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.

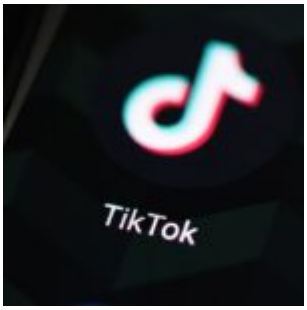
Jednak sytuacja prawna jest złożona. Sędzia federalny w Teksasie tymczasowo zablokował część stanowej ustawy SCOPE, powołując się na obawy dotyczące pierwszej poprawki. Główny radca prawny FIRE Bob Corn-Revere argumentuje: „Stany nie mogą blokować dorosłym możliwości angażowania się w legalne wypowiedzi 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.

Chiny wykorzystane jako kozioł ofiarny zakazu TikTok:

IZRAEL był siłą napędową zakazu, chciał zdusić treści propalestyńskie



Według osób wtajemniczonych w kongresie i dokumentów, które wyciekły, dążenie rządu USA do zakazania TikTok jest mniej związane z obawami o bezpieczeństwo narodowe w związku z chińską własnością, a bardziej z uciszaniem głosów propalestyńskich, które kwestionują narrację Izraela. Posunięcie to podkreśla niepokojący sojusz między amerykańskimi prawodawcami a izraelskimi interesami, rodząc pytania o wolność słowa i przejrzystość rządu.

Prawdziwa historia stojąca za zakazem TikTok

Podczas Monachijskiej Konferencji Bezpieczeństwa w lutym 2024 r. senator Mark Warner, czołowy demokrata w Senackiej Komisji Wywiadu, zasugerował „prawdziwą historię" stojącą za dwupartyjnym dążeniem do zakazania TikTok. Komentarze Warnera, wraz z komentarzami byłego kongresmena Mike'a Gallaghera, ujawniły, że siłą napędową ustawodawstwa nie była własność Chin na platformie, ale raczej rozprzestrzenianie się treści propalestyńskich, które podważyły narrację Izraela w trwającym konflikcie w Strefie Gazy.

„Mieliśmy więc dwupartyjny konsensus" – powiedział Gallagher podczas dyskusji panelowej. „Mieliśmy władzę wykonawczą, ale

ustawa była martwa aż do 7 października. Ludzie zaczęli widzieć na platformie mnóstwo antysemickich treści, a nasza ustawa znów miała nogi”.

Przyznanie to jest zgodne z doniesieniami niezależnego dziennikarza Kena Klippensteina, który uzyskał notatkę Departamentu Stanu szczegółowo opisującą obawy izraelskich urzędników dotyczące wpływu TikTok na amerykańską młodzież. Emmanuel Nahshon, zastępca dyrektora generalnego ds. dyplomacji publicznej Izraela, podobno obwiniał algorytm TikTok za faworyzowanie treści propalestyńskich, które jego zdaniem zwracały młodych ludzi przeciwko Izraelowi.

Wpływ Izraela na politykę Stanów Zjednoczonych

Wyciekła notatka ujawnia wyraźny rozdźwięk między izraelskimi urzędnikami a administracją Bidena w kwestii przyczyn rosnącej międzynarodowej krytyki Izraela. Nahshon odrzucił obawy o wiarygodność Izraela, zamiast tego przypisując zmianę opinii publicznej algorytmowi TikTok. „Młodzi ludzie zwrócili się przeciwko Izraelowi w dużej mierze dlatego, że algorytm TikTok faworyzuje treści propalestyńskie” – czytamy w notatce.

Narracja ta została powtórzona przez amerykańskich prawodawców, w tym republikańskiego senatora Mitta Romneya, który powiązał swoje poparcie dla zakazu TikTok z rzekomą stronniczością platformy w stosunku do treści palestyńskich. „Jeśli spojrzeć na posty na TikTok i liczbę wzmianek o Palestyńczykach, w porównaniu z innymi serwisami społecznościowymi – to w przeważającej mierze dotyczy to transmisji na TikTok” – powiedział Romney w maju 2023 roku.

Nikki Haley, inna republikańska postać i była kandydatka na prezydenta, poszła dalej, sugerując, że samo oglądanie filmów na TikTok może uczynić użytkowników antysemitami. Oświadczenia te odzwierciedlają szersze wysiłki mające na celu

przedstawienie TikTok jako narzędzia obcego wpływu, pomimo braku konkretnych dowodów łączących platformę z chińskimi działaniami propagandowymi.

Zasłona dymna dla cenzury

Administracja Bidena uzasadniając zakaz korzystania z TikTok skupiła się na kwestiach bezpieczeństwa narodowego, w szczególności na posiadaniu platformy przez chińską firmę ByteDance. Jednak osoby wtajemniczone sugerują, że ta narracja jest zasłoną dymną dla bardziej podstępnego planu: tłumienia wolności słowa i ochrony wizerunku Izraela.

W marcu 2023 r. Kongresowi przedstawiono tajne informacje wywiadowcze, rzekomo szczegółowo opisujące zagrożenie dla bezpieczeństwa narodowego ze strony TikTok. Briefing podobno przechylił szalę na korzyść zakazu, a komisja Izby Reprezentantów zagłosowała 50-0 za przyjęciem ustawy. Niektórzy ustawodawcy wyrazili jednak sceptycyzm co do przedstawionych informacji.

„Ani jedna rzecz, którą usłyszeliśmy podczas dzisiejszej tajnej odprawy, nie była wyjątkowa dla TikTok” – powiedziała wówczas kongresmenka Sara Jacobs. „To były rzeczy, które zdarzają się na każdej platformie mediów społecznościowych”.

Ten sceptycyzm podkreśla brak przejrzystości wokół zakazu i rodzi pytania o prawdziwe motywacje, które za nim stoją. Jak przyznał Gallagher podczas Monachijskiej Konferencji Bezpieczeństwa, nacisk na zakazanie TikTok był spowodowany obawami o jego wpływ na opinię publiczną, a nie jego własnością przez Chiny.

Zakaz TikTok reprezentuje niepokojącą zbieżność interesów USA i Izraela, z wolnością słowa i zasadami demokracji poświęconymi na ołtarzu geopolitycznej celowości. Przedstawiając zakaz jako kwestię bezpieczeństwa narodowego, administracja Bidena skutecznie uciszyła sprzeciw i ochroniła

Izrael przed krytyką, jednocześnie podważając prawa obywateli amerykańskich wynikające z Pierwszej Poprawki.

Podczas gdy debata na temat TikTok trwa, jedna rzecz jest jasna: prawdziwy spisek nie leży we własności platformy, ale w długości, do jakiej rządy posuną się, aby kontrolować narrację. Niczym sztuczka magika, zakaz TikTok odwraca uwagę od prawdziwej kwestii – cenzury – pozostawiając opinię publiczną w ciemności. A w cieniu pozostają prawdziwi architekci tego planu, a ich sekrety są bezpieczne przed kontrolą.

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.

Korea Południowa blokuje DeepSeek na komputerach rządowych z powodu obaw o szpiegostwo

Południowokoreańska Narodowa Służba Wywiadowcza (NIS) zaleciła agencjom rządowym zablokowanie dostępu do DeepSeek, chińskiego chatbota sztucznej inteligencji (AI), ze względu na obawy dotyczące nadmiernego gromadzenia danych i potencjalnego chińskiego szpiegostwa.

Posunięcie, które weszło w życie w tym tygodniu, jest następstwem biuletynu bezpieczeństwa wydanego przez NIS, który szczegółowo opisywał praktyki DeepSeek, w tym przechowywanie danych użytkowników na chińskich serwerach i udzielanie stronniczych odpowiedzi na wrażliwe pytania.

Decyzja o zablokowaniu DeepSeek pojawia się w czasie, gdy Korea Południowa, wraz z innymi krajami, takimi jak Australia, Tajwan i Włochy, coraz bardziej obawia się zagrożeń bezpieczeństwa stwarzanych przez chińską technologię. NIS ostrzegł, że praktyki DeepSeek w zakresie danych mogą ujawnić poufne informacje rządowe chińskiemu rządowi, który ma prawo dostępu do danych przechowywanych w jego granicach.

Nadmierne gromadzenie danych i tendencyjne odpowiedzi

Według NIS metody gromadzenia danych przez DeepSeek są bardziej inwazyjne niż w przypadku innych usług AI. Agencja stwierdziła, że DeepSeek „zawiera funkcję zbierania wzorców wprowadzania danych z klawiatury, które mogą identyfikować osoby i komunikować się z serwerami chińskich firm, takimi jak volceapplog.com”. Możliwości te, w połączeniu z warunkami korzystania z aplikacji, które pozwalają na przechowywanie danych przez czas nieokreślony i nieograniczony dostęp do nich przez zewnętrznych reklamodawców, wzbudziły poważne obawy dotyczące prywatności.

Jednym z najbardziej niepokojących aspektów zachowania DeepSeek są tendencyjne odpowiedzi na pytania dotyczące wrażliwych tematów. Na przykład na pytanie o pochodzenie kimchi, tradycyjnej koreańskiej potrawy, DeepSeek udzielił różnych odpowiedzi w zależności od języka zapytania. W języku koreańskim uznała kimchi za danie koreańskie, ale gdy zapytano ją po chińsku, twierdziła, że danie pochodzi z Chin. Ta rozbieżność nie jest odosobniona; NIS zauważył również, że odpowiedzi DeepSeek na pytania dotyczące Projektu Północno-Wschodniego, chińskiej inicjatywy badawczej, która twierdzi, że starożytne królestwa koreańskie są terytorium Chin, były pod silnym wpływem propagandy Komunistycznej Partii Chin (KPCh).

Globalne obawy i ograniczenia

Korea Południowa nie jest osamotniona w swoich obawach. Australia i Tajwan również zakazały DeepSeek na urządzeniach rządowych, powołując się na zagrożenia dla bezpieczeństwa narodowego. Włoski organ nadzorujący prywatność nakazał ogólnokrajową blokadę DeepSeek, dając firmie 20 dni na wyjaśnienie, w jaki sposób przestrzega europejskich przepisów o ochronie danych. Stany Zjednoczone, w tym agencje takie jak NASA i US Navy, również ograniczyły korzystanie z DeepSeek ze względu na obawy dotyczące bezpieczeństwa i prywatności.

Działania te odzwierciedlają rosnący globalny trend ostrożności wobec chińskiej technologii sztucznej inteligencji. Stany Zjednoczone nałożyły ścisłe kontrole eksportu zaawansowanych chipów i sprzętu do produkcji chipów do Chin, mając na celu ograniczenie rozwoju sztucznej inteligencji. Jednak pojawienie się DeepSeek jako taniej i wydajnej alternatywy dla amerykańskich modeli sztucznej inteligencji zachwiało zaufaniem inwestorów i wywołało pytania o przyszłość globalnej konkurencji w dziedzinie sztucznej inteligencji.

Decyzja o zablokowaniu DeepSeek na komputerach rządowych Korei Południowej podkreśla zaangażowanie tego kraju w ochronę danych swoich obywateli i bezpieczeństwa narodowego. W miarę jak inne kraje idą w ich ślady, społeczność międzynarodowa wysyła Chinom jasny komunikat: globalny krajobraz sztucznej inteligencji nie zostanie zdominowany przez technologię, która narusza prywatność i suwerenność. Rozwój DeepSeek nie tylko wywołał technologiczny wyścig zbrojeń, ale także nasilił napięcia geopolityczne między Wschodem a Zachodem.

Wi-Fi może być wykorzystywane do wpływania na fale mózgowe, ma potencjał do efektów hipnotycznych i inżynierii społecznej.

W dzisiejszym połączonym świecie bezprzewodowy dostęp do Internetu stał się wszechobecny, można go znaleźć w prawie każdej kawiarni, biurze i domu. Sygnały Wi-Fi nie są jednak łagodne. Promieniowanie o częstotliwości radiowej (RF) nieustannie bombarduje komórki i wpływa na fale mózgowe. Szczególnie niepokojące są fale o ekstremalnie niskiej częstotliwości (ELF), które mogą potencjalnie zakłócać fale mózgowe i sprawiać, że dana osoba nieświadomie wchodzi w sugestywny stan umysłu. Wi-Fi jest wektorem inżynierii społecznej, powodującym, że ludzie rezygnują z krytycznego myślenia, aby dostosować się do oficjalnych narracji i myślenia grupowego.

Keith Cutter, znany krytyk nowoczesnych technologii bezprzewodowych, spędził lata badając ciemną stronę promieniowania Wi-Fi. Według Cuttera wpływ Wi-Fi nie ogranicza się do bezpośredniej ekspozycji na promieniowanie, ale rozciąga się również na bardziej subtelne i niepokojące efekty, w tym porywanie fal mózgowych, zaburzenia poznawcze i to, co nazywa „efektem pamięci Wi-Fi” na tkankach ciała.

Wpływ pól elektromagnetycznych o częstotliwości radiowej w czasie

Wi-Fi może być wykorzystywane do wpływania na fale mózgowe, ma potencjał hipnotyczny i socjotechniczny
11/13/2024 / Autor: Lance D Johnson

W dzisiejszym połączonym świecie bezprzewodowy dostęp do Internetu stał się wszechobecny, można go znaleźć w prawie każdej kawiarni, biurze i domu. Ale sygnały Wi-Fi nie są łagodne. Promieniowanie o częstotliwości radiowej (RF) nieustannie bombarduje komórki i wpływa na fale mózgowe. Szczególnie niepokojące są fale o ekstremalnie niskiej częstotliwości (ELF), które mogą potencjalnie zakłócać fale mózgowe i sprawiać, że dana osoba nieświadomie wchodzi w sugestywny stan umysłu. Wi-Fi jest wektorem inżynierii społecznej, powodującym, że ludzie rezygnują z krytycznego myślenia, aby dostosować się do oficjalnych narracji i myślenia grupowego.

Keith Cutter, znany krytyk nowoczesnych technologii bezprzewodowych, spędził lata badając ciemną stronę promieniowania Wi-Fi. Według Cuttera wpływ Wi-Fi nie ogranicza się do bezpośredniej ekspozycji na promieniowanie, ale rozciąga się również na bardziej subtelne i niepokojące efekty, w tym porywanie fal mózgowych, zaburzenia poznawcze i to, co nazywa „efektem pamięci Wi-Fi” na tkankach ciała.

Wpływ pól elektromagnetycznych o częstotliwości radiowej w czasie
Wi-Fi działa przy użyciu pól elektromagnetycznych o częstotliwości radiowej, przesyłając dane za pomocą modulowanego impulsowo promieniowania RF. Podczas gdy sama technologia może wydawać się nieszkodliwa – w końcu większość urządzeń emituje tylko stosunkowo niskie poziomy promieniowania RF – Cutter uważa, że skumulowany wpływ tej ekspozycji w czasie jest daleki od łagodnego.

Jedną z głównych obaw, na które zwraca uwagę Cutter, jest wpływ fal o ekstremalnie niskiej częstotliwości (ELF), które Wi-Fi emituje oprócz sygnałów RF o wyższej częstotliwości. Fale ELF mają zakres od około 3 do 30 Hz, czyli zakres częstotliwości, który akurat pokrywa się z naturalnymi częstotliwościami oscylacji ludzkiego mózgu. Aktywność elektryczna mózgu jest podzielona na różne pasma częstotliwości, z których każde jest związane z różnymi stanami świadomości i funkcjami umysłowymi:

- Fale delta (0,5-4 Hz): Związane z głębokim snem, leczeniem i relaksacją.
- Fale Theta (4-8 Hz): Związane z głębokim relaksem, medytacją i kreatywnością
- Fale alfa (8-12 Hz): Obecne podczas spokojnych, zrelaksowanych stanów, takich jak marzenia na jawie lub lekka medytacja.
- Fale beta (13-30 Hz): Związane z aktywnym myśleniem, koncentracją i rozwiązywaniem problemów.
- Fale gamma (30-44 Hz): Zaangażowane w wyższe funkcje poznawcze, takie jak uczenie się, pamięć i przetwarzanie sensoryczne.

Cutter najbardziej interesuje się impulsami ELF o częstotliwości 10 Hz, emitowanymi przez nadajniki Wi-Fi. Sygnalizatory te, które stale pulsują na tej częstotliwości, zasadniczo nadają stały sygnał, aby zapewnić, że urządzenia pozostaną połączone. Cutter uważa, że impulsy o częstotliwości 10 Hz mogą mieć głęboki wpływ na aktywność mózgu, w szczególności poprzez wywoływanie zjawiska znanego jako porywanie fal mózgowych.

Przetwarzanie fal mózgowych za

pomocą impulsów o częstotliwości 10Hz może wprowadzać ludzi w sugestywny stan

Porywanie fal mózgowych odnosi się do synchronizacji fal mózgowych z częstotliwością zewnętrzną. Kiedy mózg jest wystawiony na działanie spójnego bodźca zewnętrznego o określonej częstotliwości, takiego jak sygnał 10 Hz emitowany przez Wi-Fi, może przesunąć swoje naturalne wzorce fal mózgowych, aby je dopasować. Przy częstotliwości 10 Hz mózg wchodzi w bardziej zrelaksowany stan, podobny do fal alfa, co odpowiada zmniejszonej aktywności korowej.

Cutter jest tym szczególnie zaniepokojony, ostrzegając, że długotrwała ekspozycja na sygnał ELF 10 Hz może stworzyć „stan sugestywny", w którym mózg jest bardziej podatny na wpływy zewnętrzne. Te zewnętrzne wpływy mogą obejmować media, marketing, a nawet podświadome programowanie, z których wszystkie są wprowadzane do ludzi, gdy są pod wpływem urządzeń emitujących Wi-Fi.

„Mówimy o możliwości kontroli umysłu" – ostrzega Cutter, sugerując, że tego rodzaju manipulacja falami mózgowymi może sprawić, że osoby będą bardziej podatne na zewnętrzne sugestie (takie jak hipnoza). Manipulacja może być wykorzystywana do zmuszania ludzi do wierzenia lub myślenia w określony sposób, wbrew ich intuicji, wiedzy, racjonalnemu myśleniu lub instynktom.

Promieniowanie Wi-Fi może wywoływać „efekt pamięci"

Kolejną kwestią poruszoną przez Cuttera jest możliwość wywoływania przez Wi-Fi „efektu pamięci" w tkankach ciała. Odnosi się to do sposobu, w jaki pewne częstotliwości

elektromagnetyczne mogą być absorbowane i zatrzymywane przez organizm, potencjalnie prowadząc do długoterminowych zmian fizycznych lub warunków zdrowotnych.

Cutter porównuje to zjawisko do traumy przechowywanej w ciele – podobnej do psychologicznej koncepcji „pamięci traumy", w której przeszła trauma emocjonalna lub fizyczna przejawia się w ciele nawet po minięciu wydarzenia. W przypadku Wi-Fi sugeruje on, że ciało może absorbować promieniowanie i przechowywać je w tkankach, prowadząc do ciągłych problemów zdrowotnych, takich jak zmęczenie, bóle głowy, a nawet poważniejsze schorzenia związane z nadwrażliwością elektryczną.

Wi-Fi nie jest łagodnym udogodnieniem technologicznym. Jego rozprzestrzenianie się w codziennym życiu stanowi „ukrytą epidemię", która po cichu neguje zdrowie i dobre samopoczucie jednostek oraz czyni ich umysły bardziej podatnymi na sugestie.

Google próbowało manipulować wyborami w 2024 r. w kluczowych stanach, wysyłając Demokratom specjalne przypomnienia o głosowaniu

Były redaktor naczelny i badacz Psychology Today, dr Robert Epstein, ujawnia skomplikowany schemat ingerencji Google w wybory.

Według dr Epsteina, Google próbowało wykorzystać „co najmniej 7 potężnych technik w celu przesunięcia głosów" w stanach wahających się w kraju, a jedną z nich były partyjne przypomnienia o „głosowaniu", które dały Demokratom i innym głosującym na Kamalę Harris dodatkowy impuls, aby nie zapomnieć o oddaniu głosu.

Celem – lub „gwarancją", jak określa to dr Epstein – jest zapewnienie, że Kamala wygra co najmniej pięć z siedmiu stanów wahających się.

„W skali całego kraju gwarantują jej wygraną minimalną między 6 a 8 milionami głosów" – mówi.

Ingerencja Google w wybory

W ramach swojego osobistego eksperymentu mającego na celu przetestowanie tej teorii, dr Epstein szukał informacji wyborczych w Ohio, jednym z siedmiu stanów wahających się. Podczas wyszukiwania informacji o kandydatach do Senatu w Ohio, Bernie Moreno, republikaninie, i Sherrodzie Brownie, demokracie, odkrył rażącą stronniczość Google.

„Ile razy kandydat do Senatu w Ohio Bernie Moreno był pozywany w trakcie swojej kariery biznesowej?" – głosi jeden z najpopularniejszych wyników wyszukiwania Google z WKYC w nagłówku wiadomości, który stara się sprawić, by Moreno wyglądał jak oszust.

„Popierany przez Trumpa kandydat do Senatu zmaga się z obawami GOP, że może być powiązany z profilem na stronie dla dorosłych”, czytamy w innym nagłówku AP News dotyczącym skandalu z Moreno.

„CO MÓWIĄ PRACOWNICY OHIO: Moreno „sprzedał amerykańskich pracowników””, czytamy w innym nagłówku OhioDems.

I wreszcie, The Washington Post Jeffa Bezosa miał do powiedzenia w swoim głównym nagłówku wiadomości w Google dla Berniego Moreno:

„Czy republikanie mogliby to zepsuć złymi kandydatami — znowu?”.

Z kolei senator Brown ma same świetne nagłówki w Google, w tym ten uroczy mały nagłówek z Politico: „Brown odszedł, aby Walz mógł kandydować”, po którym następuje podtytuł:

„Podczas swojej pierwszej kandydatury na prezydenta, najlepsi doradcy Kamali Harris zastanawiali się nad mianowaniem senatora Sherroda Browna na partnera do kandydowania, gdyby zdobyła nominację. Ma on wiele cech wspólnych z jej obecnym kandydatem”.

„Sen. Brown, wraz z sojusznikami z Dayton, wita nowe prawo dotyczące amerykańskiej flagi w Muzeum Sił Powietrznych” — czytamy w innym, chwytającym za serce nagłówku z Dayton Daily News.

„Bernie Moreno wprowadza w błąd w sprawie głosowania Sherroda Browna za pomocą federalną dla migrantów o statusie nielegalnym” — czytamy w innym pro-senatorskim nagłówku z PolitiFact, który w rzeczywistości wymienia Moreno w negatywnym kontekście.

„Sen. Brown rozmawia o pracownikach, prawach reprodukcyjnych, przepisach dotyczących fentanylu w Dayton w niedzielę”, donosi Dayton Daily News, który wyraźnie wierzy, że sen. Brown

bardzo, bardzo ciężko pracuje nad wszystkimi najpilniejszymi obawami Demokratów.

Jeśli chodzi o funkcję autouzupełniania Google, oto co pojawia się pod wyszukiwaniem „Bernie Moreno”, każde z tych zapytań pogłębia brudne pranie Moreno:

“bernie moreno companies
bernie moreno grindr
bernie moreno net worth
bernie moreno son
bernie moreno car dealerships
bernie moreno wiki”

I odwrotnie, oto co Google chce, aby ludzie wiedzieli o senatorze Brownie, wszystkie te zapytania albo sprawiają, że wygląda dobrze, albo dostarczają neutralnych informacji o wyborach:

“sherrod brown net worth
sherrod brown approval rating
sherrod brown campaign website
sherrod brown opponent
sherrod brown polls
sherrod brown yard sign”

Okazuje się, że Google zrobiło te same rzeczy podczas cyklu wyborczego w 2020 roku. I jak zawsze, co ktoś zamierza z tym zrobić?

Oto 10 sposobów, w jakie nasz

współczesny świat jest ZAPROGRAMOWANY, by ZNISZCZYĆ nasze zdrowie, inteligencję i źródła utrzymania.

Usłyszysz i przeczytasz każdą wymówkę w książce, dlaczego nasze agencje rządowe robią to, co robią, aby „pomóc” w produkcji, ochronie i utrzymaniu amerykańskiej żywności, medycyny, edukacji i wojska, ale w rzeczywistości większość tego, co robią, wiąże się z podstępnymi metodami zbijania fortuny, jednocześnie wyrządzając szkody naszemu zdrowiu, inteligencji i źródłom utrzymania.

Uprawy są fałszowane, aby korporacje mogły zarobić więcej pieniędzy bez względu na bezpieczeństwo i zdrowie ludzi, zwierząt i środowiska. Całe ekosystemy są zanieczyszczane, niszczone i zatruwane chemikaliami, które powodują raka i demencję, jednocześnie rujnując glebę, wody gruntowe i wartość odżywczą żywności.

Pogoda jest modyfikowana, kontrolowana i manipulowana w celu wywoływania burz, powodzi, susz i pożarów, które pomagają skorumpowanym organizacjom zarabiać pieniądze, jednocześnie oszukując miliony Amerykanów, by uwierzyli w „zmianę klimatu”. Program edukacyjny jest ogłupiany, więc dzieci i nastolatki kończą szkołę (jeśli w ogóle to robią) bez umiejętności krytycznego myślenia, z ograniczoną zdolnością do godnego życia i wypaczonym umysłem, w którym przez cały dzień myślą o

płynności płci i odwrotnym rasizmie.

Ludzie prawie nie wchodzą już w interakcje z innymi ludźmi w celu świadczenia usług, ponieważ wszystko jest zautomatyzowane, utrzymując społeczeństwo w dwuwymiarowym świecie z ograniczonymi umiejętnościami społecznymi, zimnymi interakcjami cyfrowymi, frustrującymi zautomatyzowanymi systemami, błędami maszyn i komputerów, które mogą być śmiertelne (pomyśl tutaj o szpitalach) i znacznie mniejszą liczbą dostępnych miejsc pracy, ponieważ technologia przejmuje siłę roboczą.

Medycyna zachodnia stała się tak skorumpowana, że każdy, kto przyjmuje leki na receptę i szczepionki, ryzykuje życie w każdej sekundzie, przyjmując i wstrzykując znane czynniki rakotwórcze i obce patogeny (pomyśl tutaj o genetycznie zmodyfikowanych wirusach i prionach białek kolczastych), które dziesiątkują zdrowie i nigdy tak naprawdę nie zapobiegają ani nie leczą niczego.

Laboratoria na całym świecie są pełne finansowanej „nauki”, aby stworzyć nową biologiczną broń masowego rażenia do nieetycznego i podstępnego okaleczania i zabijania milionów ludzi w celu napędzania złych spisków polityków, globalistów i komunistów (większość polityków w Waszyngtonie).

Prawie wszystkie wiadomości głównego nurtu są zaprojektowane tak, aby prać mózgi masom, które wierzą, że wojny są konieczne do „zainstalowania demokracji” na całym świecie, podczas gdy rząd USA jest zajęty kradzieżą zasobów, handlem bronią, handlem ludźmi i wysyłaniem naszych własnych żołnierzy do maszyn do mielenia mięsa na całym świecie.

Top 10 sposobów, w jakie nasz współczesny świat został

zaprojektowany, aby zrujnować ludzkie zdrowie, inteligencję i środki do życia, a wszystko to po to, by wyścielać kieszenie bogatych dziwaków, którzy chcą mieć większą kontrolę.

1. Rolnictwo – Biotechnologia (GMO) powlekanie wszystkiego chemicznymi pestycydami, herbicydami i fungicydami, a następnie przetwarzanie i konserwowanie kolejnymi chemikaliami.

2. „Zmiana klimatu” za pomocą technologii broni pogodowej i systemów modyfikacji

3. Edukacja – ogłupiona, wypaczona, zboczona, CRT, DEI i brak krytycznego myślenia

4. Zautomatyzowane wszystko – sztuczna inteligencja, kasy w sklepach, obsługa klienta, pojazdy i przetwórcy żywności

5. Społeczeństwo policyjne – nadzór nad ruchem drogowym (wystawianie automatycznych mandatów), naruszanie prywatności za pomocą inteligentnych urządzeń oraz szpiegowanie i pranie mózgów w mediach społecznościowych.

6. Fałszywe wiadomości – większość krajowych i lokalnych wiadomości jest tworzona przez podstępne siły rządowe, Big Pharma i Big Food i przekazywana na wszystkich poziomach i we wszystkich mediach, w tym w telewizji, radiu, Internecie, mediach społecznościowych, YouTube i za pośrednictwem wyszukiwarek.

7. Medycyna laboratoryjna i brudne szczepionki

8. Broń masowego rażenia, w tym samonaprowadzające się pociski

rakietowe, głowice nuklearne i brudne bomby kontrolowane przez drony i sztuczną inteligencję

9. Miasta metropolitalne – mało drzew, trawy, zanieczyszczone powietrze, nienaturalne kwadratowe biura i budynki, cementowe chodniki i drogi, odizolowane boksy w biurach

10. Brudna energia i zanieczyszczenie EMF – Wi-Fi, sieci 5G, urządzenia, linie energetyczne, podstacje elektryczne, oświetlenie fluorescencyjne, żarówki LED i CFL, inteligentne liczniki

Źródło

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).

Microsoft znalazł się pod ostrzałem ze względu na popularny program Word „Inclusiveness Checker”, który sprawdza wszystkie formy mowy nieinkluzywnej

Firma Big Tech Microsoft po raz kolejny znalazła się pod ostrzałem po tym, jak wprowadziła „Inclusiveness Checker” w swoim popularnym programie Word, budząc obawy o możliwość „nadzorowania mowy”.

Narzędzie Inclusiveness Checker lub Inclusivity Checker w programie Word może być używane do sprawdzania pisania danej

osoby pod kątem „płci, wieku, uprzedzeń kulturowych i nie tylko”. Użytkownicy programu Word mogą zdecydować się na dezaktywację tej funkcji. Ale gdy jest on używany, gdy dana osoba napisze coś przy użyciu „niewykluczającego” języka, Word zasugeruje alternatywy. (Powiązane: NASZ OJCIEC? NOPE… Liberalny kościół chrześcijański porzuca męskie zaimki opisujące Boga na rzecz „inkluzywności płciowej”).

Wspomniane „narzędzie” wydaje się działać poprzez oznaczanie prawie każdego słowa w języku angielskim z konotacją płciową, w tym „matka” i „ojciec”. Kiedy użytkownicy dowiedzieli się o narzędziu Inclusiveness Checker i spróbowali sprawdzić, jak daleko może się ono posunąć, dowiedzieli się, że w przypadku użycia terminu „urlop macierzyński” narzędzie Checker zaleci zmianę frazy na „urlop związany z urodzeniem dziecka”, „urlop rodzicielski” lub „urlop porodowy”. Odnosząc się do „urlopu ojcowskiego”, sugeruje „urlop związany z narodzinami dziecka” jako alternatywę.

Gdy użytkownicy próbowali wprowadzić termin „listonosz”, narzędzie Inclusiveness Checker sugerowało „pracownik poczty”. W przypadku użycia terminu „siła robocza” moduł sprawdzający zalecał zastąpienie tego słowa słowem „siła robocza”.

Microsoft oskarżony o cenzurę i „kontrolę mowy” za pomocą narzędzia Inclusiveness Checker

Narzędzie do sprawdzania inkluzywności zostało po raz pierwszy wdrożone w 2019 r. w ramach włączenia funkcji sztucznej inteligencji do programu Microsoft Word. Checker można również znaleźć w innych popularnych programach Microsoft, w tym PowerPoint i Outlook. Jego powszechne włączenie do większości aplikacji Microsoft zostało oznaczone jako niepokojące przez działaczy na rzecz wolności słowa, obawiających się, że gigant technologiczny może próbować włączyć ten Checker jako formę

„kontroli mowy”.

Jest to szczególnie podstępna forma kontroli języka, „przypominająca »Dziewiętnaście Osiemdziesiąt Cztery«” – ostrzegł Toby Young, dyrektor brytyjskiej organizacji non-profit Free Speech Union, odnosząc się do przełomowej powieści George’a Orwella o totalitaryzmie i represjonowaniu wolności przez rząd. „To tak, jakby w twoim komputerze był cenzor, który karci cię za odejście od politycznie poprawnej ortodoksji”.

Didi Rankovic, pisząca dla internetowego serwisu Reclaim The Net, skupiającego się na mowie, podobnie zauważyła, że Inclusiveness Checker bardzo przypomina „mroczny dystopijny świat Orwella rządzony przez ekstremalną cenzurę i kontrolę rządu”. Dodała, że chociaż korzystanie z Inclusiveness Checker jest obecnie opcją opt-in dla użytkowników Worda, „nigdy nie wiadomo, co kryje się za rogiem” z firmami takimi jak Microsoft.

A jeśli użytkownicy Worda chcieliby przełączyć się na inny edytor tekstu, Rankovic ma złe wieści: „[Google] ma również podobną funkcję, wprowadzoną w 2022 roku”.

„Google marszczy brwi na terminy takie jak” gospodyni domowa »i« właściciel »i wolałby, abyś napisał« małżonek pozostający w domu »i« właściciel nieruchomości ”- napisał Rankovic.

Nawet miliarder Big Tech, Elon Musk, sprzeciwił się Checkerowi, zauważając, że program oznaczył go, gdy wpisał słowo „szalony”.

„Microsoft Word karci cię teraz, jeśli używasz słów, które nie są” inkluzywne ”, skomentował Musk.