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".

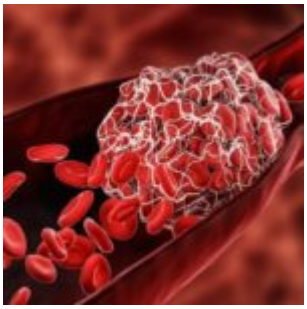
Obrońcy prywatności są szczególnie zaniepokojeni nieprzejrzystym charakterem i potencjałem nadmiernego wykorzystania sztucznej inteligencji w przestrzeni publicznej.Hurfurt wyraził poważne obawy dotyczące normalizacji takiego inwazyjnego nadzoru bez odpowiedniego publicznego dyskursu lub nadzoru.

„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".

Badanie wykazało, że szczepionki przeciw COVID wywołują 723 razy więcej zakrzepów mózgu niż szczepionki przeciw grypie



Nowe badanie pre-print przeprowadzone przez dr Petera McCullougha i kilku współpracowników ujawnia, że „szczepionki" na koronawirusa Wuhan (COVID-19) są znacznie bardziej niebezpieczne niż sezonowe szczepionki przeciw grypie, jeśli chodzi o wywoływanie mózgowych zespołów zakrzepowo-zatorowych, znanych również jako zakrzepy mózgowe.

W populacyjnym retrospektywnym badaniu kohortowym, które nie zostało jeszcze poddane wzajemnej weryfikacji, przeanalizowano wskaźniki zdarzeń niepożądanych obejmujących mózgową chorobę zakrzepowo-zatorową (CTE) po wstrzyknięciu COVID. Obejmuje ono dane z bazy danych Vaccine Adverse Event Reporting System (VAERS), zarządzanej przez U.S. Centers for Disease Control and Prevention (CDC) i U.S. Food and Drug Administration (FDA), w okresie od 1 stycznia 1990 r. do 31 grudnia 2023 r.

Dr. McCullough i jego koledzy porównali wskaźniki CTE po zaszczepieniu COVID z wskaźnikami CTE po zaszczepieniu grypą, co doprowadziło ich do odkrycia, że szczepionki COVID są znacznie bardziej ryzykowne niż szczepionki przeciw grypie.

W ciągu trzech lat po uwolnieniu szczepionek COVID w ramach operacji Warp Speed zgłoszono 5 137 przypadków CTE. Dla porównania, szczepionki przeciw grypie w ciągu ostatnich 34 lat spowodowały tylko 52 przypadki CTE.

Należy zauważyć, że w ciągu ostatnich 34 lat wszystkie szczepionki łącznie spowodowały tylko 282 przypadki CTE w porównaniu do 5 137 przypadków CTE spowodowanych zastrzykami COVID w ciągu zaledwie trzech lat. To tylko pokazuje, jak bardzo niebezpieczne są zastrzyki COVID w porównaniu do wszystkich innych zastrzyków farmaceutycznych pod względem

krzepnięcia ludzkich mózgów.

Obejrzyj poniższy film, w którym dr McCullough mówi o ryzyku rozwoju „raka turbo” po wstrzyknięciu COVID:

> *Dr. Peter McCullough Sounds the Alarm on COVID Vaccine-Induced “Turbo Cancer”*
> *pic.twitter.com/rPgsedayXv*
>
> *— Antonio Sabato Jr (@AntonioSabatoJr) April 16, 2024*

Pomiń zastrzyki

Kobiety mają większe niż mężczyźni ryzyko rozwoju CTE po wstrzyknięciu COVID, jak wykazało badanie. Migotanie przedsionków, najczęstsza możliwa do zidentyfikowania przyczyna CTE, jest również znacznie częstsze po wstrzyknięciu COVID niż w przypadku jakiegokolwiek innego zastrzyku obecnie dostępnego na rynku.

W swoim wniosku dr McCullough i jego koledzy zdecydowanie ostrzegają przed niebezpieczeństwami związanymi z wstrzyknięciem COVID, wzywając jednocześnie do wycofania wszystkich takich zastrzyków z rynku.

„Istnieje alarmujące naruszenie progu sygnału bezpieczeństwa dotyczącego AE zakrzepicy mózgowej po szczepionkach COVID-19 w porównaniu ze szczepionkami przeciw grypie, a nawet w porównaniu ze wszystkimi innymi szczepionkami” – napisali.

„Konieczne jest natychmiastowe globalne moratorium na stosowanie szczepionek przeciwko COVID-19 z bezwzględnym przeciwwskazaniem u kobiet w wieku rozrodczym”.

Dr McCullough jest zaniepokojony faktem, że Donald Trump, który wielokrotnie nazywał siebie „ojcem szczepionki” w odniesieniu do zastrzyków COVID, które szybko wprowadził na

rynek, nie mówi nic o zagrożeniach związanych z zastrzykami, które forsował przez ostatnie prawie pięć lat.

> *Dr. McCullough's Talking Points for Trump on COVID-19 Vaccines*
>
> *Dr. Gina Loudon asked what should former president and current candidate Donald Trump say about the COVID-19 vaccine debacle? This is an issue both sides of the isle want to hear about from the candidates. It could… pic.twitter.com/pAltxcjUm0*
>
> *— Peter A. McCullough, MD, MPH® (@P_McCulloughMD) July 6, 2024*

„Trump musi przeprosić za operację Warp Speed i za swoją rolę w uwolnieniu broni biologicznej, która jest ludobójstwem dla nas i naszych dzieci" – napisał ktoś na X, popierając apele dr McCullougha o śledztwo w sprawie Trumpa i wszystkich innych, którzy wypchnęli zastrzyki na Amerykanów.

„Ludzie z branży medycznej muszą przestać kryć firmy farmaceutyczne".

Szpital dziecięcy w Kijowie trafiony ukraińską rakietą, nie rosyjską

Długo oczekiwany szczyt NATO w Waszyngtonie odbył się właśnie w dniach 7-9 lipca, a najnowsze wiadomości na temat operacji zachodniego sojuszu na Ukrainie pokazują, że zachodnia machina propagandowa kłamie jak szalona na temat tego konfliktu.

New York Times opublikował zwodniczy artykuł na pierwszej stronie z nagłówkiem „Russia Strikes Children's Hospital in Deadly Barrage Across Ukraine", który jest całkowicie fałszywy, ponieważ to Kijów, a nie Moskwa, zbombardował szpital dziecięcy. Inne główne media w Stanach Zjednoczonych, Wielkiej Brytanii, Europie, a nawet Al Jazeera papugowały to twierdzenie, tylko po to, by zostało ono obalone przez niezależne media.

The Times fałszywie poinformował przed szczytem NATO, że „rosyjska rakieta" była odpowiedzialna za zniszczenie „największego ukraińskiego szpitala dziecięcego". Artykuł zawierał niepokojące zdjęcia zakrwawionych i rannych dzieci, gdy ratownicy spieszyli na miejsce zdarzenia, aby usunąć poskręcany metal, rozbity beton i inne gruzy z okolicy w poszukiwaniu ocalałych.

„Uderzenie w szpital było częścią barażu bombardowań Moskwy w całym kraju, w tym jednego z najbardziej śmiercionośnych ataków na Kijów od pierwszych miesięcy wojny" – skłamał Times.

„Co najmniej 38 osób zginęło w całym kraju, w tym 27 w Kijowie. Ponad 100 osób zostało rannych. Ukraińskie siły powietrzne oświadczyły, że zestrzeliły 30 z 38 pocisków wystrzelonych przez Rosję podczas ataku, który rozpoczął się w godzinach porannych".

Artykuł zawierał nawet fałszywy cytat z Serhija Popko, szefa ukraińskiej administracji wojskowej, opisujący atak jako „masowy", ponieważ obejmował „pociski lotnicze, balistyczne i manewrujące", które „leciały na stolicę falami i z różnych kierunków".

Atak spowodował śmierć co najmniej jednego lekarza, jednego dorosłego niebędącego lekarzem i co najmniej 10 dodatkowych obrażeń, z których siedmioro to dzieci. Co najmniej troje dzieci zostało wyciągniętych spod gruzów.

Ukraina kłamie

Media głównego nurtu oszalały na punkcie tej historii, próbując wskazać Rosję jako winowajcę, aby uzyskać większe poparcie społeczne dla dalszego finansowania. Prawda jest jednak taka, że to niecelny pocisk obrony powietrznej wystrzelony przez Ukrainę zniszczył szpital dziecięcy.

„To, co jest naprawdę wymowne, to fakt, że w wiadomościach nie było ŻADNYCH informacji o innych miejscach trafionych przez rosyjskie pociski w Kijowie" – donosi Sonar 21. „Wiesz dlaczego? Ponieważ były to cele wojskowe i prawdopodobnie były ofiary na Zachodzie. Rosja zadała ten cios w świetle dziennym w godzinach pracy, aby zadać jak najwięcej ofiar osobom zajmującym się produkcją lub naprawą broni".

Ukraina kłamała również na temat liczby pocisków, które rzekomo spadły na szpital. Ukraińskie Siły Powietrzne wyrzuciły liczbę 38, twierdząc, że zestrzeliły 30 z tych 38 „rosyjskich pocisków".

Propaganda z pewnością nie jest niczym nowym, zwłaszcza w czasie wojny, ale kłamstwo dotyczące kijowskiego szpitala dziecięcego jest szczególnie irytujące ze względu na jego polityczne implikacje. Gdyby powiedziano prawdę o tym ataku, amerykańska opinia publiczna mogłaby zacząć dwa razy zastanawiać się nad wysyłaniem większej ilości broni i gotówki

Wołodymyrowi Zełenskiemu, którego wojsko wydaje się mieć wiele problemów z nie mordowaniem ukraińskich obywateli z powodu „pomyłek”.

„Nie zdziwiłbym się, gdybyśmy później dowiedzieli się, że atak na szpital dziecięcy w Kijowie był atakiem fałszywej flagi zorganizowanym przez mistrzów NATO i ukronazistowskie marionetki na dzień przed spotkaniem NATO w Waszyngtonie tylko po to, by zebrać wszystkich razem i zapewnić większe wsparcie Zełenskiemu i jego klice” – napisał jeden z komentatorów.