
MELT
ICE

Tienes en tus manos un zine que da cuenta de las herramientas de vigilancia que usa el Servicio de Control de Inmigración y Aduanas de los Estados Unidos (de aquí en adelante, el ICE) y de la información que hemos recabado sobre cómo puedes hacerle frente a esta tecnología. Esta revista es un reportaje de 404 Media, un sitio web (¡y ahora una publicación impresa, al parecer!) operado exclusivamente por periodistas investigativos. Como somos un grupo pequeño de periodistas que también son dueños de los medios de producción (el sitio web), tenemos la libertad de informar sobre los temas que nosotros consideramos más importantes, y durante el último año, lo más importante ha sido la campaña de deportación masiva de Donald Trump y la tecnología que la hace posible. Los datos aquí publicados provienen de bases de datos de compras del sector público; entrevistas con activistas, protestantes, abogados y expertos en libertades civiles; procesos judiciales; solicitudes de la Ley por la Libertad de la Información, e información que nos divulgaron fuentes confidenciales de empresas de tecnología y organismos gubernamentales.

READ MORE
Encontrarás versiones digitales de estos artículos y este zine en **404media.co/icezine** (la versión en español también está disponible en línea).

Nos sentimos seguros sobre la calidad de la información que entregamos, pero no sabemos con seguridad qué vaya a pasar de aquí en adelante o cómo ayudar a la gente a protestar y resistirse de forma más segura; en efecto, la información aquí contenida NO debe tomarse como una recomendación de cómo protestar o resistirse: el ICE tiene miles de millones de dólares de presupuesto y ha demostrado gran creatividad y crueldad a la hora de detener y arrestar personas. Por otra parte, las empresas de vigilancia ya conocen muchas de las técnicas usadas para evadir sus sistemas y saben que hay esfuerzos por "contaminar" los datos, por lo que trabajan día a día para mejorar su tecnología y contrarrestar estas estrategias. Como periodistas, nuestro trabajo es el investigar lo que ocurre en las calles, verificar la información obtenida y luego publicar nuestros reportajes. Considera este zine no como un manual de recomendaciones, sino como un compendio de información valiosa.

Nuestro plan nunca fue pasarnos la mayor parte del último año investigando al ICE, pero hemos visto como la agencia se transformó de una organización temible a una máquina de deportación con más recursos que la mayoría de los ejércitos. Hemos visto personalmente cómo se han tomado ciudades como Los Ángeles y Chicago; cómo han desatado redadas en ciudades, pueblos y lugares de trabajo de todo el país, y cómo han secuestrado a personas que estaban en sus casas o sus trabajos, andaban de compras o solo caminaban por la calle. Y a medida que todo esto ocurría, mantuvimos al público informado sobre cómo la Administración Trump ha usado el poder del gobierno federal y de la información que posee para potenciar el aparato de vigilancia del ICE.

Tecnologías y bases de datos creadas en gobiernos anteriores, pensadas para fines tan diversos como la recaudación de impuestos, ahora son usadas como fuentes de datos para rastrear y arrestar a inmigrantes indocumentados. En efecto, derribaron todas las paredes de privacidad y uso compartido de datos entre agencias gubernamentales. Tomaron los sistemas que fueron diseñados para las policías locales o para que la gente adinerada se sintiera más segura (como los lectores de placas de vehículos) y los transformaron en herramientas policiales para el ICE. Tomaron tecnologías de vigilancia que ya eran preocupantes (herramientas para hackear teléfonos, software de monitoreo de redes sociales, algoritmos de reconocimiento facial y lentes con IA) y las volvieron en contra de algunos de los grupos más vulnerables de la sociedad. Quedan pocas razones para ser optimistas, pero ante la amenaza de la tiranía, la gente se resiste. Por eso, nos enorgullece poder darles un espacio a estas personas en nuestra revista.

DATOS PELIGROSOS

El software ImmigrationOS de Palantir demuestra por qué es importante resistirse a la recolección masiva de datos.

POR JASON KOEBLER

Los defensores de la privacidad declaran que uno de sus principios fundamentales es garantizar que la información que se recolecta para un fin no se use para otro distinto. La fuerza política del país se ha pasado las últimas décadas animando a los inmigrantes indocumentados a que paguen impuestos, envíen a sus hijos a la escuela e interactúen con partes del gobierno distintas a los organismos de seguridad, todo con una sencilla promesa: sus interacciones permanecerían aisladas e inaccesibles al aparato de seguridad del ICE. Pero llegó el gobierno de Trump y todos estos límites y mecanismos de seguridad que separaban los datos fueron derribados. Todo comenzó con una herramienta llamada "Investigative Case Management" ("Gestor de casos e investigación"), una base de datos de la empresa Palantir creada por encargo de la Administración Obama, la cual conectaba distintas bases de datos gubernamentales y permitía filtrar la información por cientos de categorías distintas. Sobre esta, los mismos estudios de riesgos y privacidad del gobierno de Obama declararon que existía la posibilidad de que la herramienta fuera abusada por administraciones futuras si las prioridades políticas cambiaban.

Y ese momento, inevitablemente, llegó. La Administración Trump le pidió a Palantir que diseñara una herramienta más poderosa, "ImmigrationOS": un sistema de vigilancia que pudiera rastrear los movimientos de la gente, incluidas sus "autodeportaciones". Para esto, la herramienta obtiene información de una abrumadora variedad de bases de datos gubernamentales, incluidas aquellas que jamás fueron pensadas para servir a los organismos de seguridad: registros de pasaportes, archivos de Seguro Social e información impositiva del IRS. Este es un ejemplo claro de por qué deben existir movimientos que se resistan a los programas invasivos de vigilancia y recolección de datos y por qué es importante que los mecanismos de derecho a la privacidad tengan garantías legalmente vinculantes: los hechos recientes demuestran que las promesas de privacidad y las prioridades políticas pueden ser efímeras. Y en el contexto de las tecnologías de vigilancia, los "mecanismos de seguridad" y los "límites de contención" significan poco cuando la Administración a cargo puede anularlos según sus ideologías.

CHRIS YANG/UNSPLASH

¿BAJO QUÉ CATEGORIAS PUEDE BUSCAR PALANTIR?

- Estado de residencia
- "Características físicas particulares"
- Cicatrices
- Tatuajes
- "Afiliación con grupos criminales"
- Ubicación
- Información de lectores de placas
- Lugar de nacimiento
- Color de cabello y ojos
- Etnia
- Número de Seguridad Social
- Lugar de trabajo
- Estado de la licencia de conducir

NO TE METAS

Should it be legal for ICE agents to wear smart glasses during raids?

BY JASON KOEBLER

Las redes sociales del gobierno se han visto inundadas de extraños y desquiciados videos que parecen propaganda: agentes del ICE persiguen a personas a través de estacionamientos de tiendas Home Depot, calles céntricas abarrotadas y barrios residenciales, todo al ritmo de la música. En algunos de los videos, a los agentes se les ve portando cámaras réflex digitales con estabilizador, cámaras corporales e incluso lentes con IA de Meta (como evidenciamos en agosto).

404 Media consiguió material audiovisual que muestra a un agente de la CBP (Oficina de Aduanas y Protección Fronteriza de Estados Unidos) equipado con lentes con IA de Meta en una redada en una tienda Home Depot en Cypress Park, Los Ángeles. Una semana más tarde, se vio a dos agentes llevando el mismo tipo de lentes en el MacArthur Park. Los lentes IA de Meta están equipadas con una cámara que puede transmitir videos en vivo, el asistente IA de Meta, tres micrófonos y características de reconocimiento de entornos. Aún no está claro por qué los agentes portaban estos lentes o si eran de su propiedad. La CBP respondió a nuestras consultas y declaró que eran dispositivos de uso personal de los agentes y que no eran reglamentarias del departamento; sin embargo, eso da paso a la pregunta: si los agentes de la CBP no están autorizados para llevar cámaras personales en sus operaciones policiales, ¿es legal que usen estos lentes?

En sus carteleras, Meta promociona sus lentes como accesorios elegantes para influencers; sin embargo, la CBP ha demostrado que el estado les ve un buen potencial como dispositivos de vigilancia y herramientas para grabar videos de propaganda. Meta sostiene que su tecnología es similar a la de un iPhone o cualquier otro tipo de cámara, y que es poco honesto destacar que está siendo usada por agentes de la CBP; sin embargo, una cámara que se lleva sobre la cara goza de un formato completamente distinto al de un iPhone o una cámara réflex digital, y el público las considera invasivas. En tiempos recientes, Meta se ha acercado más al ámbito militar: Mark Zuckerberg anunció una nueva alianza de realidad aumentada e inteligencia artificial con la contratista de defensa Anduril. Su fundador, Palmer Luckey, declaró que espera que esta colaboración "convierta a los combatientes en 'tecnomagos'".

"Creo que esto debe evaluarse en el contexto de una agencia que anima a sus agentes a intimidar a las personas y causarles terror", nos comenta Jay Stanley de la Unión Estadounidense por las Libertades Civiles. "El hecho es que cuando aparecen nuevas tecnologías de vigilancia en el mercado, siempre existe la posibilidad de que se usen para propósitos que incluyen prácticas abusivas", agrega.

Es evidente que una cámara que se lleva sobre la cara goza de un formato completamente distinto al de un iPhone o una cámara réflex digital, y el público las considera invasivas.

POR JASON KOEBLER

En 2018, una nueva empresa emergente de vigilancia comenzó a promocionar sus cámaras lectoras de placas que funcionan con energía solar a asociaciones de propietarios de todo el país. La empresa en cuestión, Flock Safety, les prometía a los propietarios que podrían ver con facilidad quién entraba y salía de sus vecindarios y que, incluso, recibirían alertas cuando el vehículo de una persona "no residente" pasara por el lugar. La compañía llamó a su sistema una "portería de barrio virtual para mantener a las comunidades a salvo", y su kit de prensa destacaba cómo se usó la tecnología para atrapar a un ladrón de bicicletas: "el sistema de cámaras Flock instalado en mi calle logró captar la cara del ladrón y el número de placa de su vehículo, y las fotografías que tomó de mi bicicleta en la cajuela tenían tanto detalle como para que las autoridades las consideraran evidencia suficiente para arrestarlo", declaraba la víctima en un caso práctico que la empresa ha publicitado en reiteradas ocasiones.

La propagación de Flock a través de los Estados Unidos y la expansión desmedida de sus fines operativos demuestran el peligro de las tecnologías de vigilancia.

En aquel entonces, el segmento de mercado al que apuntaba Flock eran los barrios acaudalados, y la idea inicial era que las asociaciones de propietarios pudieran reportar delitos contra la propiedad a las autoridades. Hoy en día, las cámaras autónomas de lectura de placas (ALPR, por sus siglas en inglés) se han convertido en uno de los métodos de vigilancia más extendidos de la nación: han pasado de ser un elemento aislado de tecnología pensado para vigilar una calle o un barrio a ser una red de más de 80 000 cámaras que conectan unas 6000 ciudades, departamentos de policía y otros organismos de todo el país. El sistema de Flock también se vende a centros comerciales, ferreterías como Home Depot y Lowes, hospitales, escuelas e iglesias. Además, ofrecen controvertidos e impugnados "micrófonos detectores de disparos" y drones que vuelan de forma autónoma para asistir a llamados de emergencia.

Cada vez que un vehículo pasa frente a una cámara Flock, el sistema le toma fotografías y registra información que incluye hora y ubicación actuales en la base de datos de la empresa. Así, las autoridades pueden establecer líneas de tiempo detalladas de los movimientos de una persona.

El año pasado, mediante solicitudes de transparencia de la información, conseguimos acceso a numerosas "auditorías de red" de Flock, las cuales son colosales hojas de cálculo con información sobre el uso que le da la policía a la red Flock. Estas hojas incluyen una pestaña etiquetada "Razón", que los agentes deben rellenar cuando hacen búsquedas, y se evidencia que la policía usa el sistema prácticamente para todo: en dos semanas, se registraron más de 160 000 búsquedas a nivel nacional, con razones que iban desde "robo" y "atropello con fuga" hasta números de caso específicos y términos tan genéricos como "investigación", "delito" o "buscado". Muchas de las búsquedas ni siquiera incluían una razón.

Pero descubrimos algo incluso más llamativo: las policías locales estaban realizando miles de búsquedas relacionadas con "inmigración", "ICE+ERO" (ERO es la "Oficina de Detención y Deportación" del ICE), "inmigración ilegal" y "HSI" ("Oficina de Investigaciones de Seguridad Nacional"). La HSI es una división del ICE que, entre otras cosas, se encarga de realizar redadas en lugares de trabajo. Esto es importante porque demuestra que el sistema Flock se está usando para tareas de control de inmigración, pero más importante aún es el hecho de que ni el ICE ni el DHS ("Departamento de Seguridad Nacional") tenían un contrato activo con el Flock en ese momento. Dicho de otro modo, la policía local estaba usando el sistema para rastrear inmigrantes indocumentados en nombre de la Administración Trump, todo de manera furtiva. En algunos casos, las policías locales se valían del programa 287(g) del ICE, que les permite realizar algunas tareas de control migratorio. Durante nuestras investigaciones, también descubrimos que las policías locales estaban extrayendo datos de cámaras Flock ubicadas en estados donde es ilegal usarlas para estos fines. Por ejemplo, la policía de Texas buscaba no solo en sus propias cámaras estatales, sino también en cámaras de California e Illinois, donde la ley prohíbe que las policías realicen tareas de control migratorio.

Nuestros reportajes han demostrado que el DHS y el ICE no solo demuestran interés por recopilar datos de placas, sino que activamente buscan nuevas formas de recolectar estos datos con fines migratorios. Por ejemplo, el ICE se vale de sus contratos con Motorola (una empresa que también fabrica cámaras de lectura de placas) y de la aplicación Mobile Companion para buscar números placas, y luego los relaciona con información de Thomson Reuters, una empresa de recolección de datos. Por su parte, Motorola vende tecnologías de reconocimiento facial e incluso un sistema que puede "predecir la ubicación futura" de un vehículo, todo para el beneficio del ICE. Dicho de otro modo, las ALPR se han convertido en uno de los tipos de tecnología de vigilancia más usados del mercado, y hoy en día es casi imposible conducir a través del país sin que se vigilen los movimientos de un vehículo, y esta tecnología ahora está siendo usada activamente en contra de inmigrantes indocumentados.

Al poco tiempo de nuestra investigación, Illinois tomó medidas contra las actividades ilícitas facilitadas por el sistema Flock, y la empresa implementó mecanismos de seguridad supuestamente diseñados para prevenir estos abusos, pero al poco tiempo implementó algo que llamó un "programa piloto" directamente con el Departamento de Seguridad Nacional. La propagación de Flock a través de los Estados Unidos y la expansión desmedida de sus fines operativos demuestran el peligro de las tecnologías de vigilancia conectadas en red, y también demuestra lo fácil que es para las empresas de vigilancia aprovecharse de sus promesas de "prevención de delitos" para firmar miles de contratos con pueblos y ciudades de todo el país, un ayuntamiento a la vez. Esto es una prueba clara de cómo herramientas de vigilancia pensadas para barrios adinerados pueden terminar siendo usadas contra los grupos más vulnerables de la sociedad. Si es que hay algo positivo que recalcar de todo esto, es que algunas ciudades ya han cancelado sus contratos con Flock debido a nuestros reportajes sobre el uso del sistema con fines de control migratorio y a un caso separado en el que se usó en contra de una mujer que se hizo un aborto autoinducido en Texas.

EN CIFRAS

6,000
las ciudades estadounidenses conectadas al sistema Flock

>80K
cámaras de Flock en toda la nación

>160K
consultas semanales a la red de Flock hechas por la policía

FOTO DE PRENSA/FLOCK

LA SOMBRA QUE TE SIGUE EN LÍNEA

POR JOSEPH COX

ShadowDragon es una empresa de vigilancia de redes sociales que le vende tecnología al ICE. La compañía puede monitorear la actividad pública de un usuario en toda clase de redes sociales, aplicaciones y sitios web. Hemos recopilado una lista de más de 200 sitios que ShadowDragon monitorea, incluidos Bluesky, OnlyFans, CashApp y las plataformas de Meta.

ILUSTRACIÓN DE FONT AWESOME/ERNIE SMITH

LA VULNERABILIDAD OCULTA QUE USA EL ICE

El ICE compró una de las herramientas de hackeo de celulares más poderosas de las que nunca has oído hablar. Los demandamos para descubrir por qué.

POR JOSEPH COX

Paragon es una empresa israelí que les vende herramientas de hackeo a los gobiernos para que sus agencias puedan vulnerar la seguridad de teléfonos móviles de forma remota y sin necesidad de que la persona siquiera tenga que hacer clic en un enlace. El ICE ya ha pagado 2 millones de dólares para acceder a esta tecnología.

Cómo funciona: Paragon usa un software llamado Graphite, el cual utiliza una variedad de vulnerabilidades para infiltrar un teléfono objetivo. Una de estas vulnerabilidades consiste en enviar un archivo PDF mediante WhatsApp: el celular del usuario carga el PDF automáticamente, la vulnerabilidad se activa y el teléfono queda expuesto a los hackers de forma silenciosa.

Qué datos puede obtener: Paragon se especializa en extraer el contenido de mensajes cifrados de aplicaciones de chat como WhatsApp y Signal y de plataformas de comunicación como Facebook Messenger y Gmail.

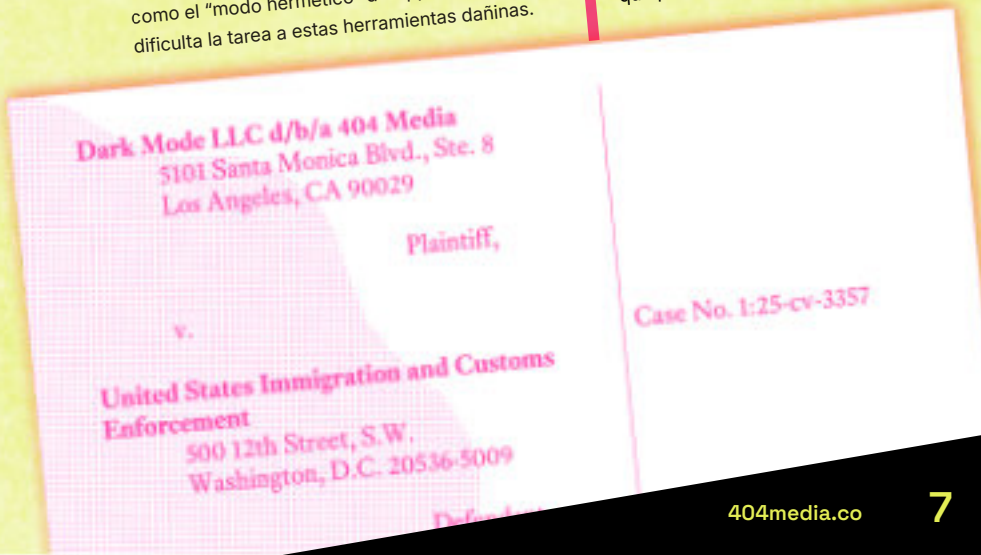
Cómo puedes protegerte: Mantén tu teléfono actualizado y, de ser posible, usa funciones como el "modo hermético" de Apple, el cual les dificulta la tarea a estas herramientas dañinas.

POR QUÉ VAMOS A DEMANDARLOS

El ICE se ha negado a entregar incluso documentos básicos sobre el contrato, a pesar de nuestra solicitud amparada bajo la Ley por la Libertad de la Información (FOIA). Por eso, en septiembre presentamos una demanda en contra del ICE en la cual exigimos que se liberen esos registros. En nuestra demanda señalamos que:

"404 Media ha solicitado al ICE la divulgación de documentos oficiales relacionados con su contrato con una empresa conocida por su poderosa herramienta de spyware, cuyo posible uso en la campaña de deportación masiva que impulsa la agencia ha llevado a legisladores, organizaciones de libertades civiles y grupos de defensa de migrantes a expresar profundas preocupaciones por potenciales abusos a los derechos civiles".

Queremos acceder a esos documentos porque pueden revelar con claridad por qué el ICE compró esta tecnología y para qué piensa usarla.


Dark Mode LLC d/b/a 404 Media
5101 Santa Monica Blvd., Ste. 8
Los Angeles, CA 90029

Plaintiff,

v.

United States Immigration and Customs Enforcement
500 12th Street, S.W.
Washington, D.C. 20536-5009

Case No. 1:25-cv-3357

FREEPIK

SU CARA, POR FAVOR

Alguna vez se pensó que el reconocimiento facial era un exceso inaceptable. Pero Mobile Fortify llegó para cambiar las reglas.

POR JOSEPH COX

"Se rehúsa a identificarse", le dice un oficial de la división de Detención y Deportación del ICE a su colega. La escena es la de un grupo de agentes federales rodeando a un auto estacionado en una calle residencial, hablándole al conductor a través de la ventana entreabierta.

"Soy ciudadano estadounidense", dice el conductor.

"Escuche. Estoy siendo muy amable con usted, ¿no?", responde el agente de ICE. "Tengo que ir a trabajar", insiste el conductor. "¿Dónde trabaja?", pregunta uno de los oficiales. "Eso no es relevante ahora", contesta el hombre.

"Soy ciudadano estadounidense, así que déjenme en paz", remata.

"Está bien. Solo tenemos que verificar esa información", dice uno de los funcionarios. La discusión aún no termina. Uno de los agentes le dice: "mire para acá un momento", y apunta la cámara de su teléfono directamente a la cara del conductor.

"Oiga, escuche", continúa el oficial, "si se quita la gorra, esto va a ser mucho más rápido". "Voy a consultar su información".

Con eso, el agente quiere decir que va a usar reconocimiento facial para verificar la identidad y el estatus migratorio del conductor.

Esta es la nueva realidad en Estados Unidos: grupos de agentes del ICE y de otras agencias interrogan a las personas por el color de su piel, su acento o simplemente por cómo se ven.

Y si alguien se niega a mostrar identificación, la policía le escanea la cara. La app de reconocimiento facial de ICE, llamada Mobile Fortify, consulta una cantidad sin precedentes de bases de datos gubernamentales y le entrega al agente el nombre, la fecha de nacimiento, el "número de extranjero" y cualquier orden de deportación vigente de la persona. El ICE sostiene que las personas no pueden negarse a que se les escanee el rostro con esta tecnología y considera que los resultados de la app son una confirmación "vinculante" de su estatus, incluso por encima de un acta de nacimiento.

El desarrollo de productos de reconocimiento facial diseñados para identificar desconocidos se consideró una empresa tan peligrosa que, durante años, empresas como Meta y Google han preferido no lanzar herramientas de ese tipo. Amazon intentó venderle su sistema Rekognition al ICE, pero quien popularizó el acceso masivo a esta tecnología fue una compañía llamada Clearview AI, que se dedicó a recolectar miles de millones de fotos de internet y luego vendió su sistema de comparación facial a autoridades locales, estatales y federales. Clearview, en teoría, fue diseñada para investigaciones criminales. Que el ICE comenzara a usar una herramienta de reconocimiento facial para desenmascarar gente y detenerla por supuestas violaciones migratorias era, tristemente, el siguiente paso lógico.

Correos internos filtrados del ICE nos revelaron la existencia de Mobile Fortify. Después tuvimos acceso a los manuales de usuario de la herramienta. Ahí se detalla que la app compara el rostro de una persona con un banco de 200 millones de imágenes.

El usuario también puede iniciar una "Super Query" (superbúsqueda), la cual consulta información de la base de datos del Centro de Registro Nacional de Información de Crímenes (NCIC) del FBI, un sistema de registro de órdenes de arresto estatales pendientes y varios otros sistemas internos de la CBP.

El desarrollo de productos de reconocimiento facial diseñados para identificar desconocidos se consideró una empresa tan peligrosa que, durante años, empresas como Meta y Google han preferido no lanzar herramientas de ese tipo.

"La fotografía que se muestra (...) de la persona es la que se haya tomado durante su encuentro más reciente con la CBP; sin embargo, su rostro se analizará contra todas las imágenes que la CBP haya recolectado de esa persona", dice uno de los documentos a los que tuvimos acceso.

Más tarde, la CBP lanzó lo que parece ser una versión reducida de Mobile Fortify para policías locales, bajo el nombre de Mobile Identify. Con esta app, un agente puede escanear la cara de una persona y el sistema le indica si debe llamar o no al ICE y le entrega un número de referencia.

Durante años, activistas y expertos advirtieron que la tecnología de reconocimiento facial nos iba a llevar exactamente a este escenario: agentes capaces de identificar prácticamente a cualquier persona en la calle. En el último año, esa advertencia ha resultado ser, lamentablemente, acertada.

FOTOS DE PRENSA

SILBA EN RESPUESTA

Conoce los silbatos que imprimen en 3D las comunidades para defenderse del ICE

POR JOSEPH COX

Bajo el alero de la reciente Operación Midway Blitz, personas en Chicago han comenzado a imprimir silbatos en 3D para alertar a su comunidad cuando agentes del ICE entran al vecindario. El código es sencillo: tres pitidos cortos significan "el ICE está cerca" y tres pitidos largos significan "Código Rojo".

Habitantes de Chicago crearon sus propios modelos de silbatos y los subieron a internet para que cualquiera pueda imprimirlos. Puedes ver un ejemplo aquí: **https://bit.ly/3MHoLlq**

Las impresoras 3D toman un diseño digital y lo usan como base para construir un objeto capa por capa. Estos silbatos impresos en 3D salen más baratos que comprarlos en Amazon y, además, rompen con la cadena de suministro tradicional que alimenta a las grandes empresas tecnológicas: ponen los medios de producción directamente en manos de la comunidad afectada.

Algunos modelos incluyen información importante o mensajes de solidaridad grabados en el propio silbato, y los silbatazos permiten comunicarse de forma rápida, incluso entre personas que no hablan el mismo idioma.

"El objetivo es evitar que secuestren a la mayor cantidad de personas posible", nos comentó Aaron Tsui, una de las personas que ha estado imprimiendo estos silbatos.

POR JASON KOEBLER

De alguna manera, la crueldad de la Administración Trump ha sido tal que incluso los hackers han decidido contraatacar. El caso más llamativo ocurrió en octubre, cuando un grupo que se hace llamar "Scattered LAPSUS$ Hunters" filtró hojas de cálculo con las supuestas identidades de 680 funcionarios del Departamento de Seguridad Nacional (incluidos agentes del ICE) y 190 funcionarios del Departamento de Justicia, y 170 correos electrónicos del FBI y sus dueños. "I want my MONEY MEXICO" ("¿DÓNDE está mi DINERO, MÉXICO?"), escribió alguien vinculado al grupo, una referencia a una acusación no comprobada de la Administración Trump de que los carteles mexicanos estaban ofreciendo recompensas por los datos personales de agentes del ICE. La filtración provino de un gigantesco hackeo a clientes de Salesforce, y 404 Media confirmó que al menos parte de la información era auténtica, incluidos nombres, domicilios, teléfonos y correos electrónicos de distintos funcionarios del gobierno.

Este fue el segundo gran hackeo reciente relacionado con inmigración. En mayo, GlobalX, una aerolínea privada que ha operado vuelos de deportación para la Administración, fue víctima de otro ataque informático. Cientos de listas en las que se detallaban los nombres de personas asignadas a vuelos específicos y tripulaciones fueron filtradas a 404 Media por alguien que decía estar vinculado a Anonymous.

Entre esos documentos obtuvimos las listas de tres vuelos de deportación que viajaron de Texas a El Salvador el 15 de marzo. Esos vuelos se convirtieron en un controvertido caso ante la Corte Suprema y recibieron un intenso escrutinio público después de que un juez intentara bloquearlos. En uno de estos vuelos fue deportado ilegalmente Kilmar Abrego García, un hombre de Maryland que fue enviado al infame CECOT de El Salvador.

Las listas hackeadas revelaron que un hombre al que el ICE había "desaparecido" había sido en realidad subido a uno de esos vuelos y dejaron al descubierto las identidades de decenas de otros pasajeros que no figuraban en ningún registro público del gobierno estadounidense: personas cuyo paradero era totalmente desconocido para sus familias hasta que los vieron en videos de propaganda gubernamental o en imágenes difundidas desde el CECOT. Entre ellos estaba Keider Alexander Flores Navas, un venezolano cuya familia reconoció en una foto del CECOT. Su nombre jamás fue incluido por el gobierno de Estados Unidos en la lista de personas deportadas.

"Estamos hablando de una lista de personas que el gobierno estadounidense jamás ha reconocido de manera formal, y no tenemos idea si están en el CECOT o en otro lugar", comentó Michelle Brané, directora ejecutiva del grupo de defensa de inmigrantes Together and Free, en relación con los manifiestos de vuelo hackeados.

Los hackers tienen la mira sobre los agentes federales... y las aerolíneas que los ayudan con las deportaciones.

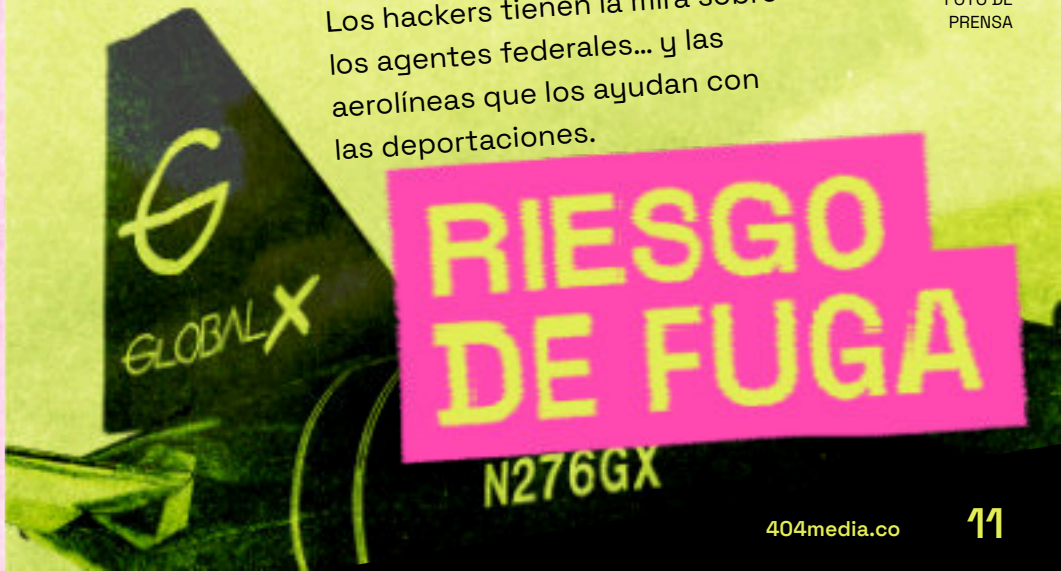


FOTO DE PRENSA

Las Grandes Tecnológicas Ya Eligieron Su Bando

En un precedente escalofriante, Apple y Google borraron aplicaciones para rastrear al ICE como ICEblock y Red Dot de sus tiendas de aplicaciones.

POR JOSEPH COX

Algunas grandes tecnológicas, y en especial Apple y Google, ya indicaron su postura en cuanto a la campaña de deportación masiva de la Administración Trump. Las dos empresas mencionadas han bloqueado aplicaciones para detectar a operativos del ICE, las cuales eran herramientas que permitían alertar a las comunidades locales sobre la presencia de agentes migratorios. Por otra parte, Google aloja en su infraestructura la aplicación de reconocimiento facial de la CBP, la misma que ayuda a las policías locales a cazar inmigrantes.

La eliminación de apps como ICEBlock y Red Dot ocurrió después de que, en septiembre, un hombre armado asesinara a dos personas detenidas e hiriera a otra en un centro del ICE. Según las autoridades, el hombre buscó en su teléfono aplicaciones para rastrear operativos del ICE, incluida ICEBlock, antes del ataque. A raíz de esto, el Departamento de Justicia le exigió a Apple que retirara ICEBlock de la App Store, y la empresa accedió. Pero no solo eso: también eliminó Eyes Up, una app que ni siquiera mostraba ubicaciones en tiempo real, sino que funcionaba como un mapa para archivar videos de abusos cometidos por el ICE.

Después vino el turno de Google, que decidió por cuenta propia eliminar aplicaciones. La empresa nos declaró que no recibió ninguna instrucción del gobierno, sino que decidió simplemente eliminarlas.

Como parte del bloqueo de Red Dot, Google describió a los funcionarios del ICE como un "grupo vulnerable", un término que usualmente se reserva para comunidades minoritarias que enfrentan violencia o persecución.

"Proveer servicios tecnológicos para potenciar las operaciones del ICE, a la vez que se bloquean herramientas para cerciorarse de que los agentes actúan responsablemente, es justamente lo contrario a lo que debería estar pasando", nos comenta Kate Ruane, directora del Proyecto Libre Expresión del Centro para la Democracia y la Tecnología. "Los agentes de ICE no quieren enfrentar consecuencias por sus actos, pero documentar las actividades del ICE y de otras fuerzas policiales es esencial para frenar abusos de poder y conductas indebidas. Desde hace décadas, los tribunales han reconocido que monitorear y reportar el actuar de las fuerzas del orden es un mecanismo de control público importante y con larga tradición", añadió.

Por su parte, Joshua Aaron, creador de ICEBlock, nos dijo: "Las grandes tecnológicas siguen poniendo las ganancias y el poder por sobre la gente, todo con la excusa de que nos están protegiendo. En este momento estamos en un punto de quiebre en la historia del país. Es hora de tomar partido: ¿fascismo o moralidad? Las grandes tecnológicas ya tomaron bando".

JAN ANTONIN KOLAR/UNSPLASH

¿Y Por Qué Ranas?

Sí, parece un sinsentido, pero la elección de esta indumentaria de protesta tiene su lógica.

POR MATTHEW GAULT

En medio de una Administración cruel en la que mucha gente se aferra como puede a cualquier chispa de esperanza, una rana inflable llegó a llenar los vacíos. La Rana de Portland se ha convertido en un símbolo sorprendentemente útil de protesta contra el ICE y la campaña de deportación masiva de Trump. El contraste es absurdo, pero poderoso: un anfibio inflable plantándole cara a agentes del ICE fuertemente armados y blindados. Pero la rana no es solo un chiste visual: también es una herramienta práctica de resistencia pasiva en una época marcada por la vigilancia masiva, la brutalidad policial y la existencia de agentes federales enmascarados que desaparecen a personas en las calles.

La noche del 2 de octubre, poco antes de las 11 p. m. en Portland, Oregón, un agente federal roció gas pimienta a través del orificio de ventilación del disfraz de rana inflable de Seth Todd. Todd estaba protestando contra el ICE frente a sus oficinas en Portland cuando vio que un agente federal empujó a otro manifestante al suelo. Él se acercó para ayudar y el agente le roció el gas pimienta directo al orificio de ventilación del traje.

Todd ni se inmutó. "He comido tamales más picantes", dijo al Oregonian.

El momento se hizo viral y se compartió una y otra vez en redes. La figura de Todd, enfundado en su traje de rana, dejó de ser solo la de "un manifestante más": se transformó en un símbolo.

> Los símbolos son importantes para cualquier movimiento, pero los mejores símbolos de protesta tienen, además, un lado práctico.

Los símbolos son importantes para cualquier movimiento, pero los mejores símbolos de protesta tienen, además, un lado práctico. Durante las protestas antiautoritarias en Hong Kong entre 2014 y 2019, la gente en las calles usó paraguas amarillos como señal de solidaridad, pero también servían para bloquear el gas pimienta y protegerse de objetos que les lanzaban. Aquí es necesario hacer una pausa y recordar que dentro de la rana inflable y debajo del paraguas amarillo hay una persona de carne y hueso. Detrás de estos símbolos hay gente valiente que se enfrenta a agentes del ICE que aterrorizan ciudades de Estados Unidos.

Al lado de una rana antropomórfica, la solemnidad fingida de los agentes del ICE y de fuerzas armadas que actúan como un ejército de ocupación contra su propia población queda al desnudo: se ve ridícula. Para quienes llevan años advirtiendo que Trump es tan aterrador como absurdo, hay algo en esa imagen de una rana rodeada de policías que hace que, por fin, más gente lo entienda. Es un meme convertido en objeto, una imagen que condensa todo el escenario político en una sola escena: una especie de jeroglífico que explica el primer año del segundo mandato de Trump.

FOTO DE JASON KOEBLER

Combatir La Vigilancia Puede Ser Un Tema De Estiloe

El atuendo indicado podría ser útil contra las innumerables cámaras presentes.

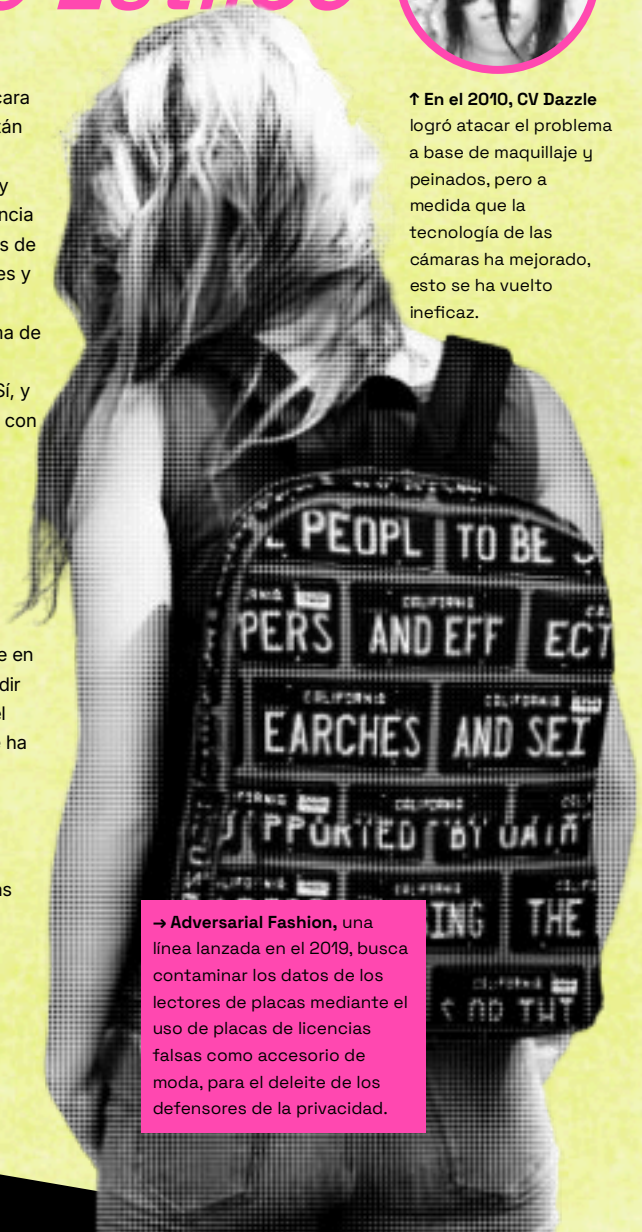
↑ En el 2010, CV Dazzle logró atacar el problema a base de maquillaje y peinados, pero a medida que la tecnología de las cámaras ha mejorado, esto se ha vuelto ineficaz.

POR SAMANTHA COLE

Los mismos algoritmos que usan tu cara para desbloquear el teléfono hoy están en manos de la policía, que los usa para reconocerte en detenciones de tránsito y redadas migratorias. Empresas de vigilancia cubren el país de cámaras, realizan miles de millones de escaneos de vehículos al mes y venden esos datos a departamentos de policía de todo el país. ¿Hay alguna forma de camuflarse frente a los sistemas de reconocimiento facial en la vida diaria? Sí, y ni siquiera es necesario comprarse ropa con diseños especiales ni gadgets futuristas antivigilancia.

Uno de los primeros experimentos del tecnólogo Adam Harvey en este campo fue CV Dazzle, el cual usaba maquillaje y peinados estratégicamente diseñados para confundir a un algoritmo específico de reconocimiento facial. Eso fue en 2010, y el maquillaje ya no sirve para evadir los sistemas actuales. Desde entonces, el género de diseño de la "antivigilancia" se ha expandido a ropa urbana y dispositivos ponibles de lujo. El problema es que la mayoría de esos productos son poco fiables: los algoritmos mejoran todo el tiempo y las cámaras tienen cada vez más resolución. En muchos casos, la "moda antivigilancia" es algo que solo se ve estiloso..., pero no funciona.

La mayoría de los sistemas de reconocimiento facial dividen tu rostro en partes: la forma de tus ojos, tus labios, tu nariz e incluso tus orejas; las distancias entre cada uno de esos puntos, y la combinación de estos elementos con tu tono de piel y otros factores.



→ Adversarial Fashion, una línea lanzada en el 2019, busca contaminar los datos de los lectores de placas mediante el uso de placas de licencias falsas como accesorio de moda, para el deleite de los defensores de la privacidad.

Incluso si no funciona a la perfección, la moda antivigilancia puede dejar el mensaje claro.

ACCESORIOS PARA ESCONDER LA CARA

Gorras: Una gorra o un sombrero con visera pueden ser una forma eficaz de hacer más difícil la detección de tus rasgos faciales, en especial de tus ojos.

Máscaras: Este accesorio te puede poner en la mira durante una protesta, pero son una forma muy eficaz de cubrir la cara de la detección de las cámaras.

Anteojos grandes: Mientras más grandes sean, mejor cubren tus rasgos faciales.

Tras ser procesada, la información biométrica de tu rostro se convierte en un código numérico. Si ese número se parece lo suficiente al de otras imágenes tuyas en sus bases de datos, el sistema concluye que eres tú.

Sabiendo esto, lo más probable es que ya tengas en tu casa el artículo de moda más efectivo contra la vigilancia: un cubrebocas de tela.

"Aunque mucha gente trate de desanimarte, cubrirte el rostro con una mascarilla sigue siendo muy efectivo", me comenta la tecnóloga y diseñadora de moda Kate Rose. En 2019, Rose creó Adversarial Fashion, una línea de ropa cubierta de placas falsas de automóvil, pensada para contaminar los datos que recolectan los lectores automáticos de matrículas.

Sumar algunas prendas comunes a tu atuendo puede reducir la probabilidad de que los sistemas biométricos te identifiquen con precisión. Puedes bajar mucho tu "puntaje de reconocimiento" si usas lentes de sol grandes, cubres tu barbilla y boca y usas una gorra o sombrero con visera que oculte parte de tu rostro de las cámaras elevadas. Y si quieres llevar tu estilo visual al siguiente nivel, existen lentes que bloquean las longitudes de onda infrarrojas que usan algunas cámaras.

El creador de la línea de lentes de bloqueo infrarrojo Reflectables (quien prefiere identificarse como Skitch) mencionó que ha visto cómo el mercado de la "moda antivigilancia" ha comenzado a volverse más mainstream con la aparición de empresas como Zenni, que vende lentes capaces de bloquear ciertos tipos de reconocimiento facial. "Veo que el mundo de los ponibles antivigilancia se está popularizando y monetizando", comentó Skitch. "Si la gente con dinero se entera de que hay un segmento de mercado no explorado en el que existe la posibilidad de llenarse los bolsillos, tarde o temprano van a encontrar la forma de entrar y quedarse con ese dinero".

Aunque no funcione a la perfección, la moda antivigilancia puede seguir siendo una declaración política. "Le da a la gente una excusa para hablar entre sí sobre lo que les importa, y ayuda al público a entender algo que suele ser muy técnico y abstracto: cómo funciona una tecnología de vigilancia que hoy en día es omnipresente", explicó Rose. Si una simple camiseta puede sabotear la base de datos de cámaras lectoras de placas, tal vez deberíamos pensar dos veces antes de poner una cámara en cada esquina.

"A mí me gusta la definición de privacidad del Manifiesto Cypherpunk: 'La privacidad es el poder de revelarte selectivamente'", dijo Harvey, en referencia al texto de 1993 del tecnólogo y criptógrafo Eric Hughes que llamaba a crear sistemas de información cifrados. "Cuando permites que otras personas recolecten, vean o monitoreen todo lo que haces... ahí hay una relación de poder en la que tú siempre llevas las de perder. En el fondo se trata de poder y de la libertad de acción de cada persona, pero también hay un componente político y democrático muy destructivo en permitir que estos sistemas de vigilancia masiva sigan creciendo".

← Reflectacles es una línea de anteojos para quienes se preocupan por la privacidad y usan materiales de bloqueo infrarrojo para que las cámaras no vean tus ojos.

FOTOS DE PRENSA

404 MEDIA

404 Media fue fundado por:
Jason Koebler
Samantha Cole
Emanuel Maiberg
Joseph Cox

Con aportes de:
Becky Ferreira
Matthew Gault
Evy Kwong

Diseño editorial:
Ernie Smith
Ilustración de portada:
Veri Alvarez

Impresión risográfica por Punch Kiss Press, Los Angeles

Agradecimientos especiales a heaven2nite, LA Fights Back! & CHIRLA.

¿Quiénes Somos?

404 Media es un medio independiente, propiedad de periodistas y operado por periodistas, fundado en agosto de 2023. Antes trabajábamos en VICE Media, una empresa que nos dio una enorme libertad editorial, mucha experiencia... y una vista privilegiada de cómo NO manejar una compañía. Los últimos dos años y medio los hemos dedicado a intentar construir algo más sostenible y más humano, en un mundo (y en una internet) que cada vez se siente más automatizado e imprudente. Creemos que un equipo pequeño, pero comprometido, sí puede hacer periodismo de investigación potente y transformador: uno que intenta que las empresas y centros de poder que nos empujan hacia un mundo más inhumano finalmente nos rindan cuentas, sin necesidad de vivir obsesionados con complacer algoritmos de redes sociales y buscadores. Y también creemos que es posible hacerlo de una forma financieramente sostenible.

Una de las maneras de depender menos de los modelos de distribución dominados por las grandes tecnológicas es poner nuestro trabajo en papel: algo que se pueda mandar por correo, vender en tiendas, repartir en conciertos. Algo que puedas leer y luego pasarle a una amiga, donar a una tienda de segunda mano para que alguien lo encuentre durante un fin de semana de ocio o incluso tirar al contenedor de reciclaje para que lo rescate cualquier persona que pase por ahí. Es un elemento físico que puede descubrirse de forma orgánica en el mundo real. Este zine es nuestro primer experimento en formato impreso y, como todo lo que hacemos, empezamos a baja escala con la esperanza de que a la gente le guste y lo apoye, y ojalá podemos seguir lanzando nuevas ediciones.

404 Media necesita el apoyo de suscripciones pagadas. Puedes suscribirte en 404media.co.

Si quieres hacer una donación deducible de impuestos para apoyar nuestro trabajo, escríbenos a **donate@404media.co**. Para cualquier otra consulta, escríbenos a **jason@404media.co** o **support@404media.co**.

Como en otros proyectos, nos hemos apoyado tanto en nuestra comunidad virtual (amistades, fuentes y personas expertas) como en nuestra comunidad local para crear este zine.