się wszechobecne. Te konstelacje satelitów transmitują sygnały, które umożliwiają odbiornikom obsługującym GNSS określenie dokładnych danych o lokalizacji, wspierając szeroki zakres zastosowań w różnych sektorach i

demonstrując ich szerokie zastosowanie w nowoczesnej technologii i życiu codziennym.

Niebezpieczeństwa, zagrożenia i słabe punkty geolokalizacji

Technologia geolokalizacji stwarza poważne zagrożenia dla prywatności i bezpieczeństwa użytkowników. Systemy pozycjonowania WiFi, które są używane zarówno na zewnątrz, jak i wewnątrz budynków, gromadzą obszerne dane, które mogą zostać niewłaściwie wykorzystane przez nieupoważnione podmioty.

Integracja geolokalizacji z krytycznymi systemami bezpieczeństwa wprowadza wyzwania związane z cyberbezpieczeństwem. Cyberataki mogą manipulować danymi o lokalizacji, zagrażając bezpieczeństwu służb ratowniczych i osób znajdujących się w niebezpieczeństwie. Dlatego też ochrona wewnętrznych systemów geolokalizacji przed cyberzagrożeniami ma kluczowe znaczenie.

Przykłady solidnych środków cyberbezpieczeństwa obejmują wdrażanie silnych protokołów szyfrowania w celu zabezpieczenia przesyłanych danych o lokalizacji; stosowanie uwierzytelniania wieloskładnikowego w celu kontrolowania dostępu do poufnych informacji; oraz przeprowadzanie regularnych testów penetracyjnych w celu identyfikacji i naprawy luk w zabezpieczeniach.

Usługi geolokalizacji wewnątrz budynków są podatne na zagrożenia cybernetyczne, podobnie jak każdy inny sektor technologiczny. Cyberprzestępcy wykorzystują luki w oprogramowaniu i protokołach komunikacyjnych, aby uzyskać dostęp do danych o lokalizacji w czasie rzeczywistym lub przechowywanych informacji z tych systemów. Ponadto ataki spoofingowe wprowadzają w błąd sygnały lokalizacji, prowadząc do błędów nawigacji i potencjalnego zagrożenia bezpieczeństwa użytkowników.

Urządzenia infrastrukturalne zintegrowane z systemami geolokalizacji, takie jak beacony i bramy, mogą być również celem ataków cybernetycznych. Komponenty te służą jako punkty wejścia dla zdalnych ataków lub nieautoryzowanego dostępu za pośrednictwem połączeń Bluetooth.

Zabezpieczenie tych punktów dostępu ma zasadnicze znaczenie dla zapobiegania naruszeniom i ochrony poufnych danych związanych z geolokalizacją w pomieszczeniach. Na przykład konfiguracja zapór ogniowych i systemów wykrywania włamań może pomóc w monitorowaniu i blokowaniu podejrzanej aktywności sieciowej.

Powszechne przyjęcie geolokalizacji rodzi obawy o niewłaściwe wykorzystanie osobistych danych o lokalizacji. Reklamodawcy wykorzystują te dane do ukierunkowanych reklam, podczas gdy złośliwe podmioty mogą wykorzystywać je do inwigilacji lub kradzieży tożsamości. Ochrona wrażliwych informacji jest najważniejsza w usługach geolokalizacji wewnątrz budynków, wymagając solidnych środków bezpieczeństwa, takich jak bezpieczne praktyki programistyczne, szyfrowanie, silne uwierzytelnianie i regularne audyty bezpieczeństwa.

Aby skutecznie ograniczyć to ryzyko, osoby fizyczne i organizacje powinny priorytetowo traktować zabezpieczanie sieci Wi-Fi za pomocą szyfrowanych połączeń. Wdrożenie rygorystycznych ustawień prywatności na urządzeniach i aplikacjach pomaga ograniczyć informacje o lokalizacji udostępniane stronom trzecim. Ponadto podnoszenie świadomości na temat zagrożeń cyberbezpieczeństwa i promowanie najlepszych praktyk wzmacnia ogólne bezpieczeństwo IT, zapewniając bezpieczne i odpowiedzialne korzystanie z technologii geolokalizacji.

Wielka Brytania wykorzystuje sztuczną inteligencję opracowaną przez Amazon do odczytywania nastrojów ludzi na stacjach kolejowych

Seria testów sztucznej inteligencji (AI) w Wielkiej Brytanii z udziałem tysięcy pasażerów pociągów, którzy zostali nieświadomie poddani oprogramowaniu wykrywającemu emocje, wzbudziła obawy o prywatność.

Technologia opracowana przez Amazon i stosowana na różnych głównych stacjach kolejowych, w tym londyńskich Euston i Waterloo, wykorzystywała sztuczną inteligencję do skanowania twarzy i oceny stanów emocjonalnych wraz z wiekiem i płcią. Dokumenty uzyskane przez grupę wolności obywatelskich Big Brother Watch za pośrednictwem wniosku o wolność informacji ujawniły te praktyki, które mogą wkrótce wpłynąć na strategie reklamowe.

W testach tych wykorzystano technologię CCTV i starsze kamery połączone z systemami opartymi na chmurze w celu monitorowania szeregu działań, w tym wykrywania wtargnięcia na tory kolejowe, zarządzania wielkością tłumu na peronach i identyfikowania zachowań antyspołecznych, takich jak krzyki lub palenie. Testy monitorowały nawet potencjalne kradzieże rowerów i inne incydenty związane z bezpieczeństwem.

Dane pochodzące z tych systemów mogłyby zostać wykorzystane do zwiększenia przychodów z reklam poprzez ocenę zadowolenia pasażerów poprzez ich stany emocjonalne, uchwycone, gdy osoby przekroczyły wirtualne tripwires w pobliżu barier biletowych.Krytycy twierdzą, że technologia ta jest zawodna i wzywają do jej zakazania.

W ciągu ostatnich dwóch lat osiem stacji kolejowych w Wielkiej Brytanii przetestowało technologię nadzoru AI, z kamerami CCTV, które mają ostrzegać personel o incydentach związanych z bezpieczeństwem i potencjalnie zmniejszyć niektóre rodzaje przestępstw.

Szeroko zakrojone testy, nadzorowane przez organ infrastruktury kolejowej Network Rail, wykorzystywały rozpoznawanie obiektów – rodzaj uczenia maszynowego, które może identyfikować elementy w kanałach wideo. W oddzielnych testach wykorzystano czujniki bezprzewodowe do wykrywania śliskich podłóg, pełnych pojemników i odpływów, które mogą się przepełnić.

„Wdrożenie i normalizacja nadzoru AI w tych przestrzeniach publicznych, bez większych konsultacji i rozmów, jest dość niepokojącym krokiem” – powiedział Jake Hurfurt, szef badań i dochodzeń w Big Brother Watch.

Wykorzystanie technologii do wykrywania emocji jest zawodne

Badacze sztucznej inteligencji często ostrzegali, że wykorzystanie technologii do wykrywania emocji jest „niewiarygodne”, a niektórzy twierdzą, że technologia ta powinna zostać zakazana ze względu na trudności w ustaleniu, jak ktoś może się czuć na podstawie dźwięku lub obrazu. W październiku 2022 r. brytyjski organ regulacyjny ds. danych, Information Commissioner’s Office, wydał publiczne oświadczenie ostrzegające przed stosowaniem analizy emocji,

mówiąc, że technologie te są „niedojrzałe” i „mogą jeszcze nie działać, a nawet nigdy”.

Obrońcy prywatności są szczególnie zaniepokojeni nieprzejrzystym charakterem i potencjałem nadmiernego wykorzystania sztucznej inteligencji w przestrzeni publicznej.Hurfurt wyraził poważne obawy dotyczące normalizacji takiego inwazyjnego nadzoru bez odpowiedniego publicznego dyskursu lub nadzoru.

„Network Rail nie miała prawa wdrażać zdyskredytowanej technologii rozpoznawania emocji przeciwko nieświadomym osobom dojeżdżającym do pracy na niektórych z największych stacji w Wielkiej Brytanii, a ja złożyłem skargę do komisarza ds. informacji na temat tej próby” – powiedział Hurfurt.

„Niepokojące jest to, że jako organ publiczny zdecydował się na przeprowadzenie zakrojonej na szeroką skalę próby nadzoru AI stworzonego przez Amazon na kilku stacjach bez świadomości publicznej, zwłaszcza gdy Network Rail zmieszał technologię bezpieczeństwa z pseudonaukowymi narzędziami i zasugerował, że dane mogą być przekazywane reklamodawcom” – dodał.

„Technologia może odegrać rolę w zwiększaniu bezpieczeństwa kolei, ale potrzebna jest solidna debata publiczna na temat konieczności i proporcjonalności stosowanych narzędzi. Nadzór oparty na sztucznej inteligencji może zagrozić naszej prywatności, zwłaszcza jeśli zostanie niewłaściwie wykorzystany, a lekceważenie tych obaw przez Network Rail pokazuje pogardę dla naszych praw”.

Wojskowe korzenie Facebooka

Komentarz: Przecież to jasne , że nie ma czegoś takiego jak geniusz, który napisał aplikację i z zera został miliarderem. Bez opieki odpowiednich ludzi nie robi się takiej kariery. Tak samo z Gates'em – gdyby nie to że to był SWÓJ chłop, z dziadkiem związanym z klinikami aborcyjnymi, to by też nie był promowany. Tak samo jak Owsiak. Krzysztof

Rosnąca rola Facebooka w stale rozwijającym się aparacie nadzoru i „przedkryminalnym" państwie bezpieczeństwa narodowego wymaga nowej analizy pochodzenia firmy i jej produktów w odniesieniu do poprzedniego, kontrowersyjnego programu nadzoru prowadzonego przez DARPA, który był zasadniczo analogiczny do tego, co jest obecnie największą na świecie siecią społecznościową.

W połowie lutego Daniel Baker, amerykański weteran określany przez media jako „antytrumpowy, antyrządowy, przeciwny białej supremacji i przeciwny policji", został oskarżony przez wielką ławę przysięgłych z Florydy o dwa zarzuty „przekazywania wiadomości komunikat w handlu międzystanowym zawierający groźbę porwania lub zranienia."

Komunikat, o którym mowa, Baker umieścił na Facebooku, gdzie stworzył stronę wydarzenia mającą na celu zorganizowanie zbrojnego wiecu w stosunku do zaplanowanego przez zwolenników Donalda Trumpa 6 stycznia w stolicy Florydy, Tallahassee. „Jeśli boisz się umrzeć, walczyć z wrogiem, a potem zostań w łóżku i żyj. Zadzwoń do wszystkich swoich znajomych i powstańcie!" – napisał Baker na swojej stronie wydarzenia na

Facebooku.

Sprawa Bakera jest godna uwagi, ponieważ jest to jedno z pierwszych aresztowań „przed przestępstwem” opartych wyłącznie na wpisach w mediach społecznościowych – logiczny wniosek płynący z wysiłków administracji Trumpa, a obecnie Bidena, na rzecz normalizacji aresztowań osób za wpisy w Internecie, aby zapobiec aktom przemocy, zanim będą one mogły to zrobić. zdarzyć. Począwszy od rosnącego stopnia zaawansowania programów predykcyjnych działań policyjnych Palantira, przedsiębiorstwa wywiadu USA/kontraktora wojskowego , po formalne ogłoszenie przez Departament Sprawiedliwości programu zakłócania i wczesnego zaangażowania w 2019 r. po pierwszy budżet Bidena, który obejmuje 111 mln dolarów na ściganie i zarządzanie „rosnącą liczbą spraw związanych z terroryzmem krajowym” – Pod rządami każdej administracji prezydenckiej po 11 września zauważalny był stały postęp w kierunku skupionej przed przestępczością „wojny z terroryzmem wewnętrznym”.

Ta nowa, tak zwana wojna z terroryzmem krajowym faktycznie zaowocowała wieloma tego typu postami na Facebooku. I chociaż Facebook od dawna starał się przedstawiać siebie jako „rynek miejski”, który umożliwia nawiązywanie kontaktów ludziom z całego świata, głębsze spojrzenie na jego pozornie wojskowe pochodzenie i ciągłe powiązania wojskowe ujawnia, że największa na świecie sieć społecznościowa zawsze miała działać jako narzędzie nadzoru służące identyfikowaniu i zwalczaniu sprzeciwu w kraju.

Część 1 tej dwuczęściowej serii na temat Facebooka i amerykańskiego stanu bezpieczeństwa narodowego bada początki tej sieci mediów społecznościowych oraz czas i charakter jej powstania w związku z kontrowersyjnym programem wojskowym, który został zamknięty tego samego dnia, w którym uruchomiono Facebooka. Program, znany jako LifeLog, był jednym z kilku kontrowersyjnych programów obserwacji po 11 września, realizowanych przez Agencję Zaawansowanych Projektów

Badawczych w dziedzinie Obronności (DARPA) Pentagonu, który groził zniszczeniem prywatności i swobód obywatelskich w Stanach Zjednoczonych, a jednocześnie miał na celu zebranie danych do celów produkujących „humanizowaną” sztuczną inteligencję (AI).

Jak wykaże ten raport, Facebook nie jest jedynym gigantem z Doliny Krzemowej, którego początki ściśle pokrywają się z tą samą serią inicjatyw DARPA i którego obecne działania stanowią zarówno silnik, jak i paliwo dla zaawansowanej technologicznie wojny z krajowym sprzeciwem.

Eksploracja danych DARPA dla „bezpieczeństwa narodowego” i „humanizowania” sztucznej inteligencji

W następstwie ataków z 11 września DARPA, w ścisłej współpracy ze społecznością wywiadowczą USA (w szczególności z CIA), rozpoczęła opracowywanie „przedprzestępczego” podejścia do zwalczania terroryzmu, znanego jako Total Information Awareness (TIA). Celem TIA było opracowanie „wszystkowidzącego” aparatu wojskowego nadzoru. Oficjalna logika stojąca za TIA była taka, że inwazyjna inwigilacja całej populacji USA była konieczna, aby zapobiec atakom terrorystycznym, zjawiskom bioterroryzmu, a nawet naturalnie występującym epidemiom chorób.

Pomysłodawcą TIA i człowiekiem, który przewodził jej podczas jej stosunkowo krótkiego istnienia, był John Poindexter , najbardziej znany z tego, że był doradcą Ronalda Reagana ds. bezpieczeństwa narodowego podczas afery Iran-Contras i został skazany za pięć przestępstw w związku z tym skandalem. Mniej znaną działalnością przedstawicieli Iran-Contras, takich jak Poindexter i Oliver North, było opracowanie przez nich bazy danych Main Core do wykorzystania

w protokołach „ciągłości rządzenia”. Main Core został wykorzystany do sporządzenia listy amerykańskich dysydentów i „potencjalnych wichrzycieli”, z którymi należy się uporać w przypadku powołania się na protokoły COG. Na protokoły te można się powołać z różnych powodów, w tym z powodu powszechnego sprzeciwu opinii publicznej wobec amerykańskiej interwencji wojskowej za granicą, powszechnego sprzeciwu wewnętrznego lub niejasno określonego momentu „kryzysu narodowego” lub „czasu paniki”. Amerykanie nie byli informowani, czy ich nazwisko znalazło się na liście, a dana osoba mogła zostać dodana do listy tylko dlatego, że w przeszłości brała udział w protestach, nie płaciła podatków lub miała inne, „często błahe” zachowania uznawane za „ nieprzyjazny” przez jego architektów w administracji Reagana.

W świetle tego nie było przesadą, gdy felietonista *„New York Timesa”* William Safire zauważył, że dzięki TIA „Poindexter realizuje teraz swoje dwudziestoletnie marzenie: uzyskanie mocy „eksploracji danych” umożliwiającej szpiegowanie każdego publicznego i prywatnego działania każdego Amerykanina”.

Program TIA spotkał się ze znacznym oburzeniem obywateli po jego ujawnieniu opinii publicznej na początku 2003 r. Wśród krytyków TIA znalazła się Amerykańska Unia Wolności Obywatelskich, która twierdziła , że wysiłki inwigilacyjne „zabiją prywatność w Ameryce”, ponieważ „każdy aspekt naszego życia byłby skatalogowane”, podczas gdy kilka mediów głównego nurtu ostrzegało, że TIA „walczy z terroryzmem poprzez przerażanie obywateli USA”. W wyniku nacisków DARPA zmieniła nazwę programu na Terrorist Information Awareness, aby brzmiała mniej jak panoptykon dotyczący bezpieczeństwa narodowego, a bardziej jak program skierowany szczególnie do terrorystów w epoce po 11 września.

Logo Biura Świadomości Informacyjnej DARPA, które nadzorowało Total Information Awareness podczas jego krótkiego istnienia

Projekty TIA nie zostały jednak w rzeczywistości zamknięte, a większość z nich została przeniesiona do tajnych tek Pentagonu i społeczności wywiadowczej USA. Niektóre z nich, jak na przykład Palantir Petera Thiela , stały się finansowane przez wywiad i kierowały przedsięwzięciami sektora prywatnego , podczas gdy inne pojawiły się ponownie po latach pod pozorem walki z kryzysem związanym z Covid-19.

Wkrótce po zainicjowaniu TIA podobny program DARPA nabierał kształtu pod kierownictwem bliskiego przyjaciela Poindextera, menadżera programu DARPA Douglasa Gage'a. Projekt Gage'a, LifeLog, miał na celu „zbudowanie bazy danych śledzącej całe życie danej osoby", która obejmowałaby relacje i komunikację danej osoby (rozmowy telefoniczne, poczta itp.), jej nawyki dotyczące korzystania z mediów, zakupy i wiele innych w celu zbudowania cyfrowy zapis „ wszystko, co dana osoba mówi, widzi lub robi". LifeLog następnie pobierze te nieustrukturyzowane dane i uporządkuje je w „ dyskretne odcinki " lub migawki, jednocześnie „mapując relacje, wspomnienia, wydarzenia i doświadczenia".

Według Gage'a i zwolenników programu LifeLog stworzyłby trwały i przeszukiwalny elektroniczny dziennik całego życia danej osoby, który według DARPA mógłby zostać wykorzystany do stworzenia „cyfrowych asystentów" nowej generacji i zaoferować użytkownikom „niemal idealną pamięć cyfrową". " Gage upierał się , że nawet po zakończeniu programu poszczególne osoby miałyby „pełną kontrolę nad własnymi działaniami związanymi z gromadzeniem danych", ponieważ mogłyby „decydować, kiedy włączyć, a kiedy wyłączyć czujniki i kto udostępni dane". Od tego czasu analogiczne obietnice dotyczące kontroli użytkowników składali giganci technologiczni z Doliny Krzemowej, ale wielokrotnie łamali je dla zysku i w celu zasilania rządowego aparatu nadzoru wewnętrznego.

Informacje, które LifeLog zbierał na podstawie każdej interakcji danej osoby z technologią, byłyby łączone z informacjami uzyskanymi z nadajnika GPS, który śledził i dokumentował lokalizację danej osoby, czujników audiowizualnych rejestrujących to, co dana osoba widziała i mówiła, a także biomedycznych monitorów oceniających zdrowie danej osoby. Podobnie jak TIA, LifeLog był promowany przez DARPA jako potencjalnie wspierający „badania medyczne i wczesne wykrywanie pojawiającej się epidemii".

Krytycy w mediach głównego nurtu i poza nim szybko zwrócili uwagę, że program nieuchronnie zostanie wykorzystany do budowania sylwetek dysydentów, a także podejrzanych o terroryzm. W połączeniu z wielopoziomowym monitorowaniem osób przez TIA, LifeLog poszedł dalej, „dodając informacje fizyczne (takie jak to, jak się czujemy) i dane medialne (takie jak to, co czytamy) do danych transakcyjnych". Jeden z krytyków, Lee Tien z Electronic Frontier Foundation, ostrzegł wówczas , że programy realizowane przez DARPA, w tym LifeLog, „mają oczywiste i łatwe ścieżki do wdrożenia w ramach bezpieczeństwa wewnętrznego".

W tamtym czasie DARPA publicznie utrzymywała , że LifeLog i TIA nie są ze sobą powiązane, pomimo ich oczywistych

podobieństw, oraz że LifeLog nie będzie wykorzystywany do „tajnego nadzoru”. Jednakże w dokumentacji DARPA dotyczącej LifeLog odnotowano, że w ramach projektu „będzie można . . . wywnioskować o rutynach, zwyczajach i relacjach użytkownika z innymi ludźmi, organizacjami, miejscami i przedmiotami oraz wykorzystać te wzorce, aby ułatwić mu zadanie”, w którym uznano jego potencjalne zastosowanie jako narzędzia masowej inwigilacji.

Oprócz możliwości profilowania potencjalnych wrogów państwa, LifeLog miał inny cel, prawdopodobnie ważniejszy dla państwa zapewniającego bezpieczeństwo narodowe i jego partnerów akademickich – „humanizację” i rozwój sztucznej inteligencji. Pod koniec 2002 roku, zaledwie kilka miesięcy przed ogłoszeniem istnienia LifeLog, DARPA opublikowała dokument strategiczny szczegółowo opisujący rozwój sztucznej inteligencji poprzez zasilanie jej ogromnym strumieniem danych z różnych źródeł.

Projekty nadzoru wojskowego po 11 września – LifeLog i TIA to tylko dwa z nich – zapewniły ilości danych, których uzyskanie wcześniej było nie do pomyślenia, a które mogłyby potencjalnie stanowić klucz do osiągnięcia hipotetycznej „osobliwości technologicznej”. Dokument DARPA z 2002 r. omawia nawet wysiłki DARPA mające na celu stworzenie interfejsu mózg-maszyna, który przesyłałby ludzkie myśli bezpośrednio do maszyn w celu rozwoju sztucznej inteligencji poprzez ciągłe zalewanie jej świeżo wydobytymi danymi.

Jeden z projektów przedstawionych przez DARPA, Cognitive Computing Initiative, miał na celu rozwój zaawansowanej sztucznej inteligencji poprzez stworzenie „trwałego, spersonalizowanego asystenta poznawczego”, nazwanego później Perceptive Asystent, który się uczy , (PAL). PAL od samego początku był powiązany z LifeLog, którego pierwotnym zamierzeniem było zapewnienie „asystentowi” sztucznej inteligencji przypominającego człowieka zdolności podejmowania decyzji i rozumienia poprzez przekształcanie mas

nieustrukturyzowanych danych w format narracyjny.

Przyszli główni badacze projektu LifeLog odzwierciedlają także końcowy cel programu, jakim jest stworzenie humanizowanej sztucznej inteligencji. Na przykład Howard Shrobe z Laboratorium Sztucznej Inteligencji MIT i jego ówczesny zespół mieli być ściśle zaangażowani w LifeLog. Shrobe pracował wcześniej dla DARPA nad „ewolucyjnym projektowaniem złożonego oprogramowania", zanim został zastępcą dyrektora Laboratorium AI na MIT i poświęcił swoją długą karierę na budowaniu „sztucznej inteligencji w stylu kognitywnym". W latach po odwołaniu LifeLog ponownie pracował dla DARPA, a także przy projektach badawczych związanych ze sztuczną inteligencją związanych ze społecznością wywiadowczą. Ponadto laboratorium AI na MIT było ściśle powiązane z korporacją z lat 80. XX wieku i wykonawcą DARPA o nazwie Thinking Machines , która została założona przez wielu luminarzy laboratorium i/lub zatrudniała wielu luminarzy laboratorium, w tym Danny'ego Hillisa, Marvina Minsky'ego i Erica Landera, i starała się budować superkomputery AI zdolne do myślenia na poziomie ludzkim. Później okazało się, że wszystkie trzy osoby były bliskimi współpracownikami i/lub sponsorowanymi przez powiązanego z wywiadem pedofila Jeffreya Epsteina, który również hojnie przekazał darowizny na rzecz MIT jako instytucji oraz był głównym fundatorem i orędownikiem badań naukowych związanych z transhumanizmem.

Wkrótce po zamknięciu programu LifeLog krytycy obawiali się, że podobnie jak TIA będzie on kontynuowany pod inną nazwą. Na przykład Lee Tien z Electronic Frontier Foundation powiedział *VICE* w momencie anulowania LifeLog: „Nie zdziwiłbym się, gdybym dowiedział się, że rząd w dalszym ciągu finansował badania, które popchnęły tę dziedzinę do przodu, nie nazywając go LifeLog".

Wraz z krytykami jeden z potencjalnych badaczy pracujących nad LifeLog, David Karger z MIT, również był pewien, że projekt DARPA będzie kontynuowany w nowej formie. Powiedział *Wired* ,

że „Jestem pewien, że takie badania będą nadal finansowane z innego tytułu. . . Nie mogę sobie wyobrazić, że DARPA „porzuci” tak kluczowy obszar badawczy”.

Wydaje się, że odpowiedź na te spekulacje należy do firmy, która uruchomiła usługę dokładnie tego samego dnia, w którym Pentagon zamknął LifeLog: Facebooka.

Świadomość informacyjna Thiela

Po znacznych kontrowersjach i krytyce pod koniec 2003 roku TIA została zamknięta i pozbawiona finansowania przez Kongres, zaledwie kilka miesięcy po jej uruchomieniu. Dopiero później ujawniono, że TIA *tak naprawdę* nigdy nie została zamknięta , a jej różne programy zostały potajemnie podzielone pomiędzy sieć agencji wojskowych i wywiadowczych tworzących amerykańskie państwo zapewniające bezpieczeństwo narodowe. Część z nich została sprywatyzowana.

W tym samym miesiącu, w którym TIA została zmuszona do zmiany nazwy w związku z rosnącymi sprzeciwami, Peter Thiel założył firmę Palantir, która, nawiasem mówiąc, opracowywała podstawowe oprogramowanie panopticon, którego TIA miała nadzieję używać. Wkrótce po założeniu Palantir w 2003 r. Richard Perle, notoryczny neokonserwatysta z administracji Reagana i Busha oraz architekt wojny w Iraku, zadzwonił do Poindextera z TIA i powiedział, że chce przedstawić go Thielowi i jego współpracownikowi Alexowi Karpowi, obecnie dyrektorowi generalnemu Palantir. Według raportu magazynu *New York* Poindexter „był dokładnie tą osobą”, z którą Thiel i Karp chcieli się spotkać, głównie dlatego, że „ich nowa firma miała podobne ambicje do tego, co Poindexter próbował stworzyć w Pentagonie ” , czyli TIA . Podczas tego spotkania Thiel i Karp starali się „wybrać mózg człowieka obecnie powszechnie postrzeganego jako ojciec chrzestny współczesnej inwigilacji”.

Peter Thiel przemawia na Światowym Forum Ekonomicznym w 2013 r., Źródło: Mirko Ries Dzięki uprzejmości Światowego Forum Ekonomicznego

Wkrótce po założeniu Palantira, choć dokładny termin i szczegóły inwestycji pozostają ukryte przed opinią publiczną, In-Q-Tel z CIA stał się, obok samego Thiela, pierwszym sponsorem firmy, przekazując jej szacunkową kwotę 2 milionów dolarów. Informacje o udziałach In-Q-Tel w Palantir zostaną podane do wiadomości publicznej dopiero w połowie 2006 roku .

Pieniądze z pewnością się przydały. Ponadto Alex Karp powiedział *New York Times* w październiku 2020 r.: „prawdziwą wartością inwestycji In-Q-Tel było to, że zapewniła ona Palantirowi dostęp do analityków CIA, którzy byli jego zamierzonymi klientami”. Kluczową postacią w inwestycjach In-Q-Tel w tym okresie, w tym w inwestycji w Palantir, był dyrektor ds. informacji CIA, Alan Wade, który był głównym przedstawicielem społeczności wywiadowczej w zakresie Totalnej Świadomości Informacyjnej. Wade był wcześniej współzałożycielem firmy Chiliad, dostawcy oprogramowania

Homeland Security po 11 września, wraz z Christine Maxwell, siostrą Ghislaine Maxwell i córką działacza Iran-Contras, agenta wywiadu i barona medialnego Roberta Maxwella.

Po inwestycji In-Q-Tel CIA była jedynym klientem Palantira aż do 2008 roku. W tym okresie dwaj czołowi inżynierowie Palantira – Aki Jain i Stephen Cohen – podróżowali co dwa tygodnie do siedziby CIA w Langley w Wirginii . Jain pamięta, że w latach 2005–2009 odbył co najmniej dwieście podróży do siedziby CIA. Podczas tych regularnych wizyt analitycy CIA „testowali [oprogramowanie Palantira] i przekazywali opinie, a następnie Cohen i Jain wracali do Kalifornii, aby je ulepszyć". Podobnie jak w przypadku decyzji In-Q-Tel o inwestycji w Palantir, główny specjalista ds. informacji CIA pozostał w tym czasie jednym z architektów TIA. Alan Wade odegrał kluczową rolę w wielu z tych spotkań, a następnie w „udoskonalaniu" produktów Palantir.

Obecnie produkty Palantir są wykorzystywane do masowej inwigilacji, predykcyjnych działań policyjnych i innych niepokojących polityk amerykańskiego państwa zapewniającego bezpieczeństwo narodowe. Wymownym przykładem jest znaczne zaangażowanie Palantir w nowy program nadzoru nad ściekami prowadzony przez służbę zdrowia i opiekę społeczną, który po cichu rozprzestrzenia się w całych Stanach Zjednoczonych. Jak zauważono w poprzednim raporcie *Unlimited Hangout* , system ten jest wskrzeszeniem programu TIA o nazwie Biosurveillance. Przesyła wszystkie swoje dane do zarządzanej przez Palantir i tajnej platformy danych HHS Protect. Decyzja o przekształceniu kontrowersyjnych programów prowadzonych przez DARPA w prywatne przedsięwzięcia nie ograniczała się jednak do Palantira Thiela.

Powstanie Facebooka

Zamknięcie TIA w DARPA miało wpływ na kilka powiązanych programów, które również zostały zlikwidowane w wyniku

publicznego oburzenia wywołanego programami DARPA po 11 września. Jednym z takich programów był LifeLog. Gdy wieść o programie rozeszła się po mediach, wielu z tych samych głośnych krytyków, którzy zaatakowali TIA, z podobną gorliwością zaatakowało LifeLog, a Steven Aftergood z Federacji Amerykańskich Naukowców powiedział wówczas *Wired* , że „LifeLog ma potencjał, aby stać się czymś jak „TIA w kostkach". Postrzeganie LifeLog jako czegoś, co mogłoby okazać się jeszcze gorsze niż niedawno odwołany TIA, miało wyraźny wpływ na DARPA, która właśnie anulowała zarówno TIA, jak i inny powiązany program po znacznych protestach opinii publicznej i prasy.

Burza krytyki programu LifeLog zaskoczyła jego menadżera programu, Douga Gage'a, a Gage w dalszym ciągu zapewniał, że krytycy programu „całkowicie błędnie scharakteryzowali" cele i ambicje projektu. Pomimo protestów Gage'a oraz potencjalnych badaczy i innych zwolenników LifeLog, projekt został publicznie porzucony 4 lutego 2004 r. DARPA nigdy nie wyjaśniła swojego cichego ruchu w celu zamknięcia LifeLog, a rzecznik stwierdził jedynie, że było to powiązane z „ zmiana priorytetów" dla agencji. W związku z decyzją dyrektora DARPA Tony'ego Tethera o zabiciu LifeLog, Gage powiedział później *VICE* : „Myślę, że TIA tak go poparzyła, że nie chciał mieć do czynienia z dalszymi kontrowersjami z LifeLog. Śmierć LifeLog była szkodą uboczną związaną ze śmiercią TIA.

Szczęśliwie dla zwolenników celów i ambicji LifeLog, firma, która okazała się jej odpowiednikiem z sektora prywatnego, narodziła się tego samego dnia, w którym ogłoszono zakończenie działalności LifeLog. 4 lutego 2004 r. Facebook, będący obecnie największą siecią społecznościową na świecie, uruchomił swoją witrynę internetową i szybko wspiął się na szczyty mediów społecznościowych, pozostawiając inne ówczesne firmy zajmujące się mediami społecznościowymi w tyle.

Sean Parker z Founders Fund przemawia podczas konferencji LeWeb w 2011 r., Źródło: @Kmeron dla LeWeb11 @ Les Docks de Paris

Kilka miesięcy po uruchomieniu Facebooka, w czerwcu 2004 roku, współzałożyciele Facebooka Mark Zuckerberg i Dustin Moskovitz wprowadzili Seana Parkera do zespołu wykonawczego Facebooka. Parker, wcześniej znany ze współzałożyciela Napstera, później połączył Facebooka z pierwszym inwestorem zewnętrznym, Peterem Thielem. Jak wspomniano, Thiel w tym czasie, w porozumieniu z CIA, aktywnie próbował wskrzesić kontrowersyjne programy DARPA, które zostały zlikwidowane w poprzednim roku. Warto zauważyć, że Sean Parker, który został pierwszym prezydentem Facebooka, miał także historię związaną z CIA, która zwerbowała go w wieku szesnastu lat, wkrótce po tym, jak FBI przyłapało go za włamywanie się do korporacyjnych i wojskowych baz danych. Dzięki Parkerowi we wrześniu 2004 r. Thiel formalnie nabył akcje Facebooka o wartości 500 000 dolarów i został włączony do jego zarządu. Parker utrzymywał bliskie kontakty z Facebookiem i Thielem, a w 2006 roku Parker został zatrudniony jako partner zarządzający Thiel’s

Founders Fund.

Thiel i współzałożyciel Facebooka, Mosokvitz, zaangażowali się poza siecią społecznościową długo po tym, jak Facebook zyskał na znaczeniu, a fundusz założycielski Thiela stał się znaczącym inwestorem w firmie Moskovitz Asana w 2012 r. Długotrwała symbiotyczna relacja Thiela ze współzałożycielami Facebooka rozciąga się na jego firmę Palantir, jak wynika z danych informacje, które użytkownicy Facebooka upubliczniają, niezmiennie trafiają do baz danych Palantir i pomagają w napędzaniu silnika monitorującego, który Palantir obsługuje garstkę amerykańskich departamentów policji, wojska i służb wywiadowczych. W przypadku skandalu związanego z danymi Facebooka i Cambridge Analytica Palantir był również zaangażowany w wykorzystywanie danych z Facebooka na potrzeby kampanii prezydenckiej Donalda Trumpa w 2016 r.

Dziś, jak wykazały niedawne aresztowania, takie jak aresztowanie Daniela Bakera, dane z Facebooka mają pomóc w nadchodzącej „wojnie z terroryzmem krajowym", biorąc pod uwagę, że informacje udostępniane na platformie są wykorzystywane do „przed popełnieniem przestępstwa" przechwytywania obywateli USA na szczeblu krajowym . W świetle tego warto zatrzymać się nad faktem, że wysiłki Thiela mające na celu wskrzeszenie głównych aspektów TIA jako jego własnej prywatnej firmy zbiegły się w czasie z tym, że stał się pierwszym inwestorem zewnętrznym w czymś, co zasadniczo było analogią do innego programu DARPA, głęboko powiązanego z TIA.

Facebook, front

Ze względu na zbieg okoliczności, że Facebook uruchomił się tego samego dnia, w którym zamknięto LifeLog, pojawiły się ostatnio spekulacje, że Zuckerberg rozpoczął i uruchomił projekt wspólnie z Moskovitzem, Saverinem i innymi w drodze zakulisowej koordynacji z DARPA lub innym organem. państwa bezpieczeństwa narodowego. Chociaż nie ma bezpośrednich

dowodów potwierdzających to dokładne twierdzenie, wczesne zaangażowanie Parkera i Thiela w projekt, szczególnie biorąc pod uwagę czas innych działań Thiela, ujawnia, że w rozwój Facebooka zaangażowane było państwo zapewniające bezpieczeństwo narodowe. Dyskusyjne jest, czy Facebook od samego początku miał być analogiem LifeLog, czy też stał się projektem mediów społecznościowych, który spełniał te wymagania po jego uruchomieniu. To drugie wydaje się bardziej prawdopodobne, zwłaszcza biorąc pod uwagę, że Thiel zainwestował także w inną wczesną platformę mediów społecznościowych, Friendster .

Ważnym punktem łączącym Facebooka i LifeLog jest późniejsza identyfikacja Facebooka z LifeLog przez samego architekta DARPA tego ostatniego. W 2015 roku Gage powiedział *VICE* , że „Facebook jest obecnie prawdziwą twarzą pseudo-LifeLog". Wymownie dodał: „Skończyło się na udostępnianiu tego samego rodzaju szczegółowych danych osobowych reklamodawcom i brokerom danych, nie wywołując przy tym takiego sprzeciwu, jaki wywołał LifeLog".

Użytkownicy Facebooka i innych dużych platform mediów społecznościowych byli dotychczas zadowoleni, umożliwiając tym platformom sprzedaż ich prywatnych danych, o ile działają one publicznie jako przedsiębiorstwa prywatne. Reakcja pojawiła się naprawdę dopiero wtedy, gdy takie działania zostały publicznie powiązane z rządem USA, a zwłaszcza z armią amerykańską, mimo że Facebook i inni giganci technologiczni rutynowo udostępniają dane swoich użytkowników państwu zapewniającemu bezpieczeństwo narodowe. W praktyce różnica pomiędzy podmiotami publicznymi i prywatnymi jest niewielka.

Edward Snowden, sygnalista NSA, w szczególności ostrzegł w 2019 r., że Facebook jest tak samo niegodny zaufania jak wywiad USA, stwierdzając, że „wewnętrznym celem Facebooka, niezależnie od tego, czy podaje to publicznie, czy nie, jest gromadzenie doskonałych zapisów życia prywatnego w maksymalnym stopniu możliwości, a następnie wykorzystać je do wzbogacenia

własnego przedsiębiorstwa. I cholera, konsekwencje.

Snowden stwierdził również w tym samym wywiadzie, że „im więcej Google o Tobie wie, im więcej wie o Tobie Facebook, tym więcej może. . . tworzyć trwałe zapisy życia prywatnego, tym większy wpływ i władzę mają na nas.” To podkreśla, jak zarówno Facebook, jak i powiązane z wywiadem Google osiągnęły wiele z tego, co zamierzał LifeLog, ale na znacznie większą skalę, niż pierwotnie przewidywała DARPA.

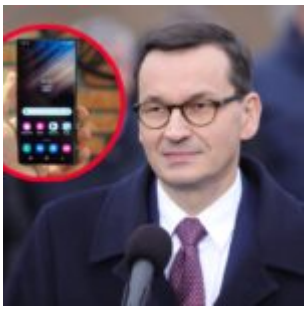
Rzeczywistość jest taka, że większość dzisiejszych dużych firm z Doliny Krzemowej jest od samego początku ściśle powiązana z amerykańskim establishmentem zapewniającym bezpieczeństwo narodowe. Godnymi uwagi przykładami, poza Facebookiem i Palantirem, są Google i Oracle . Dziś firmy te bardziej otwarcie współpracują z agencjami wywiadu wojskowego, które kierowały ich rozwojem i/lub zapewniały finansowanie na wczesnym etapie, ponieważ są wykorzystywane do dostarczania danych niezbędnych do napędzania nowo ogłoszonej wojny z terroryzmem krajowym i towarzyszącymi mu algorytmami.

To nie przypadek, że ktoś taki jak Peter Thiel, który zbudował Palantir wraz z CIA i pomógł zapewnić rozwój Facebooka, jest również mocno zaangażowany w oparte na Big Data „predykcyjne działania policyjne” oparte na sztucznej inteligencji i podejściu do inwigilacji i egzekwowania prawa, zarówno za pośrednictwem Palantira, jak i jego inne inwestycje . TIA, LifeLog oraz powiązane programy i instytucje rządowe i prywatne uruchomione po 11 września zawsze miały na celu wykorzystanie przeciwko amerykańskiemu społeczeństwu w wojnie przeciwko sprzeciwowi. Zostało to zauważone przez ich krytyków w latach 2003-2004 oraz przez tych, którzy badali pochodzenie zwrotu „bezpieczeństwa wewnętrznego” w USA i jego powiązanie z przeszłymi programami „antyterrorystycznymi” CIA w Wietnamie i Ameryce Łacińskiej.

Ostatecznie iluzja, że Facebook i powiązane z nim firmy są niezależne od amerykańskiego państwa zapewniającego

bezpieczeństwo narodowe, uniemożliwiła rozpoznanie rzeczywistości platform mediów społecznościowych i ich od dawna planowanych, ale ukrytych zastosowań, które – jak zaczynamy – zaczynają wychodzić na jaw po wydarzeniach z 6 stycznia. Teraz, gdy miliardy ludzi jest zmuszonych do korzystania z Facebooka i mediów społecznościowych w codziennym życiu, pojawia się pytanie: czy gdyby dziś ta iluzja została bezpowrotnie rozwiana, zrobiłoby to różnicę dla użytkowników Facebooka? A może społeczeństwo tak przyzwyczaiło się do oddawania swoich prywatnych danych w zamian za napędzane dopaminą pętle walidacji społecznej, że nie ma już znaczenia, kto ostatecznie będzie przechowywał te dane?

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