Communication from Public

Name:	Casey Maddren/Citizens for a Better Los Angeles
Date Submitted:	11/01/2023 10:59 PM
Council File No:	22-0392
Comments for Public Posting:	Citizens for a Better Los Angeles opposes the Transportation Communication Network and the associated implementing ordinance. Our detailed comments are attached.

CBLA

Citizens for a Better Los Angeles

November 1, 2023

Planning & Land Use Management Committee
Los Angeles City Hall
200 N. Spring St.
Los Angeles, CA 90012

Re: Transportation Communication Network, TCN Ordinance, Digital Billboards, Environmental Impact Report, Amended Findings
Council File: 22-0392
CPC-2022-5401-CA; CPC-2023-3653-ZC
Strongly Opposed

Members of the Planning & Land Use Management Committee,

Citizens for a Better Los Angeles (CBLA) is a nonprofit public benefit corporation organized to protect the rights and promote the well-being of all people throughout Los Angeles County.

We're writing to state our strong opposition to the proposed ordinance intended to implement the Transportation Communication Network. While we have a number of objections to the TCN and the proposed ordinance, our overriding concern is that the program involves the collection of data from electronic devices belonging to individuals in public spaces. There is ample evidence to show that digital out-of-home advertising companies use wireless technology to collect data from passersby. This violates the right to privacy guaranteed by the first article of the California Constitution, and also opens the door to violations of the Fourth Amendment of the US Constitution.

There are numerous reasons to be concerned about the TCN. To list just a few:

> The digital billboard structures permitted by the Ordinance would collect data from private citizens, including minors, in violation of the California Constitution and could lead to violations of the US Constitution;

> Members of the US Congress have recognized that surveillance advertising represents a danger to the public, as evidenced by the proposed "Banning Surveillance Advertising Act", introduced in September 2023 by Representatives Jan Schakowsky and Anna G. Eshoo, and Senators Ron Wyden and Cory Booker;

> The EIR prepared by LA Metro is inadequate in many respects. A fundamental flaw is the difference between the name of the project and the project described. The project is called the "Transportation Communication Network", but the EIR does not provide any specific information about the communication network. It does not describe the types of communications hardware to be installed or the number of devices. It does not describe the network infrastructure or its lifespan or how the components will be disposed of at the end of their useful life.

> The EIR is does not assess cumulative impacts that will result from the addition of the TCN digital billboards to the numerous existing digital billboards in the City of LA and surrounding cities. It also fails to assess cumulative impacts from planned projects within the City of LA, including the Sidewalk & Transit Amenities Program;

> The amended findings are not supported by the evidence. They claim that the TCN will allow the collection and analysis of transportation data to improve regional transportation systems, but offer few details and no analysis. The existing Regional Integration of Intelligent Transportation Systems (RIITS) already performs many of the functions attributed to the TCN, and RIITS could easily be expanded without any digital billboards at all.

> Placing digital billboards alongside the City's roads and freeways will result in an increase in distracted driving, increasing traffic injuries and fatalities.

Violation of Privacy Rights

The City has ignored evidence that the collection of cell phone data is an integral part of digital out-of-home advertising. To support this statement, we offer the following articles where advertising executives explain clearly their intention to gather data from cell phones.

Billboards that follow you? It's not sci-fi. They're already here, from LA TImes, August 25, 2020 - Exhibit A
https://www.latimes.com/business/story/2020-08-25/column-clear-channel-billboards-privacy

Clear Channel Chief Executive William Eccleshare:
"We can follow your movement to a store," he said. "We can follow what you purchase. And yes, we can look at your viewing habits that evening if you pass an ad for a Netflix show." [Emphasis added.]

Digital Billboards Are Tracking You, from Consumer Reports, November 2019 - Exhibit B
https://www.consumerreports.org/privacy/digital-billboards-are-tracking-you-and-they-want-you-to-see-their-ads-a1117246807/

Consumer Reports quoting Five Tier CEO Frank O'Brien:
"As we stand here, there are devices behind that screen that are picking ID numbers from our cell phones," O'Brien tells me, gesturing toward a billboard at 42nd Street and 7th Avenue. Using those devices and other technology, he says, "We know who is in Times Square at a given moment." [Emphasis added.]

How Digital Billboards Target Passersby (Hint:It's Cellphone Data), from NPR, February 7, 2020 - Exhibit C
https://www.npr.org/2020/02/07/803907447/how-digital-billboards-target-passersby-hint-its-cellphone-data

NPR offers another quote from Five Tier CEO Frank O'Brien:
"The amount of data that can be pulled in is really infinite at this point. With mobile devices - latitude, longitude, altitude; if someone's in an elevator, changing an ad based on the floor that they're on in the elevator." [Emphasis added.]

While ad executives promise that no personally identifiable data is collected, their promises are empty. In reality, there's no way for governments or individuals to ascertain what data is being collected, and there's also no way to find out how the information is used once it flows into the vast, unregulated global data ecosystem.

It's especially important to highlight Clear Channel's statements on this issue, because the TCN is actually an extension of Metro's Billboard Program, which has been in existence for over a decade. The Billboard Program is managed by Allvision, and through the Program, at least two Clear Channel digital billboards have already been erected, one in Long Beach and one in Downey.

Some Clear Channel employees have downplayed their former CEO's comments about following consumers and tracking their habits, but let's take a look at information available on Clear Channel's website regarding its RADAR system.

Get More Results with Clear Channel Outdoor RADAR
https://clearchanneloutdoor.com/radar-data-solutions/

This web page includes a slideshow under the following heading:

"CCO RADAR delivers audiences exposed to OOH by using four criteria for accurate and verified exposure:"

The slideshow can be seen in Exhibits D 1 - 4.

It should be noted that each of the slides includes the following disclaimer at the bottom:

"CCO out-of-home media does not collect any personal information. CCO licenses data in aggregated and/or anonymous formats from business partners."

Similar disclaimers are commonplace throughout the digital out-of-home industry. However, the text that appears on the individual slides appears to call this claim into question. Also, please note that the disclaimer acknowledges that CCO does obtain "aggregated and/or anonymous" data from business partners.

For example, Slide 3, Exhibit D 3, includes the following text:

"Location signal strength: We want to see continuous device activity from when a mobile device approaches, passes, and drives away from the billboard advertisement."

Slide 4, Exhibit D 4, includes the following text:

"Digital exposure: When device IDs are observed and analyzed, we understand the specific time of day and duration of advertisements run on our digital billboards, in order to match them with users' location data."

The phrase "We want to see continuous device activity" in Slide 3 appears to indicate that Clear Channel is monitoring personal electronic devices. The phrase "When device IDs are observed and analyzed" in Slide 4 clearly indicates that Clear Channel has access to individual device IDs.

Device IDs are unique identifiers belonging to individual devices. They can easily be matched to a specific individual. This is obviously Clear Channel's intent, as shown by their desire to "match them with users' location data." It's hard to reconcile Clear Channel's claim that they don't collect "personal information" with the slideshow text that shows they do access device IDs.

Speaking before the US House of Representatives Energy & Commerce Committee, Justin Sherman, a Duke University Senior Fellow and Research Lead for the Data Brokerage Project, warned that the global data brokerage ecosystem is gathering massive amounts of data that is being used by private interests for their profit.

Expert Warns Data Brokers Profit from Unregulated Surveillance, House Energy & Commerce Committee, May 18, 2023 - Exhibit E
https://energycommerce.house.gov/posts/expert-warns-data-brokers-profit-from-unregulated-surveillance

"The entire data brokerage ecosystem—from companies whose entire business model is data brokerage, to the thousands of other apps, advertisers, tech giants, and companies that collect, buy, sell, and share Americans' personal data—profits from unregulated surveillance of every American, particularly the most vulnerable."

Advertisers' claims that they collect no personally identifiable information are meaningless, since they're well aware that "re-identification" of individuals is possible by combining data sets. Data brokers make vast data sets available to almost anyone who's willing to pay for it. With the computing power available to businesses today, it's an easy matter to "re-identify" individuals using even a small number of data points.

Re-Identification of "Anonymized Data", B. Lubarsky, Georgetown Law Technology Review, 2017 - Exhibit F

"The proliferation of publicly available information online, combined with increasingly powerful computer hardware, has made it possible to reidentify "anonymized" data. This means scrubbed data can now be traced back to the individual user to whom it relates. Scrubbed data is commonly reidentified by combining two or more sets of data to find the same user in both. This combined information often reveals directly identifying information about an individual."

Returning to Clear Channel, their Radar web page actually provides case studies showing their ability to target and observe individuals who have been exposed to their campaigns.

Clear Channel Radar Case Study: Digital billboards drive online engagement for Twitch - Exhibit G
https://clearchanneloutdoor.com/case-studies/dooh-drives-online-engagement-for-twitch/

"90% incremental lift in active users
Utilizing DOOH ads secured through a mix of programmatic and direct buying, and leveraging RADARSync to find the exact gamers they wanted to target, the brand experienced a 90% incremental lift in monthly active users on the platform among DOOH-exposed accounts" [Emphasis added.]

Clear Channel Radar Case Study: Driving innovation for Pharma - Exhibit H
https://clearchanneloutdoor.com/case-studies/driving-innovation-for-pharma/

"OOH drove 50% lift in consideration intent
CCO RADARProof is our campaign measurement and attribution solution that allows us to observe consumer devices exposed to an OOH campaign. In this pharma study, we learned that the campaign effectively reached the target audience and influenced their intention to consider the product. Among those exposed to the OOH campaign, consideration intent was lifted by 50%." [Emphasis added.]

CBLA is especially concerned about the fact that data brokers are already providing law enforcement agencies with massive troves of data, and that this new kind of passive surveillance will mostly impact low-income communities of color. By allowing the gathering and sharing of data which can potentially be accessed by law enforcement, the TCN opens the door to potential violations of the Fourth Amendment of the US Constitution.

Data Broker LexisNexis Sued for Helping ICE Target Immigrant Communities, from Democracy Now, August 2022 - Exhibit I
https://www.democracynow.org/2022/8/19/immigrant_rights_groups_sue_data_broker

Companies are already offering to sell data to law enforcement agencies in order to increase surveillance capabilities.

Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police - Exhibit J
https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police

This data is not just available to law enforcement agencies. It's available to anyone who's willing to pay for it. Please see the story below about how the unregulated data ecosystem enabled anti-abortion groups to target women visiting abortion clinics.

The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics - Exhibit K
https://www.lawfaremedia.org/article/data-broker-caught-running-anti-abortion-ads%E2%80%94-people-sitting-clinics#:~:text=Recently%2C%20the%20Federal%20Trade%20Commission,be%20used%20to%20identify%20medical

In 2017, the Massachusetts attorney general reached a settlement with the data broker Copley Advertising—which surveilled women and other people visiting abortion clinics, geofenced advertising around those clinics, and then enabled anti-abortion organizations to run anti-abortion ads to people sitting in clinic waiting rooms.

Clear Channel may be hoping to convince us that a device ID is not personally identifiable information simply because it may not immediately indicate the individual's name or address, but they acknowledge that they also use data from other sources, and their Radar web page makes clear that they're able to target individuals and to observe devices. Their web page makes clear that their goal is to gather the most detailed information possible to target consumers precisely.

The evidence presented above demonstrates that Clear Channel is violating the privacy rights of citizens of the State of California, and could potentially make them vulnerable to violations of the US Constitution. Through intermediary Allvision,

Metro has already signed agreements which allow it to receive revenue from digital billboards operated by Clear Channel.

The Threat of Commercial Surveillance Is Growing, as Recognized by the Federal Government

The Federal Government recognizes the threat of commercial surveillance, including surveillance advertising, as evidenced by actions taken by the Federal Trade Commission and members of the US Congress.

The FTC has sought public comment on the harms stemming from commercial surveillance as it considers whether new rules are needed to protect people's privacy and information.

FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices, Exhibit L
https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices

The Federal Trade Commission today announced it is exploring rules to crack down on harmful commercial surveillance and lax data security. Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Mass surveillance has heightened the risks and stakes of data breaches, deception, manipulation, and other abuses.

"Firms now collect personal data on individuals at a massive scale and in a stunning array of contexts," said FTC Chair Lina M. Khan. "The growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent. Our goal today is to begin building a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices and what those rules should potentially look like."

Surveillance advertising is a problem that has caught the attention of members of the US Congress. In September of this year, Representatives Jan Schakowsky and Anna G. Eshoo and Senators Ron Wyden and Cory Booker introduced the Banning Surveillance Advertising Act.

Banning Surveillance Advertising Act, Press Release from US Rep. Jan Schakowsky - Exhibit M
https://schakowsky.house.gov/media/press-releases/schakowsky-eshoo-wyden-booker-introduce-bill-ban-surveillance-advertising

"The 'surveillance advertising' business model is premised on the unseemly collection and hoarding of personal data to enable ad targeting. This pernicious practice allows online platforms to chase user engagement and increase their

revenue at the expense of our safety and security. It is at the root of disinformation, discrimination, voter suppression, privacy abuses, and so many other harms. The surveillance advertising business model is broken," said Representative Anna Eshoo.

The EIR Offers No Details on the Communications Hardware and Network Infrastructure to Be Used in the Communications Network

The project's proponents call it the Transportation Communication Network, but amazingly, the EIR gives almost no information about the actual communications network. It does not describe the types of communications hardware to be installed or the number of devices. It does not describe the network infrastructure or its lifespan or how the components will be disposed of at the end of their useful life. Neither the Energy chapter of the EIR or Appendix F, Energy Calculations, appear to offer any assessment of the energy to be consumed by the communications network component of this project. On page II-5 of the Projection Description, in the section titled "TCN Components/Intelligent Technology", we find the following:

"The TCN Structures would be equipped with Metro's Regional Integration of Intelligent Transportation Systems (RIITS), which provides comprehensive, timely, and real-time information among freeway, traffic, transit, and emergency systems, and across various agencies [...,]"

Further on in the same paragraph we find this language:

"The additional intelligent technology components of the TCN Program would assist Metro in increasing the quantity and speed of data collection of real time travel/traffic data, processing, and transmission to transportation agencies. Further, the TCN Structures may include live video and security feeds to supplement Caltrans' limited number of existing cameras on the freeway and street corridors for public safety."

In describing the communications network component of the project, this is about as specific as it gets. While the EIR contains numerous claims regarding the improved collection of real-time traffic information and the benefits to both drivers and bus riders, it does not actually explain how the communications network will do this. Again, there is no description of hardware, network infrastructure, device lifespan or energy consumption with regard to the communications component. Simply saying that the TCN structures will be "equipped with Metro's [RIITS]" does not give the public the information it needs to understand what this entails. Furthermore, the EIR gives us no information about how the TCN structures will connect with the existing RIITS system.

In short, the EIR fails to offer the specific details on the communications network component that would enable the public to assess its impacts and its benefits. And because the EIR is entirely focussed on the impacts related to the digital billboards

to be installed, we suggest that Metro consider changing the title to "Digital Billboard Network".

Metro TCN EIR Does Not Address Cumulative Impacts from Adding 86 Digital Billboards to Exisiting Number of Digital Billboards in LA County

The EIR prepared by LA Metro does not assess cumulative impacts that will result from the addition of the 86 TCN digital billboards to the numerous existing digital billboards in the City of LA and surrounding cities, including West Hollywood, Inglewood, Long Beach and Downey.

Images of Existing Digital Billboards in the City of LA and Surrounding Cities - Exhibit N

The EIR also fails to assess cumulative impacts in conjunction with the Sidewalk & Transit Amenities Program (STAP), which involves the placement of digital display panels on bus shelters. The City of LA was considering adoption of the STAP at the same time that it was developing the Transportation Communication Network with Metro.

The EIR does not assess cumulative impacts with regard to light pollution or the increased demand on the electrical grid, nor does it make any effort to calculate impacts from electronic waste as these devices come to the end of their life cycle and must be replaced.

The Amended Findings Make Claims that Are Not Supported by the Evidence

The Amended Findings make numerous claims about the benefits of the TCN, but do not offer evidence to support these findings. The existing Regional Integration of Intelligent Transportation Systems (RIITS) already performs many of the functions described in the findings, and neither the EIR nor the findings give any details about how the TCN will actually extend/improve its performance. The Amended Findings make many claims about how the TCN supports the Mobility Plan's policies, but offer scant details. While offering vague language about improving the collection and sharing of data, the Amended Findings do not appear to be based on any actual analysis of how the TCN will improve LA's transportation landscape.

RIITS is a valuable, proven system that currently offers many benefits to transit agencies in the LA area, but the proponents of the TCN do not explain how the project will enhance it. RIITS could easily be expanded without any digital billboards at all.

The Amended Findings make the following claims:

Policy 4.1 New Technologies:

Support new technology systems and infrastructure to expand access to transportation choices. Aside from digital displays, the TCN structures will also contain new technology systems to collect transportation data, promote Metro's services, and plan for future road improvements utilizing data collected by each TCN structure. The TCN structures will assist Metro and the City in increasing the quantity and speed of data collection of real-time travel and traffic data, which will be shared with different governmental agencies.

The authors claim that the TCN structures will contain "new technology systems", but offer no details on these systems. They claim the TCN will increase the speed and quantity of data collection without explaining how.

Policy 4.2 Dynamic Transportation Information:
Support a comprehensive, integrated transportation database and digital platform that manages existing assets and dynamically updates users with new information.

RIITS already offers a transportation database that manages assets and updates users with new info. Specifically how will the TCN support RIITS?

Policy 4.7 Performance Evaluation:
Evaluate performance of new transportation strategies through the collection and analysis of data.

Again, the EIR offers no details on the communications infrastructure that will fulfill this promise.

Policy 4.11 Cohesive Regional Mobility:
Communicate and partner with the Southern California Association of Governments (SCAG), Los Angeles County Metropolitan Transportation Authority (Metro), and adjacent cities and local transit operators to plan and operate a cohesive regional mobility system.

All of this is already done through RIITS, and the EIR gives no information on the TCN's communications infrastructure and how it will extend/improve RIITS.

Digital Billboards by the City's Roads and Freeways Will Like Increase Distracted Driving

Placing scores of digital billboards alongside the City's roads and freeways will result in an increase in distracted driving, likely causing a greater number of traffic injuries and fatalities. We are alarmed at the fact that the TCN Ordinance's definition of a "digital display" includes moving images, flashing images, video and animation.

From TCN Ordinance
Digital Display. *A sign face, building face, and/or any building or structural component that displays still images, scrolling images, moving images, or*

flashing images, including video and animation, through the use of grid lights, cathode ray projections, light emitting diode displays, plasma screens, liquid crystal displays, fiber optics, or other electronic media or technology that is either independent of or attached to, or integrated into a building or structural component, and that may be changed remotely through electronic means.

Does the City truly believe 1,200 square foot billboards featuring video advertisements will not increase the risk of distracted driving? Neither the City of LA nor Metro have conducted any meaningful analysis of safety risks associated with the TCN program. This is especially troubling given the high number of traffic fatalities in the City of LA, and the City's failure so far to reduce that number. In 2015 the City implemented the Vision Zero program with the goal of eliminating traffic deaths by 2025. Instead, the number of traffic fatalities has been increasing, going from 186 in 2015 to 312 in 2022. Digital billboards displaying animated messages are likely to drive the death toll even higher.

For the reasons given above, CBLA strongly opposes approval of the TCN Ordinance. We urge the City Planning Commission to reject this ordinance.

Sincerely,
Casey Maddren
Citizens for a Better Los Angeles

EXHIBIT A

BUSINESS

Column: Billboards that follow you? It's not sci-fi. They're already here

Los Angeles Times

Remember the scene in "Minority Report" where Tom Cruise is marketed to by digital billboards? We're now a step closer to that reality. (DreamWorks/20th Century Fox)

BY DAVID LAZARUS | BUSINESS COLUMNIST

AUG. 25, 2020 6 AM PT

Clear Channel Outdoor, one of the world's largest billboard companies, will in coming days roll out technology across Europe capable of letting advertisers know where people go and what they do after seeing a particular

billboard.

Sounds creepy, no?

Well, brace yourself. Clear Channel has been quietly using this technology in the United States for the last four years, including in Los Angeles.

“They’re spying on you in your own neighborhood,” said Jeff Chester, executive director of the Center for Digital Democracy.

“You don’t know it’s happening,” he told me. “You don’t know who they’re sharing the information with.”

Chester and other privacy advocates said Clear Channel’s system is an example of how private companies are building out commercial surveillance networks right under our noses.

“The scary thing is that there are so many companies handling different pieces of this, the ecosystem is enormous,” said Alan Butler, interim executive director and general counsel for the Electronic Privacy Information Center in Washington, D.C.

“All this data is being collected and we have no idea how it’s being used,” he said.

Clear Channel isn’t alone in developing what’s known as “out of home marketing” — a decidedly benign term for such a potentially invasive practice.

Different companies are rushing to install similar systems in malls, subways and other crowded venues. The aim is not just to see where you go and what you do but also to prompt impulse purchases at nearby merchants.

If you're like me, the image that comes to mind is that scene from Steven Spielberg's "Minority Report" where Tom Cruise is recognized and marketed to as he passes a series of digital billboards.

Current out-of-home marketing technology isn't like that — yet. But experts say it's just a matter of time.

"We're already used to being tracked online," said Lori B. Andrews, director of the Institute for Science, Law and Technology at the Illinois Institute of Technology. "Now it's bleeding into the real world."

Clear Channel is an especially powerful force in this field because its more than 500,000 print and digital billboards worldwide provide a far-reaching foundation from which to track passers-by and share data with marketing partners.

The company calls its technology Radar. The system, Clear Channel says, "leverages anonymous, aggregated mobile location data to help advertisers understand consumer mobility, behavior and true campaign impact."

An animated video for Radar appears to depict people on foot and in cars passing a Clear Channel billboard and connecting automatically via Wi-Fi, providing marketers with "highly customized solutions" to help them "connect with the right customers at the right time and place."

That's a bit misleading.

Jason King, a Clear Channel spokesman, acknowledged to me that the company "does not equip its billboards with technology aimed at tracking individuals."

Rather, Clear Channel gathers location and tracking information from multiple sources — apps, data firms — and then analyzes the info for insights about how people behave after passing a Clear Channel billboard.

The idea is to be able to tell advertising clients that a consumer is likely to visit the client's business after being exposed to a billboard touting the client's products or services, or to market to that consumer based on their location.

King said Radar "helps advertisers understand what happens after someone sees their ad."

Wireless companies for years have been using "geolocation" data from smartphones to bolster advertisers' marketing campaigns.

Basically, if you carry a phone, your whereabouts are known to your wireless provider every second of the day — and the companies make money selling that info to others.

Clear Channel is taking this capability up a level by creating a bridge between a consumer's location and their exposure to an outdoor marketing pitch.

Now advertisers can go beyond just passively plastering a message on a billboard. They can follow you after you've seen the ad, and watch where you go and what you do.

Clear Channel is being disingenuous when it insists all data collected as part of Radar is anonymous, privacy experts say.

Kyle M.L. Jones, an Indiana University assistant professor who focuses on data mining, said that for a company to target you with advertising, it has to know who you are and have an idea about your personal tastes.

Even if you're identified only by a number affiliated with your phone, rather than by your name, it's not difficult to extrapolate from there if a more robust marketing profile is desired.

"Enough of a mixture of geographic, behavioral and demographic data will almost inevitably open up opportunities for re-identification," Jones said. "It's hard to know what their privacy-protecting practices are, but their practices have risk."

Although Clear Channel's King played down the "Minority Report" implications of Radar, the company's chief executive, William Eccleshare, told the Financial Times that the September introduction of Radar in Europe will create a host of eye-opening opportunities for advertisers.

"We can follow your movement to a store," he said. "We can follow what you purchase. And yes, we can look at your viewing habits that evening if you pass an ad for a Netflix show."

For businesses, that's pretty exciting.

For consumers, it should send a shiver down your spine.

Nanda Kumar, an associate professor of information systems at New York's Baruch College, said "lackluster privacy laws" are partly to blame for companies feeling free to monitor consumers as they go about their daily affairs.

Many out-of-home-marketing businesses "take individuals' privacy for granted and collect information from them opaquely without providing consumers any reasonable ways to control the flow of their data," he said.

I wrote last week about how difficult some companies make it to opt out of data sharing. Clear Channel is no exception.

The company's privacy policy says it's up to individual consumers to "refer to your device's or browser's technical information for instructions on how to delete and disable all or some cookies, and other tracking tools, as available, including how to reset your advertising identifiers and limit advertising tracking."

Yeah, good luck with that.

The privacy policy also acknowledges that even though Clear Channel primarily relies on "de-identified" personal information, it does in fact disclose identifiable info to business partners.

This can include your name, address, purchase history, online behavior and "inferences drawn from any of the foregoing to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes."

Inferences about people's intelligence, predispositions and psychological trends?

Not so benign after all.

"When they made 'Minority Report,' it wasn't science fiction," said Chester at the Center for Digital Democracy. "That scene was based on what they knew was actually coming."

And here we are.

BUSINESS TECHNOLOGY

David Lazarus

Twitter Instagram Email Facebook

David Lazarus is an award-winning business columnist for the Los Angeles Times. He also appears daily on KTLA Channel 5. His work runs in newspapers across the country and has resulted in a variety of laws protecting consumers.

EXHIBIT B

Digital Billboards Are Tracking You. And They Really, Really Want You to See Their Ads.

How the most intrusive parts of the web are expanding into the real world, complete with data collection and targeted ads

By Thom ermain

November 13 019

CR privacy and technology reporter Thomas Germain in New York City's Times Square, a moment after his photo was triggered on a billboard across the street.

Karen Shinbaum/Consumer Reports

On a bright Friday morning, Frank O'Brien is giving me a tour through Times Square in New York City. Thousands of strangers are milling around us on the sidewalk, and in the crowd, it's easy to feel anonymous. But according to O'Brien, many of the billboards and screens towering over our heads in every direction know a lot about who we are.

"As we stand here, there are devices behind that screen that are picking ID numbers from our cell phones," O'Brien tells me, gesturing toward a billboard at 42nd Street and 7th Avenue. Using those devices and other technology, he says, "We know who is in Times Square at a given moment."

O'Brien, the CEO of a high-tech advertising platform called Five Tier, launches an app on his phone. He taps a few buttons and in an instant, the billboard changes to display a picture of me I'd sent him the day before. Suddenly, I'm famous, with a 20-foot-high photo of me gazing out over the tourists. "It still amazes me sometimes," he says.

Five Tier doesn't typically change the content manually. In practice, automated systems update the ads in real time based on a stream of data from nearby cell phones, which is combined with personal information on those passersby from data brokers who trade in the details of consumers' lives.

When we go out into public, we are often surrounded by screens showing ads. They can be on the side of the road, at the gym, in store windows, in doctors' offices, and in elevators. You might assume that the marketing messages are playing on a loop, but sometimes these ads are changing because people like you are nearby.

ON DIGITAL
CY

uide to Digital
y & Privacy

ed Reviews on
n Can Trick
ers

nd Destroy Your
d Online Accounts

You Watch a Super
d, It May Be
ing You Back

igital Lab

Data including your gender, age, race, income, interests, and purchasing habits can be used by a company such as Five Tier to trigger an advertisement right away. Or, more often, it will be used for planning where and when to show ads in the future—maybe parents of school-age children tend to pass a particular screen at 3 p.m. on weekdays, while 20-something singles usually congregate nearby on Saturday nights.

Then the tracking continues. Once your phone is detected near a screen showing a particular ad, an advertising company may follow up by showing you related ads in

your social media feed, and in some cases these ads may be timed to coordinate with the commercials you see on your smart TV at night.

It doesn't stop there. Advertisers are keenly interested in "attribution," judging how well a marketing campaign influences consumer behavior. For instance, is it better to target people like you with online ads for fast food right after you see a restaurant's new TV commercial, or to wait until after you drive by a new billboard the next day? The advertising industry looks for the answers by watching where you go in person, what you do online, and what you buy with your credit card.

These aren't futuristic scenarios. They are a recent but growing trend, according to executives in the advertising business. "The industry has really started to wake up to this within the last year," says Ian Dallimore, the director of digital growth for Lamar Advertising, a leader in out-of-home advertising. "If you're not using data to better plan and buy ads, then you're probably not doing out-of-home the right way."

Researchers say that as tracking and ad targeting spill over from the web into the real world, our collective privacy and sense of control are eroding. If you don't want to see ads at home, you can close your browser or turn off your phone, but you can't avoid the ads you see in public. And there's no practical way to completely block the location tracking used to place those ads.

"Advertising has been increasingly interested in using behavioral psychology to nudge people in particular ways," says Matthew Crain, assistant professor of media and culture at Miami University in Oxford, Ohio. "The ability to gather data on what we do and how we move through the world makes that more effective. It raises new questions about the lines between persuasive advertising and manipulation."

The out-of-home market provides a fresh window into how consumer data is being used by advertisers. Soon, it seems, almost every part of your life may be

just another data point for marketing clients to consider and another opportunity to monetize your attention by showing you an ad.

Hey, I Spotted You at Kohl's. Wanna See a DSW Billboard?

Out-of-home advertising covers everything from old-fashioned billboards to the little TV screens on the sides of gas pumps. Until recently, the companies that handled these ads only thought about competing with each other, says François-Xavier Pierrel, chief data officer at JCDecaux, a global leader in the industry. But as targeted advertising took over the web, that changed—clients started to expect more data, and more personalization. "We had to step up," Pierrel says.

Today, the out-of-home advertising business is adopting the model that runs ads on the web, with more ads being sold based on granular details about the audiences that will be exposed to them.

Last summer, Lamar Advertising helped the shoe retailer DSW use out-of-home screens to promote the grand opening of a new store at a mall in Mount Prospect, Ill., a suburb northwest of Chicago. The company found consumers to target through "geofencing," using location-tracking technology to sniff out cell phones that entered competing stores, such as Kohl's, Macy's, Marshalls, and Nordstrom Rack. The owners of those phones would be good prospects, so Lamar used geofencing at screens around town, waiting until enough of those phones were detected nearby, and then automatically triggering ads for the DSW store.

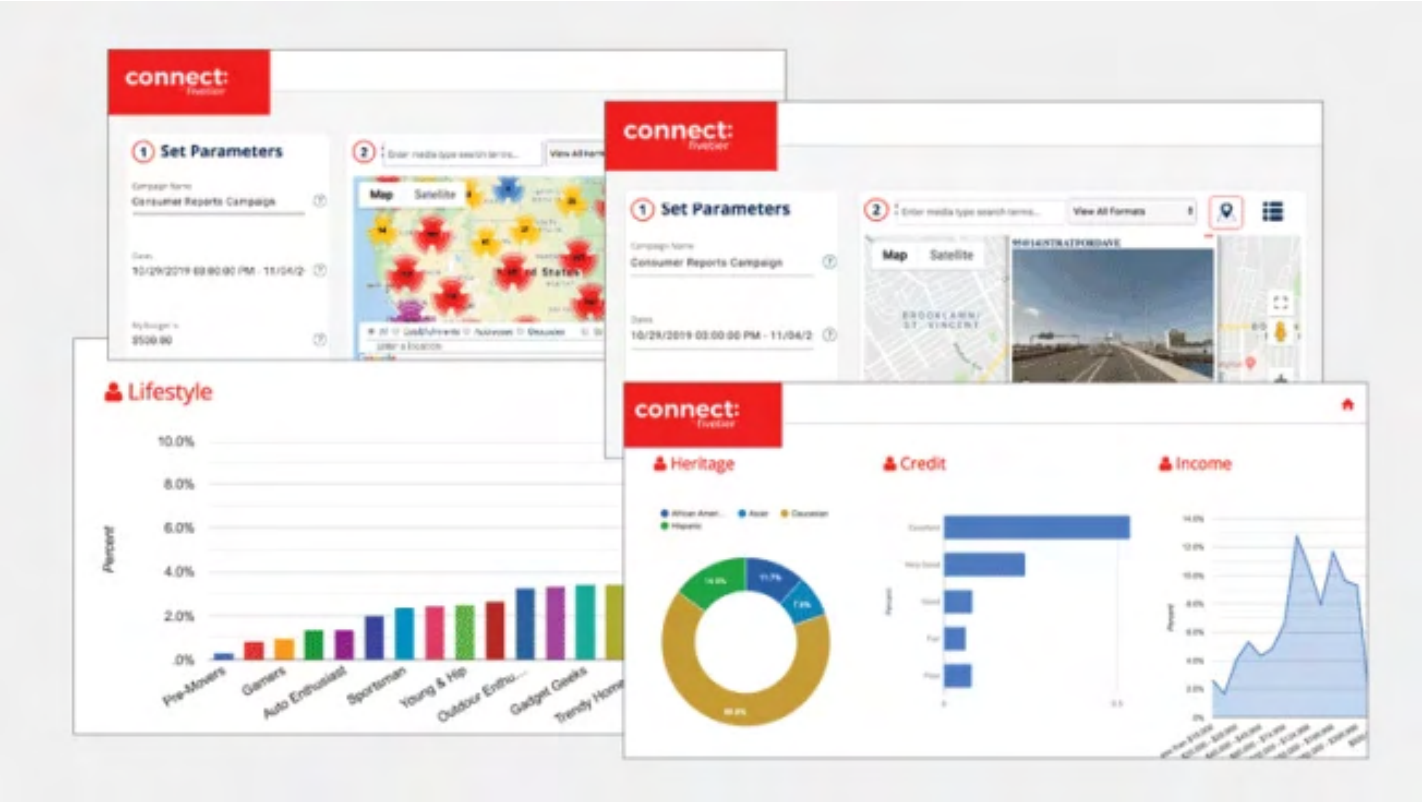
"It's happening everywhere," says Lamar's Dallimore. "As the data changes, we're changing the creative in real time."

Later, the company wanted to measure how many people who were exposed to the DSW advertisements went to the new store. Using location tracking, Lamar estimated that 442 people walked into the DSW as a result of the ads.

Out-of-home ad networks typically don't learn the names or email addresses of individuals, but the data they receive can feel highly personal.

Back at Five Tier's office in midtown Manhattan, O'Brien shows me the system that runs the company's advertising platform. One tab he pulls up displays a list of mobile devices that are currently in Times Square. Another shows the number of 18- to 24-year-old women in range of a particular set of screens in Germany. A third loads metrics from an ad campaign for a car dealership in Oklahoma, laying out the genders, ages, races, credit scores, income levels, and lifestyles of people seen in the area at different times of the day.

"We want data as fast as it's available," O'Brien says. "We have some that's coming in every second."



Consumer Reports

Out-of-home advertising networks operated by companies such as Five Tier allow clients to use online dashboards to (clockwise from upper left) set up ad campaigns;

look for digital billboards where their ads can be shown; and learn details about frequent passersby, such as their race, credit score, income, and interests.

Would-be clients can bid on out-of-home advertising slots by using automated platforms operated by Five Tier, JCDecaux, Lamar, and other companies. And more big tech companies are moving into this business—Google confirmed to Consumer Reports that it is starting to experiment with out-of-home advertising.

You can glimpse the potential scale of the out-of-home advertising industry courtesy of a firm called Adomni, headquartered in Las Vegas. Type your city into the company's website, and a list appears with all the screens where Adomni can serve an ad. There are tens of thousands of them in the U.S. On a recent day, you could play 15-second ads in Times Square for just over $10 a pop, while 42-and-a-half cents bought the same screen time on a highway billboard near Citi Field, home of the New York Mets. In Mount Prospect, Ill., ad time on a network of screens in doctor's office waiting rooms cost about a quarter.

Out-of-home ad companies don't need to own the screens they use, and often they don't. Any display connected to the internet can be hooked up to an advertising network. "Think of us as the pipes," says Jonathan Gudai, Adomni's CEO. "Screens are popping up everywhere around us. As long as it's in a high enough traffic area, then it's a good candidate to be listed on our platform and monetized."

Tag—You're a Prospect

Out-of-home advertising relies on a tangled web of companies that collect, analyze, and trade information about consumers. "We do not produce any mobile data ourselves," JCDecaux's Pierrel says. "We buy it from third parties."

One location data broker that specializes in out-of-home advertising is PlaceIQ. The company pairs location data collected from software embedded in all kinds of mobile apps with additional details sourced from other data brokers to create a detailed picture of the people passing through an area.

Location data brokers can generate some details based on physical tracking alone—where you shop, work, or attend church can say a lot that's of interest to advertisers. PlaceIQ says it also uses outside sources to gather information such as your recent purchases, driving habits, and what you watch on TV. The company's list of data partners includes companies such as Experian, Mastercard, and Nielsen Catalina Solutions. (PlaceIQ did not respond to Consumer Reports' request for comment.)

Karen Shinbaum/Consumer Reports

Bluetooth beacons (left) and WiFi sniffers are placed in many public areas,

including shopping centers and malls, to determine which smartphones—and their owners—are nearby. A number of marketing companies use these devices to plan advertising, while others rely on data collected and shared by mobile apps.

Here's how it works. A location data broker may gather data streaming off mobile apps on your phone and record the fact that you go to the gym twice a week. Other companies may know that you frequently use your credit card at natural-foods grocery stores and that you subscribe to a running magazine. Later, when a food manufacturer wants to promote its new organic protein bar, the advertising firm it hires can target you for a marketing campaign, along with lots of others consumers—who have all been tagged as health fanatics.

The location-tracking part of that process depends on one piece of technology not owned by the data companies: your smartphone.

"I would expect that almost everyone has at least one app on their phones that sends location data to third parties," says Serge Egelman, a digital security and privacy researcher at the University of California, Berkeley, who studies how apps gather consumer data.

"Your device is constantly broadcasting unique identifiers," Egelman says. For instance, your phone transmits Bluetooth and WiFi MAC addresses to help it discover and communicate with wireless networks and other devices. Some location brokers make use of small, inconspicuous devices that can pick those numbers out of the air to identify the phones that wander by. These devices are scattered across public spaces. (You may be sitting near one right now.)

However, Apple and Google, the maker of the Android operating system, have recently taken steps to make it harder for phones to be tracked this way.

Targeted Ad, or Just a Billboard?

In the advertising industry, some people are concerned about a privacy backlash, even as personalization is making ads more relevant and useful to consumers.

"We are moving towards a world in which advertising will essentially follow us around based on data from our phones or other devices," says Jeremy Katz, worldwide editorial director for Ogilvy, one of the world's leading advertising agencies. "But I don't think we've decided as a society whether or not that's how we want our world to look."

Several out-of-home advertising insiders echoed those concerns. It would be easy for companies to target ads in public directly at individuals, several executives told me, but for now, that isn't happening. That's partly because it's not cost-effective but also because it might feel creepy. "For us it's about transparency," Lamar's Ian Dallimore says. "Our biggest thing is making sure we're not being too specific to an individual."

Companies such as Adomni, Five Tier, JCDecaux, and Lamar emphasize that they don't learn identifying details such as the names, email addresses, or phone numbers of the people whose data flows across their screens. And most of the information is aggregated—they want to know how many people of a certain target audience are present at a particular time, not who each individual is. They don't need that information to plan ad placements and to keep the revenue flowing.

Still, the data that fuels advertising systems, online and offline, is highly personal. "I guess I'm glad they're not specifically interested in me as an individual, but the privacy violation is the same," says Justin Brookman, who directs privacy and security policy at Consumer Reports. "The data collection and sharing is still happening."

Lawmakers and regulatory agencies such as the Federal Trade Commission are paying more attention to data privacy, but it's not clear how the measures being put in place will affect the way individuals are tracked through their phones,

and how the data is used by data brokers and their clients. Several out-of-home advertising companies I spoke with said they already comply with GDPR, Europe's sweeping privacy regulation that was implemented in 2018. The companies also say they are prepared for the most stringent privacy legislation in the U.S., the California Consumer Privacy Act, which is supported by Consumer Reports and goes into effect in January 2020.

Five Tier's Frank O'Brien says that, just like every other industry, the out-of-home advertising business should be regulated. But for now, if you're not comfortable with how out-of-home advertising uses your information, you don't have much recourse. "I don't think there's anything you can do about it," he says.

In the meantime, out-of-home advertising is charging ahead. Last summer, Adomni ran a campaign for the Ultimate Fighting Championship based on the daily travel patterns of consumers singled out as potential fans. Over the past year in Buffalo, N.Y., Lamar targeted consumers exposed to out-of-home advertising for Tim Hortons restaurants with additional ads on their mobile devices. And in Times Square, Five Tier helped promote an event by a Sikh religious organization by playing ads when the target demographic was nearby.

If this kind of geofencing and ad targeting bothers you, you can adjust the location permissions on your phone to limit which apps have access to your GPS data, and delete as many apps as possible. You can put your device on airplane mode, or even leave it at home. That will all make a difference, but you can't opt out entirely if you like using 21st century technology.

Recently, I was heading home after meeting a friend for dinner. I'd been thinking about selling my old Samsung Galaxy phone, and as I approached a screen on the side of a bus stop, a new ad popped up, promoting used cell phones on eBay. Was the ad triggered because I was there and I'd been researching how much I could get for my used phone in recent weeks? Had some advertising company noticed that eBay shoppers tended to pass by this corner around 8 p.m. on Thursdays? Or was the ad just playing on a loop?

The internet has long since changed the way we access information and communicate with each other, and today it's altering the way we experience the physical world. As companies fight for your attention, you can probably feel it all happening, but for most people, the details are just out of reach.

Want more Digital Privacy news?

Follow this interest and we'll customize your news feed with this content.

What's New from Consumer Reports Follow

Get trusted advice delivered weekly straight to your inbox.

See More Interests

Sign Up

Thomas Germain

I want to live in a world where consumers take advantage of technology, not the other way around. Access to reliable information is the way to make that happen, and that's why I spend my time chasing it down. When I'm off the clock, you can find me working my way through an ever-growing list of podcasts. Got a tip? Drop me an email (thomas.germain@consumer.org) or follow me on Twitter (@ThomasGermain) for my contact info on Signal.

More From Consumer Reports

BUSINESS

How Digital Billboards Target Passersby (Hint: It's Cellphone Data)

February 7, 2020 · 4:25 PM ET
Heard on All Things Considered

KAREN DUFFIN

3-Minute Listen

PLAYLIST Download Transcript

More and more digital billboards are popping up around the U.S. Many are tracking us through our cell phones — similar to what happens online. Here's a close look at one in Times Square.

MARY LOUISE KELLY, HOST:

We've come to expect we're being tracked by advertisers online. It's also happening in the physical world with digital billboards. Karen Duffin from NPR's Planet Money podcast went to one of the most iconic advertising locations in the world.

KAREN DUFFIN, BYLINE: I went to the heart of Times Square to look at a billboard with Frank O'Brien, who is the CEO of a marketing software company called Five Tier.

What's on the screen right now?

FRANK O'BRIEN: This looks like a jerk chicken ad placement.

DUFFIN: Using only an app on his cellphone, Frank can make this billboard say anything he wants. And today, he's making it say what we want.

O'BRIEN: So when I hit edit, it will launch as soon as I hit save. And there it is.

DUFFIN: Oh, my God. That's our ad.

Projected from this billboard onto Times Square is the Planet Money logo.

That's magical.

This little magic trick is actually the least of what this billboard can do. This billboard and many other digital billboards are watching you. O'Brien can tell which cellphones are near his billboards. The billboards themselves have sensors, and he also buys location data from cellphone carriers. He syncs that with data he buys about who owns those cellphones, from places like search engines, data aggregators, apps.

So he knows a lot about who sees the ads on his billboards. He knows age, race, gender, credit scores, lifestyle preferences. He knows what you've been doing before; sometimes he even knows what you've been doing before, during and after you look at his billboard.

O'BRIEN: The amount of data that can be pulled in is really infinite at this point. With mobile devices - latitude, longitude, altitude; if someone's in an elevator, changing an ad based on the floor that they're on in the elevator.

DUFFIN: Say you go up to the third floor of a mall, they might know from your Google searches that you've been looking for shoes. So they make the billboard on that floor say shoes are 20% off at Macy's. O'Brien says, don't worry - most of the data is anonymized, unless you've opted in to share your data, which sometimes just happens when you click agree on some terms and services agreement. At that point, he can track you and target ads at you very personally. O'Brien is very excited about this. He says it leads to much more relevant ads. But me - not so much.

Like, I know the ways in which it does make my life easier. But I know that I'm paying a price for it, which is the willingness to allow myself to be monitored most of the - pretty much all day, every day.

O'BRIEN: That's great. It's great to hear. And I think that...

DUFFIN: Wait - why is that great to hear?

O'BRIEN: Because you show an acceptance in some way.

DUFFIN: I mean, it doesn't feel like acceptance to me; it feels like resignation.

O'BRIEN: My God, there you are again with another great question.

DUFFIN: You can't flatter me out of this.

(LAUGHTER)

DUFFIN: It's not acceptance; it's like - it is resignation. It's a thing that's going to happen whether or not I like it.

O'BRIEN: And from the cave man days, you know, you can't change if it's going to rain today or if it's going to be sunny tomorrow or - so, OK, I'll agree that - you know, resignation. I concede. But it's the same resignation as, aw, shoot - it's raining outside.

DUFFIN: No because this is in our control. I can't control the rain. Can you control the rain? (Laughter).

He cannot. But if it does rain, his billboards will be happy to tell you about a discount umbrella just around the corner. And if all of this makes you nervous, not excited, you can always change the privacy settings on your cellphone. But the reality is, you're really only as private as your least private app.

Karen Duffin, NPR News.

(SOUNDBITE OF THE VENTURES' "PIPELINE")

EXHIBIT D, 1 – 4

Exhibit D 1

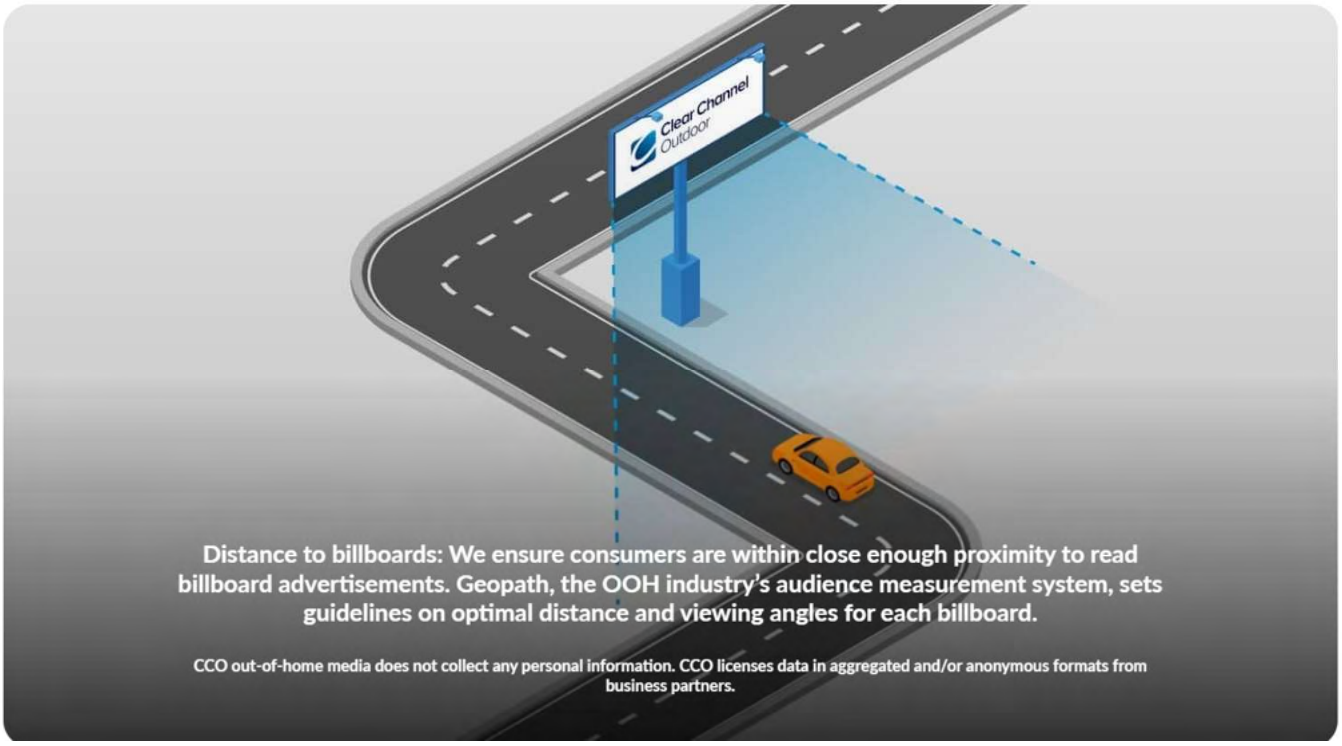


Exhibit D 2

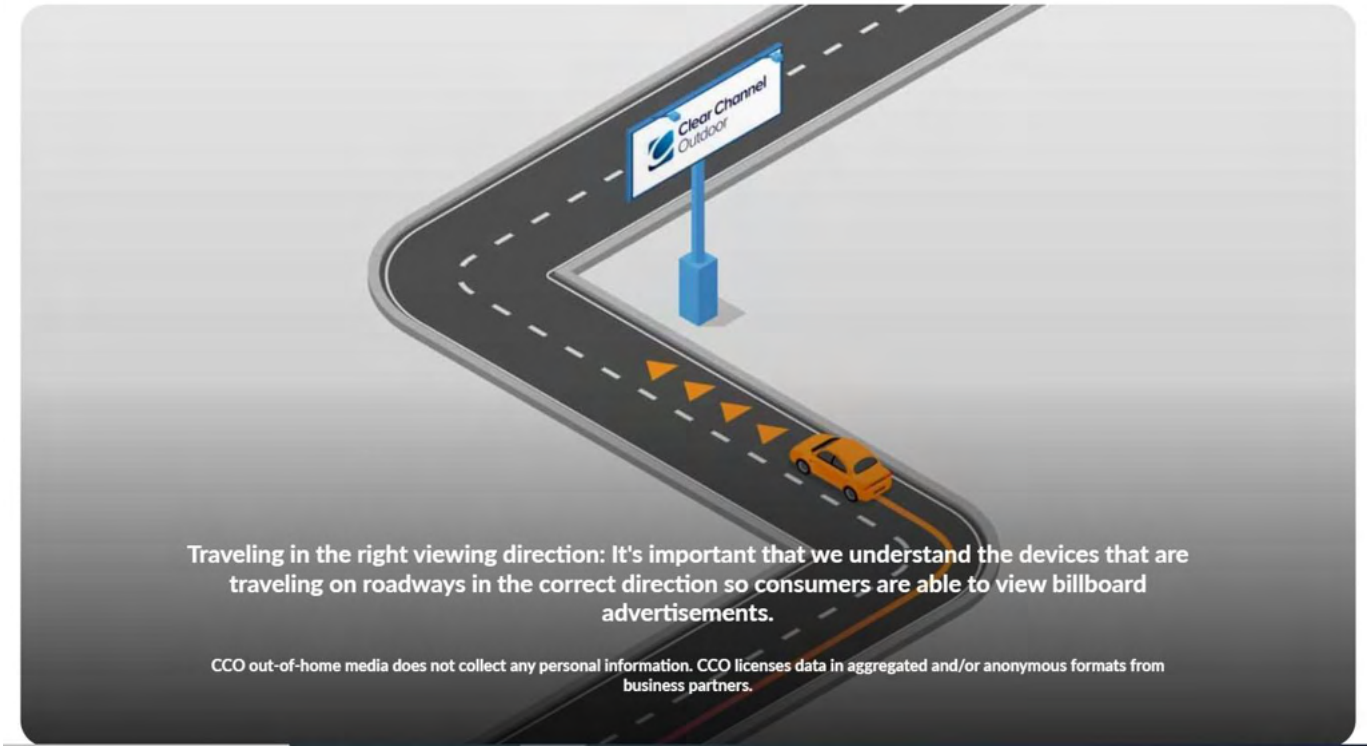


Exhibit D 3

Exhibit D 4

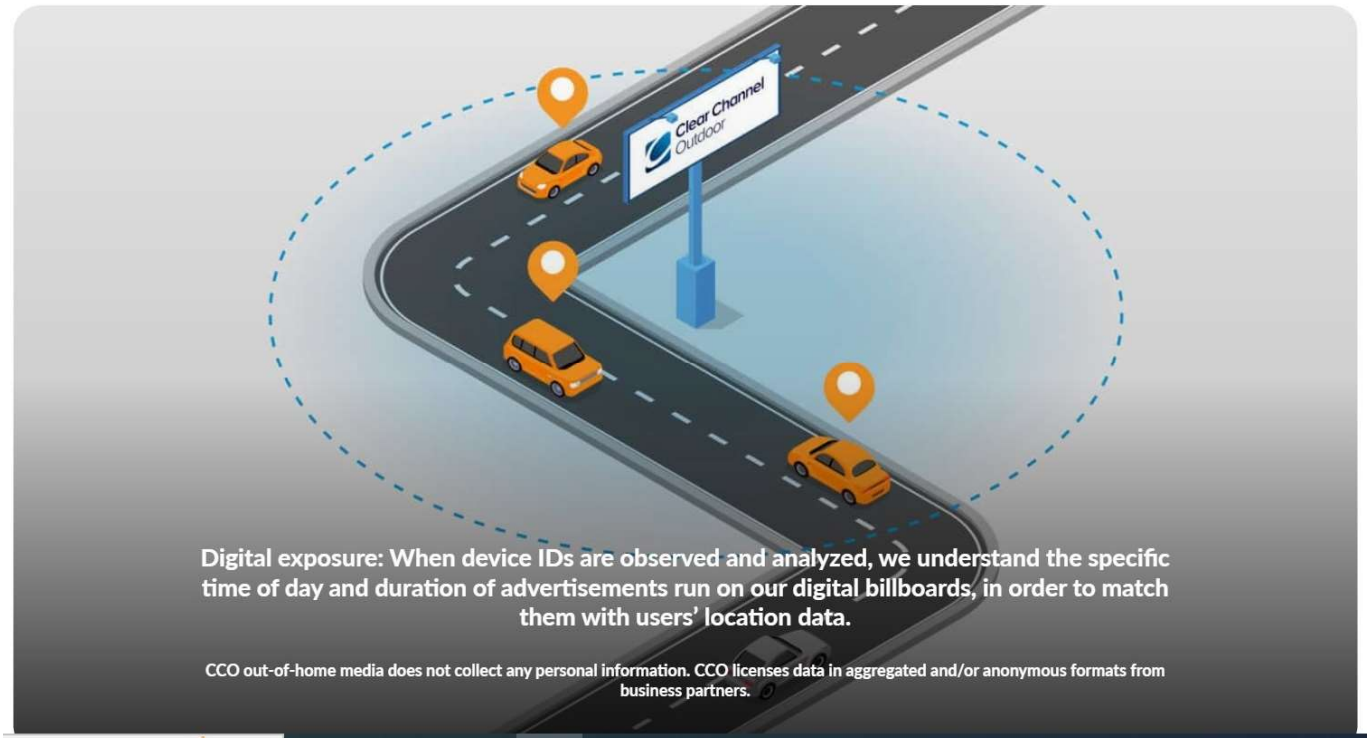


EXHIBIT E

Expert Warns Data Brokers Profit from Unregulated Surveillance

May 18, 2023 Innovation, Data, & Commerce Blog Big Tech Oversight & Investigations

With more Americans than ever using online apps and digital services, a stunning amount of information and personal data is being collected on you and potentially exploited by data brokers. Energy and Commerce is investigating how these companies are harvesting your data, selling or sharing it without your knowledge, and failing to keep it secure.

WHAT EXPERTS ARE SAYING: At an April 19 Oversight and Investigations Subcommittee hearing, Justin Sherman, a Duke University Senior Fellow and Research Lead for the Data Brokerage Project, outlined the risks and dangers of continuing to let data brokers exploit your data without consequence, saying:

"Data brokerage is a threat to Americans' civil rights, consumers' privacy and well-being, and U.S. national security. The entire data brokerage ecosystem—from

companies whose entire business model is data brokerage, to the thousands of other apps, advertisers, tech giants, and companies that collect, buy, sell, and share Americans' personal data—profits from unregulated surveillance of every American, particularly the most vulnerable."

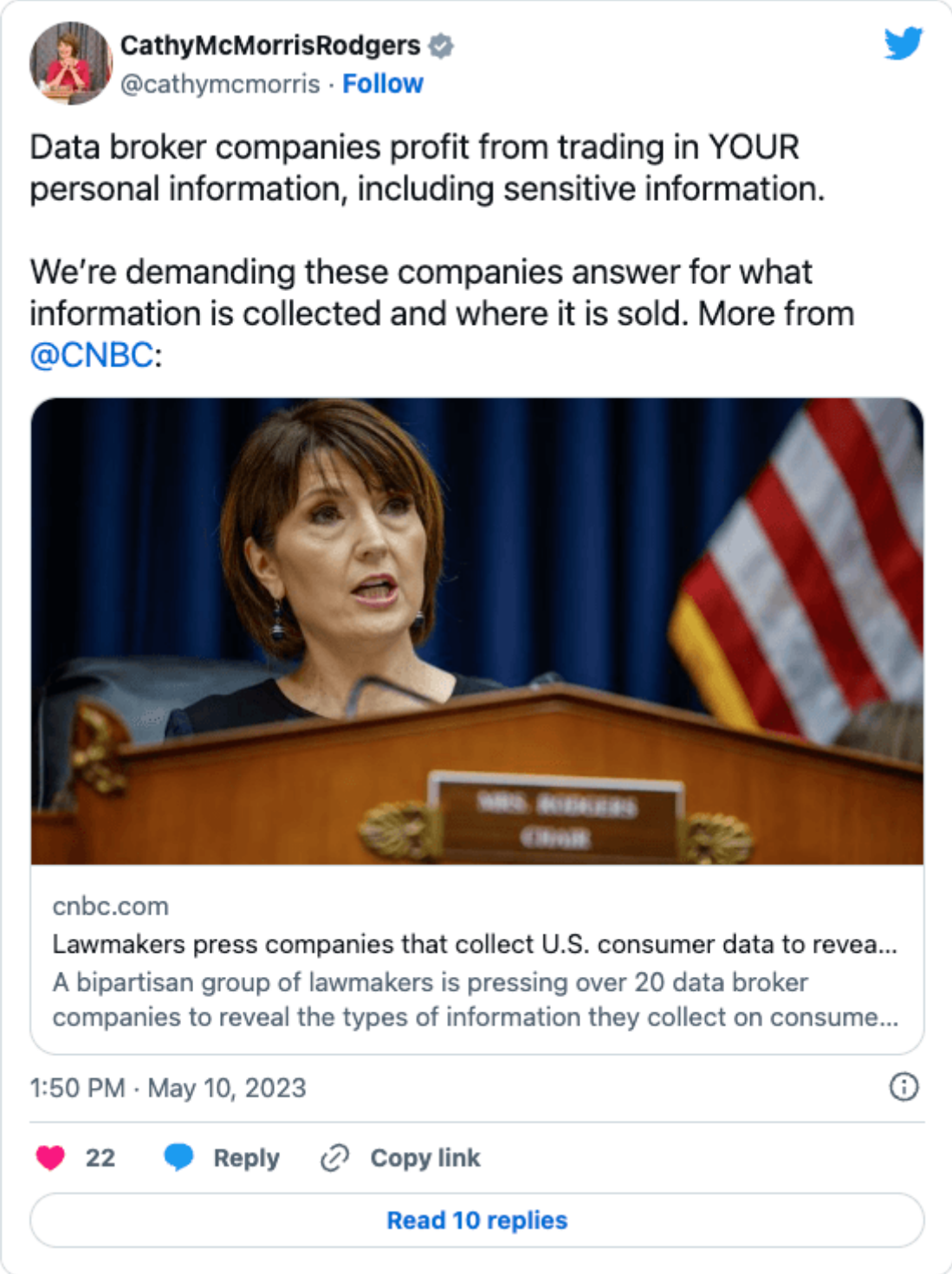
INFORMATION COLLECTED BY DATA BROKERS: The best way to change the status quo and restore Americans' control of their personal information is through a comprehensive data privacy and security framework, which will:

- Protect your sensitive information online—like GPS, health, and mobile phone data—from being transferred to data brokers and sold without your knowledge to another private entity or government agency.
- Prevent data brokers from aggregating your personal online information and selling that information to an employer or bank, who could then weaponize it to prevent you from getting a job or buying a home.
- Restore your control over your personal online information by giving you the power to demand data brokers delete all of the information they've collected and stop further collection.
- Require greater transparency around data brokers whose sole purpose is to covertly take money off of your information.

WHY IT MATTERS: You are the product driving data brokers' bottom line—these companies are willing to violate your civil liberties to turn a profit. This was made clear at the height of the COVID-19 pandemic, when data brokers collected Americans' location data and sold it to federal and local government entities, including government entities in California and Washington, D.C., as well as to the Center for Disease Control and Prevention. The information was then weaponized to spy on people during lockdowns to see who was attending activities, like church services, in person.

BIG PICTURE: Next-generation technologies like artificial intelligence and virtual reality will further deepen our reliance on online services and increase the amount of information collected. Without proper guardrails, that information can easily be sold to data brokers. Robust guardrails and a national privacy and data security standard would help prevent your information from being exploited further by these new technologies.

DON'T MISS: Last week, a bipartisan group of Energy and Commerce Committee Leaders sent letters to several data broker firms calling on them to be transparent about their data collection practices, selling practices, and the risks posed for Americans. The letters follow the April 19 Oversight and Investigations Subcommittee hearing examining the role of data brokers in the digital economy.



From *CNBC:*

The letters ask whether the brokers consider any type of data to be off limits for them to buy or sell, what restrictions they put on data they share with third parties

and how they verify the accuracy of the data they collect and distribute. Additional questions span from seeking to understand how much money the businesses make from selling data to how many sources they use to get that information.

Last month, the subcommittee on oversight and investigations held a hearing with expert witnesses to examine "the role of data brokers in the digital economy." The letters indicate the committee remains focused on this slice of the tech industry as it looks to pass comprehensive privacy legislation. It also shows that Congress is focused on a broader swath of companies than just the massive players like Google and Facebook that attract so much scrutiny.

CLICK HERE to read more.

Share on

Energy & Commerce Committee

ENERGY &

CHAIR RODGERS

OFFICE

2125 Rayburn House Office Building

Washington, D.C. 20515

Main: (202) 225-3641

EXHIBIT F

RE-IDENTIFICATION OF "ANONYMIZED DATA"

Boris Lubarsky*

CITE AS: 1 GEO. L. TECH. REV. 202 (2017)
https://perma.cc/86RR-JUFT

I. INTRODUCTION

Today, almost everything about our lives is digitally recorded and stored somewhere. Every interaction with technology creates data about that user. Each credit card purchase, medical diagnosis, Google search, Facebook post, or Netflix preferences is another recorded data point about that individual user. Beyond that, every census report, home purchase, voter registration, medical history, and cell phone geolocation is recorded and stored. This data is then analyzed and used by the entities that collect it. Netflix analyzes user preferences to recommend movies; medical researchers study patient data to find new treatments and cures; and Google reviews search queries to improve its search results. That aggregated data is also sold and transmitted to third parties, such as analytics companies, marketing companies, or commercial data brokers.

Currently there are some legal protections that aim to prevent the disclosure or sale of personally identifiable information, such as name, Social Security numbers, and medical conditions when data is sold or transmitted.

* GLTR Staff Member; Georgetown Law, J.D. expected 2018; Georgetown University, B.S.F.S. 2011.

However, if that data is scrubbed, of a small category of personally identifiable information it can be considered "anonymized" data.[1] There is no regulation of "anonymized" data: it can be sold to anyone and used for any purposes. The theory is that once the data has been scrubbed, it cannot be used to identify an individual person and is therefore safe for sale, analysis, and use.[2]

The proliferation of publicly available information online, combined with increasingly powerful computer hardware, has made it possible to re-identify "anonymized" data. This means scrubbed data can now be traced back to the individual user to whom it relates. Scrubbed data is commonly re-identified by combining two or more sets of data to find the same user in both. This combined information often reveals directly identifying information about an individual. Re-identification of anonymized data has grave privacy and policy implications as regulators, businesses, and consumers struggle to define privacy in the modern permanently-recorded age.

II. LEVELS OF IDENTIFIABILITY

Personal data exists on a spectrum of identifiability. Think of a staircase. At the top is data that can directly identify an individual: a name, phone number, or Social Security number. These data are collectively called "direct identifiers."

The second step down is data that can be indirectly, yet unambiguously, linked to an individual. Only a very small amount of data is needed to uniquely identify an individual – 63% of the population can be uniquely identified by the combination of their gender, date of birth, and zip code alone.[3] These data are collectively called "indirect identifiers."

The third step down the staircase is data that can be ambiguously connected to multiple people – physical measurements, restaurant preferences, or individuals' favorite movies. The fourth step down is data that cannot be linked to any specific person – aggregated census data, or broad survey results. Finally, there is data that is not directly related to individuals at all: weather reports and geographic data.

In this way, information that is more difficult to relate to an individual is placed lower on the staircase. However, as data becomes more and more

---

[1] Paul Ohm, *Broken Promises: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1754 (2010).

[2] *Id*. at 1755.

[3] Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the US Population*, 5 ACM WORKSHOP ON PRIVACY ELEC. SOC'Y 77, 78 (2006) (using 2000 census data).

scrubbed of personal information, its usefulness for research and analytics directly decreases. As a result, privacy and utility are on opposite ends of this spectrum – maximum usefulness from the data at the top of the staircase and maximum privacy at the bottom of the staircase. As data gets more and more scrubbed – its usefulness for analysis decreases.

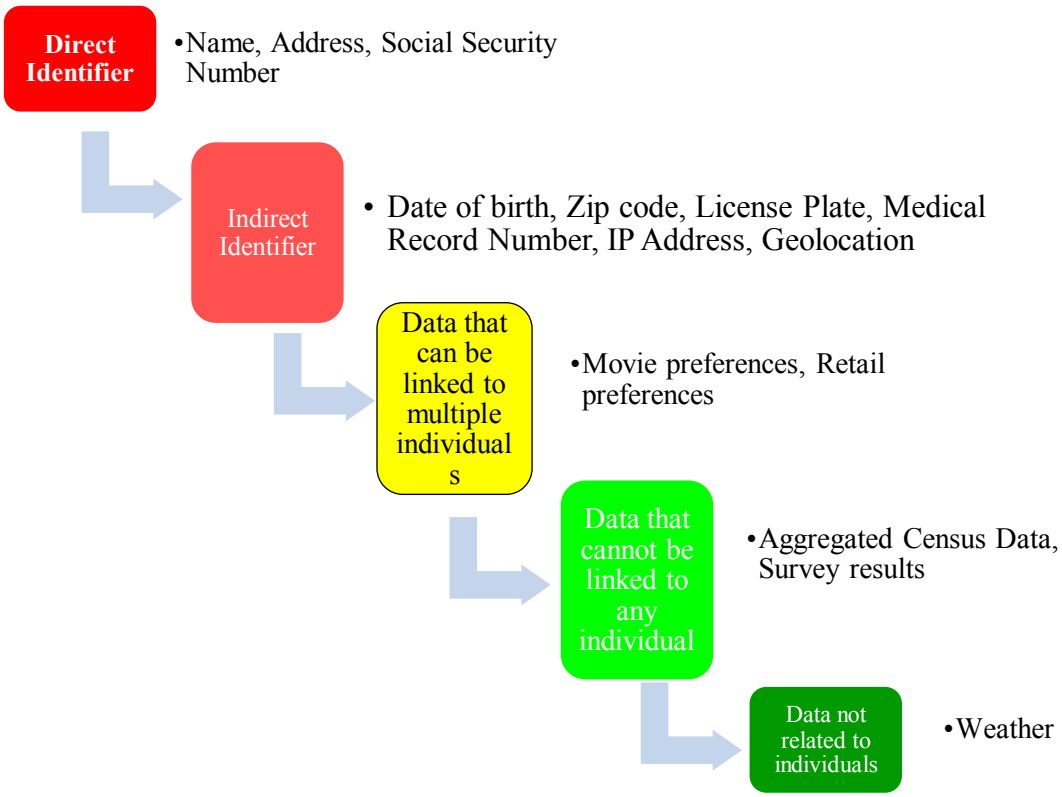


Figure 1. Examples of Personal Information

III. THE FOUR TYPES OF DATA SCRUBBING

The process of scrubbing, or removing, identifying information from data is done by a collection of approaches, tools, and algorithms.[4] There are four main categories of techniques used to scrub data of identifying information – (1) removing data; (2) replacing data with pseudonyms; (3) adding statistical "noise"; and (4) aggregation.

The first two techniques are used mainly for direct identifiers and the latter two are used for indirect identifiers. While direct identifiers can be easily removed or replaced, indirect identifiers can be difficult to remove as they might be important for later analysis or use. For example, a dataset for medical research would be nearly worthless if data scrubbing removed the symptoms or diagnosis.

A. Deletion or Redaction

The first method is to entirely remove or redact any data that directly identifies a person – names, Social Security numbers, etc. This can often be accomplished through automation. In a database with structured data – in a chart that identifies its variable – an entire column of identifying information can be deleted easily and automatically. In the table below, the first column, "Name," can be removed without compromising the usefulness of the data for future research.

Name	**DOB**	**Zip Code**	**Gender**	**Race**	**Diagnosis**
Adam Smith	1/1/1970	20002	M	Caucasian	Congestive Heart Failure
Betty Davis	2/2/1980	20001	F	African American	Pneumonia
Carlos Hernandez	3/3/1990	20007	M	Hispanic	Addison's Disease

Table 1: Sample Structure Database, Raw Data

[4] Simson Garfinkel, *De-Identification of Personal Information*, 8053 NAT'L INST. OF STANDARDS & TECH. INTERNAL REP. 1, 6 (2015), http://dx.doi.org/10.6028/NIST.IR.8053 [https://perma.cc/7X86-FBFG].

However, simply redacting or removing data is not foolproof. For example, medical records contain large amounts of unstructured text such as transcriptions of conversations and hand written notations.[5] Direct identifiers might not be clearly marked, and important medical information may be mistaken for personal information and deleted accidentally.[6] If a data set is released with insufficient de-identification, the missed direct or indirect identifiers can be used to re-identify the individual involved.[7]

B. Pseudonyms

Name	DOB	Zip Code	Gender	Race	Diagnosis
NAME1	1/1/1970	20002	M	Caucasian	Congestive Heart Failure
NAME2	2/2/1980	20001	F	African American	Pneumonia
NAME3	3/3/1990	20007	M	Hispanic	Addison's Disease

Table 2: Structured Database with pseudonym replacing names.

The second approach is a process called pseudonymization replacing data with pseudonyms that are either randomly generated or determined by an algorithm. Pseudonymization preserves the usefulness of the data but replaces the identifying information. This approach shares weaknesses with data deletion – direct identifiers can be difficult to identify and replace, and indirect identifiers are inadvertently left in the dataset.

Pseudonymization comes with its own additional weaknesses. If the pseudonyms are not assigned randomly but by a predetermined algorithm, the data can be re-identified. For example, in 2014 the New York City Taxi and Limousine Commission released a dataset of all taxi trips taken in New York City that year.[8] Before releasing the data the Taxi and Limousine Commission attempted to scrub it of identifying information, specifically they

[5] *Id*. at 30.
[6] *Id*.
[7] *Id*.
[8] Anthony Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset*, NEUSTAR RESEARCH (Sept. 15, 2014), http://research.neustar.biz/author/atockar/ [https://perma.cc/5LZG-YZM8].

pseudonymized the taxi cab medallion numbers and driver's license numbers. Bloggers were, however, able to discover the algorithm used to alter the medallion numbers and then reverse the pseudonymization.[9]

Pseudonyms also cease to be effective if the same unique pseudonym is continually used throughout a dataset, in multiple datasets, or for a long period. Any of these increase the likelihood an individual will by identified by non-direct identifiers associated with that unique pseudonym.[10] Some pseudonymization is meant to be reversible and a "key" is kept to reverse the process. This adds an extra level of security for medical records, for example, but still allows full access to the patient's identifying information. However, as long as a key is retained or the algorithm can be reverse engineered or discovered, pseudonymization can be easily reversed and the data re-identified.

C. Statistical Noise

The third approach to scrubbing datasets of indirect personally identifying information is to introduce statistical "noise." Like pixelating someone's face on TV or in an image, statistical noise allows the viewer to "see" the data, but uses static to obscure the identity of the individuals involved. Static can be introduced in a number of ways such that identifying a specific individual becomes difficult. These include:

- Generalization: Specific values can be reported as a range. For instance, a patient's age can be reported as 70-80 instead of giving a full birthdate.[11]
- Perturbation: Specific values can be randomly adjusted for all patients in a dataset. For example, systematically adding or subtracting the same number of days from when a patient was admitted for care.[12]
- Swapping: Data be exchanged between individual records within a dataset.

As with all scrubbing techniques, the more direct or indirect identifiers are removed, or obscured with static, the less useful the data is for research and analytics.

---

[9] *Id.*; Garfinkel, *supra* note 4, at 17.
[10] Garfinkel, *supra* note 4, at 17.
[11] *Id*. at 20.
[12] *Id*.

D. Aggregation

The fourth scrubbing approach, aggregation, is closely related to statistical noise. Instead of releasing raw data, the dataset is aggregated and only a summary statistic or sub-set is released. For example, a dataset might only provide the total number of patients treated, rather than each patient's individual record. However, if only a small subsample is released, the probability of re-identification increases.[13]

No. Patients	No. Female
3	1

Table 3: Aggregated Patient Data

In an aggregated dataset, an individual's direct or indirect identifiers are withheld from publication. However, the summary data must be based on a broad enough range of data to not lead to the identification of a specific individual. For instance, in the above example, only one female patient visited the hospital. She would be easier to re-identify than if the data included thirty women who had spent time at the hospital.

As with all four scrubbing techniques, the more direct or indirect data that is removed about an individual, the less useful the data becomes.[14] Data utility and individual privacy are on opposite ends of a spectrum. The more the data is scrubbed the less useful it is. The more indirect, or direct, variables that are in a dataset the more useful it is for analysis but at the cost of individual privacy. As a result there is an incentive for data re-identification – the more specific a data set is the more useful it is for research, marketing, and nefarious purposes. If you re-identify "anonymized" data you have much greater information about a specifically identified person while being outside the current regulatory framework of reporting and data security laws.

IV. RE-IDENTIFICATION

Data re-identification occurs when personally identifying information is discoverable in scrubbed or so called "anonymized" data. When a scrubbed data set is re-identified, either direct or indirect identifiers become known and

[13] *Id*.
[14] Ohm, *supra* note 1, at 1754.

the individual can be identified. Direct identifiers reveal the real identity of the person involved, while the indirect identifiers will often provide more information about the person's preferences and habits. Scrubbed data can be re-identified through three methods: insufficient de-identification, pseudonym reversal, or combing datasets. These techniques are not mutually exclusive; all three can be used in tandem to re-identify scrubbed data.

A. Insufficient De-Identification

Insufficient de-identification occurs when a direct or indirect identifier inadvertently remains in a data set that is made available to the public. Both structured and unstructured data are prone to re-identification, as inadvertently leaving direct or indirect identifiers can lead to the discovery of a person's identity. Structured data are those that organize the information into tables with identified values. Tables 1-3 above are structured data, as the column containing the name, date, zip code etc. are clearly identified. Unstructured data is basically everything else—it is usually plain text and can be much more variable. Internet searches, doctors' notes, and voice commands are all unstructured data.

1. Insufficiently De-Identified Structured Data

Insufficiently de-identified structured data can occur when indirect identifiers are left in a data set, either inadvertently or for utility purposes. In the mid-1990's, Massachusetts purchased health insurance for state employees and subsequently released records summarizing every state employee's hospital visits.[15] Then-governor of Massachusetts William Weld, assured the public that the data had been properly scrubbed.[16] The fields containing explicit identifiers such as name, address, and Social Security numbers were removed, however, the record still contained almost a hundred unscrubbed attributes per patient that were unscrubbed.[17] Latanya Sweeney, then a graduate student, obtained the data and used the Governor's zip code, birthday, and gender to identify his medical history, diagnosis, and prescriptions.[18]

---

[15] *Id*. at 1719.
[16] Henry T. Greely, *The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks*, 8 ANN. REV. GENOMICS & HUM. GENETICS 343, 352 (2007).
[17] Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000).
[18] *Id*.

A study showed that 63% of the population can be uniquely identified by the simple combination of their gender, date of birth, and zip code available from census data.[19] As a result of Sweeney's study on re-identification, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA regulates personally identifiable information in medical records.[20] Its "Safe Harbor" provision specifically established that only the first three digits of a zip code could be reported in scrubbed data.[21]

2. Insufficiently De-Identified Unstructured Data

In 2006 AOL released 20 million search queries for 650,000 users, from three months of data.[22] AOL attempted to scrub the data of any direct or indirect identifiers: it deleted direct identifiers such as usernames and IP addresses. To preserve the data's utility, AOL replaced that information with unique identifying numbers through pseudonymization.[23] Because each user had a unique number, each user's search results could be viewed as a group. Soon after the release, two New York Times reporters were able to track down a sixty-two year-old widow in Georgia by analyzing her AOL searches.[24]

B. Pseudonym Reversal

Pseudonyms are only an effective scrubbing mechanism if they cannot be reversed. There are several ways pseudonymization can be defeated. Some pseudonyms are designed to be reversible and a "key" is kept to reverse the process, however, this precludes their security function. Secondly, the longer the same pseudonym is used for a specific individual, the less secure and easier it is to re-identify that individual. Thirdly, if the method used to assign pseudonyms is discovered or becomes know the data can be re-identified.

1. New York City Taxi and Limousine Data

---

[19] Golle, *supra* note 3, at 78.
[20] 45 C.F.R. § 164.514
[21] 45 C.F.R. § 164.514(b)(2) (2013) (stating that the safe harbor also identified seventeen other specific types of data that would have to be removed before the statute would apply).
[22] Ohm, *supra* note 1, at 1717.
[23] *Id*.
[24] *See* Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES (Aug. 9, 2006), http://www.nytimes.com/2006/08/09/technology/09aol.html [https://perma.cc/4297-VE9X].

After the New York Taxi dataset of all taxi rides in 2014 was de-identified by reverse identifying the medallion pseudonym, a data scientist intern at Neustar discovered he could find pictures taken of celebrities entering or leaving taxicabs with the medallion number in the picture.[25] He used indirectly identifying information—medallion number, time, and date—to locate specific rides in the dataset released by the New York City Taxi and Limousine commission. From those 3 indirect identifiers, the intern then used the dataset to identify pick up location, drop of location, amount paid, and even amount tipped.[26]

C. Combining or Linking Datasets

The most powerful tool for re-identifying scrubbed data is combing two datasets that contain the same individual(s) in both sets. Dr. Sweeney was able to re-identify Governor Weld's supposedly "anonymized" set of medical data by linking two databases together. She purchased the voter rolls from Cambridge, where Weld resided, then combined those rolls with the hospital data. Six people in Cambridge shared Weld's birthday, of those, half were men and only one lived in Weld's zip code.[27] In this way she circumvented the scrubbing procedures and re-identified the "anonymized" data.

When two or more anonymized datasets are linked together, they can then be used to unlock other anonymized datasets. Once one piece of data is linked to a person's real identity, that data can then be used to destroy the anonymity of any virtual identity with which that data is associated. The ability to link even supposedly innocuous data exposes people to potential harm because of this.[28]

1. Netflix Prize Data

In 2006, Netflix publicly released one-hundred million records revealing hundreds of thousands of user ratings from 1999 through 2005 and offered a million dollar prize for the first team to significantly improve Netflix's movie recommendation algorithm. [29] Although the data contained no direct

[25] Tockar, *supra* note 9.
[26] *Id*.
[27] Sweeney, *supra* note 18.
[28] Ohm, *supra* note 1, at 1746.
[29] *Id*. at 1720; *The Netflix Prize Rules*, NETFLIX, http://www.netflixprize.com/rules (last visited June 12, 2010) [https://perma.cc/RA6L-LB8B].

identifiers, within weeks of the data's release, two researchers were able to re-identify a subset of specific people by cross-referencing the Netflix data with IMDB.com ratings. Using just six ratings of obscure movies, the researchers re-identified individuals 84% of the time (if they were in both datasets).[30] Including an approximate time of the rating was made allowed identification 99% of the time. Although this only worked to re-identify Netflix users that also had IMDB accounts, the Netflix information could be cross-referenced with social media movie preference found on online dating apps and Facebook for similar results.[31]

V. CONCLUSION

The current regulatory framework is predicated on the supposition that data that has been scrubbed of direct identifiers is "anonymized" and can be readily sold and disseminated without regulation because, in theory, it cannot be traced back to the individual involved. However, today's techniques of re-identification effectively nullify scrubbing and compromise privacy. The examples of Governor Weld, Netflix, AOL, and NYC taxi illustrate how any data scrubbed of direct personal identifiers can still be readily re-identified if it is combined with another set that also contains data about the same individuals.

Once a dataset is released to the public it can never be strengthened, only 'weakened' by future information that may be released that could lead to that information being re-identified.[32] Re-identification can also be achieved by anyone from government entities, to data brokers, to blackmailers, and is nearly impossible to trace. Once a comprehensive database of previously "anonymized" data is created, it can readily be de-identified. One data broker, InfoUSA, alone claims to have data on 235 million US consumers and uses 29 billion records from over 100 sources to update its database of raw data every year.[33]

The re-identification of anonymized data presents serious policy and privacy implications. For example, this information can be used to bypass password recovery mechanisms for email and bank accounts. Consider that Sarah Palin's email was famously hacked in 2008 when someone guessed her

---

[30] Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, PROC. 2008 IEEE SYMP. ON SEC. & PRIVACY 111, 121 (2008).
[31] *Id*.
[32] Ohm, *supra* note 1, at 1717.
[33] *Data Quality*, INFOUSA, https://www.infousa.com/data-quality/ (last visited Mar. 29, 2017) [https://perma.cc/ZRZ7-CXT8].

password recovery question that she met her husband at "Wasilla high."[34] Re-identification of scrubbed data can lead to the publication of sensitive or embarrassing information from a person's past that they may not want their employer, spouse, or community to discover. Medical history, sexual preferences and proclivities, reproductive choices, or even details of one's conception can be discovered. Today, that sensitive or embarrassing piece of information more than likely resides on an "anonymized" dataset up for sale. Without regulation of re-identified anonymized data, employers, neighbors, and blackmailers have an unprecedented window into an individual's most private information.

Consider the smartphone. You can unlock it with facial recognition; give it a command or ask it directions; make a credit card payment; and confirm it by swiping your fingerprint. Every one of those interactions is a recorded data point about that individual user: facial print, voice print, finger print, credit card information, and geolocation – on one device. All that information is stored; sent to third parties; reviewed and analyzed; and, after a brief scrubbing, sold on the commercial market.

There is no comprehensive data privacy law in America – it is regulated on an ad-hoc, sector-by-sector basis. None of this patchwork of laws and regulations covers "anonymized" data. There is no duty to report if data has been re-identified. There is no private cause of action for an individual seeking redress for re-identified data, and no external way to verify if a private entity has privately de-identified "anonymized" data exists. The theory that data scrubbed of personally identifying information cannot be re-identified has time and again been shown to no longer hold true. Our current ad-hoc approach is antiquated and inadequate for addressing the new technological challenges re-identified data presents.

[34] *See* Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED (July 18, 2008, 10:05 AM), https://www.wired.com/2008/09/palin-e-mail-ha/ [https://perma.cc/HH54-QVWJ].

Clear Channel Outdoor

EXHIBIT G

Back to Case Studies

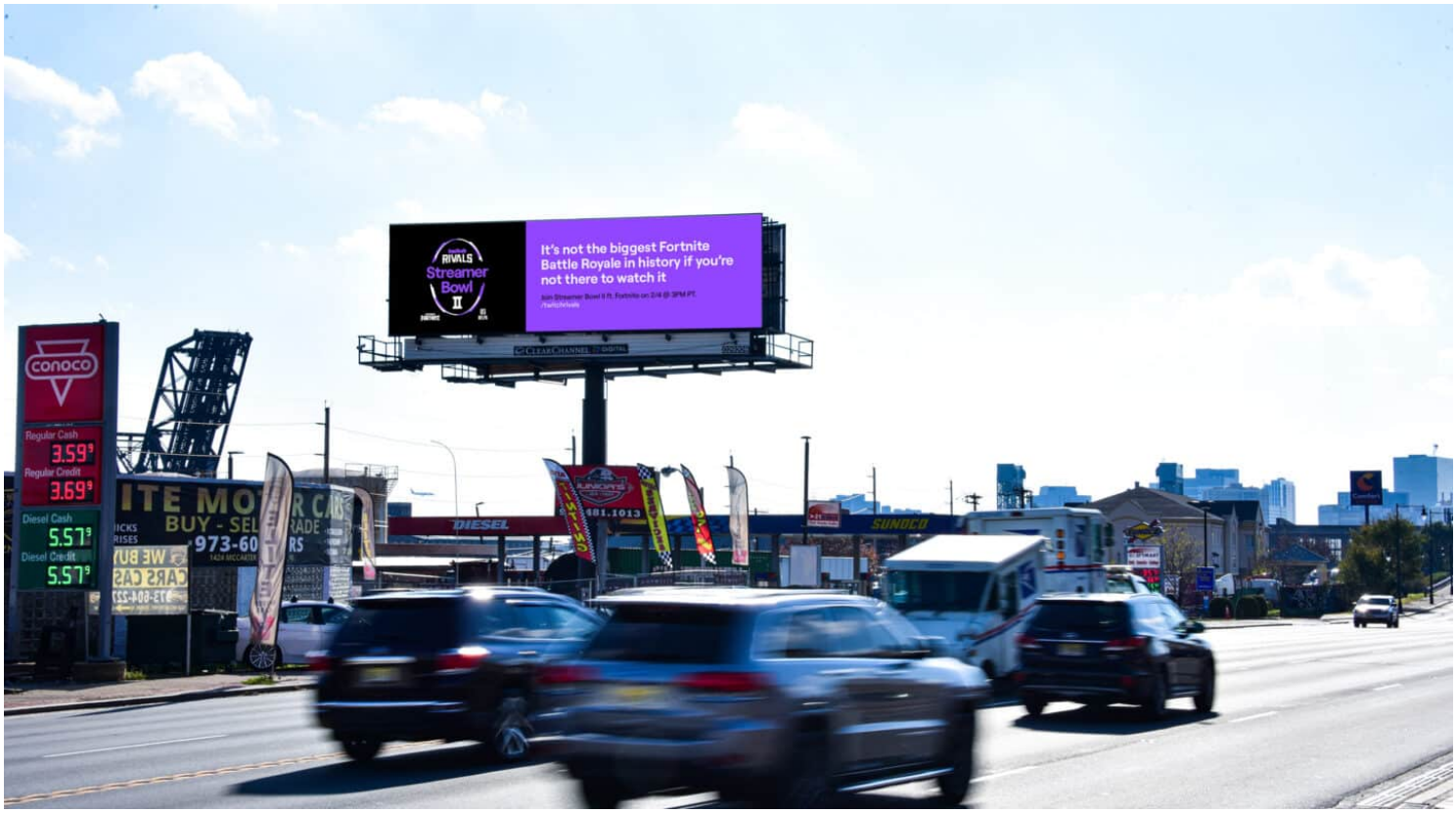
RADARSync (BETA)

Brand Awareness & Online Engagement

Digital billboards drive online engagement for Twitch

Download Case Study

- 245% lift in monthly video views
- 90% incremental lift in monthly active users
- 168% increase in hours watched



Objective

Twitch was mounting its second annual Streamer Bowl tournament and wanted to drive gamers to the platform to watch the event.

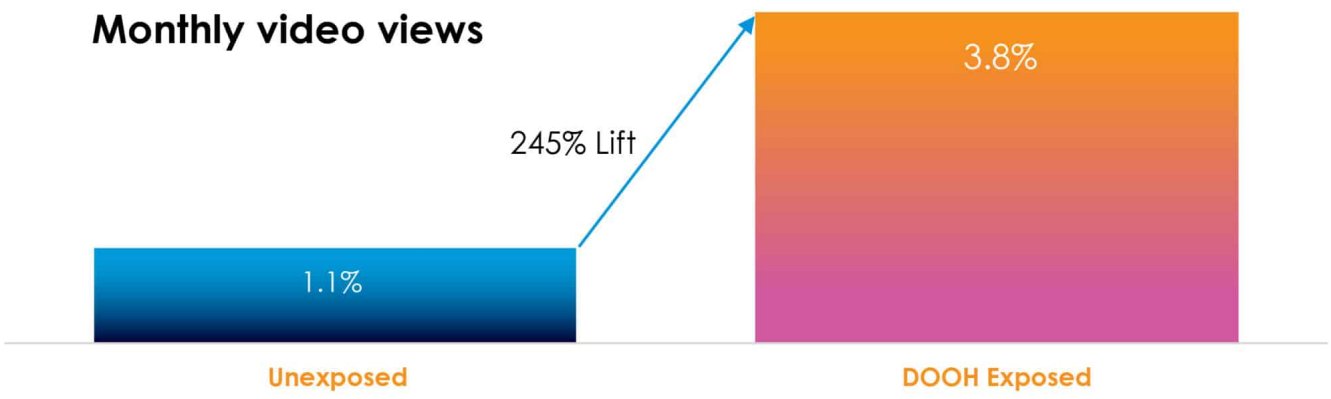
Solution

In order to reach gamers in the real world, the brand partnered with Clear Channel Outdoor (CCO), leveraging billboards in cities whose NFL stars were participating in the Streamer Bowl tournament. CCO then activated a campaign with hand-selected digital out-of-home (DOOH) units through direct buying, and an efficient programmatic overlay. The combination offered scale and reached football fans and gamers that were matched to their Twitch IDs via CCO RADARSync.

Results

The highly targeted combination of direct and programmatic buying for the DOOH campaign delivered significant lifts in monthly video views, monthly active users, and hours watched for Twitch's Streamer Bowl event.

In addition, the campaign was recognized for "Best Use of Programmatic" by Adweek and won a MediaPost Online Media Marketing & Advertising (OMMA) Award.



245% lift in video views

The targeted campaign yielded a big time pay-off. Twitch users exposed to the outdoor ads were more likely to tune-in, resulting in a 245% lift in video views from those who saw the billboard campaign.

90% incremental lift in active users

Utilizing DOOH ads secured through a mix of programmatic and direct buying, and leveraging RADARSync to find the exact gamers they wanted to target, the brand experienced a 90% *incremental lift* in monthly active users on the platform among DOOH-exposed accounts

Incrementality helps us understand the extent to which advertising changes consumer behavior and drives new online actions. More than showing a campaign's effectiveness in driving users to a platform, incrementality reveals whether the campaign drove *new or additional* users to a platform.

168% increase in hours watched

As a result of the combined direct and programmatic DOOH campaign, the brand also saw an increase in time spent on the platform. There was a 168% increase in hours spent among those audiences who were exposed to the billboard campaign.

Source: CCO RADARSync; Twitch, February, 2021

How can we help you?

We invite you to find out exactly what it means to GET MORE WITH US. Reach out for expert help and smart, customized solutions. We're here to talk options, plan your campaign, or simply answer questions. Just fill out the form. We'll be in touch quickly.

First Name *

First Name

Last Name *

Last Name

Company Name *

Company

Job Title *

Job Title

Zip Or Postal Code *

Zip Or Postal Code

Phone Number *

Phone Number

Email *

Email

Message *

How can we help with your outdoor advertising needs?

I would like to receive Clear Channel Outdoor newsletters and updates

By submitting your information, you acknowledge our Privacy Statement and agree to our Terms of Use.

protected by reCAPTCHA
Privacy - Terms

Submit

Connect with your audience. Drive measurable results. Get more with Clear Channel Outdoor.

Contact Us

About Us

Solutions

Investors

Clear Channel Outdoor

EXHIBIT H

Back to Case Studies

RADARProof®

Audience Targeting, Brand Awareness, Doctor Visits & Script Lift

Driving innovation for Pharma

Download Case Study

- Integrated Pharma brand's target audiences for OOH planning
- Raised consideration intent by 50%
- Increased doctor visits by 20%
- Increased new prescriptions for the category by 75%
- Delivered a 76% lift in sales of the advertised brand

Objective

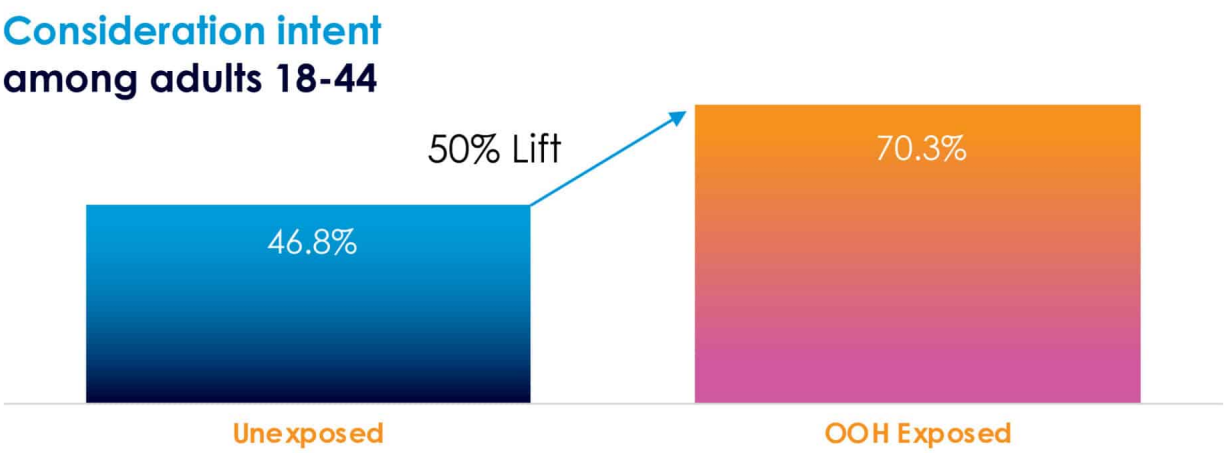
A pharmaceutical company sought to build awareness and increase sales of a brand used to treat a specific, moderate-to-severe medical condition.

Solution

Clear Channel Outdoor (CCO) leveraged our proprietary CCO RADAR suite of data-driven solutions, and our best-in-class data partners, Veeva Crossix and LiveRamp, to onboard the brand's target audience into our RADARView platform for campaign planning. We further amplified the OOH campaign with a mobile retargeting campaign through RADARConnect. And finally, with RADARProof, we were able to measure brand awareness, doctor visits, and number of prescriptions issued.

Results

The OOH campaign successfully drove brand awareness and further retargeting through mobile, increased visitations to a specialist, and also drove lift in prescriptions for the overall category and for the advertised drug.

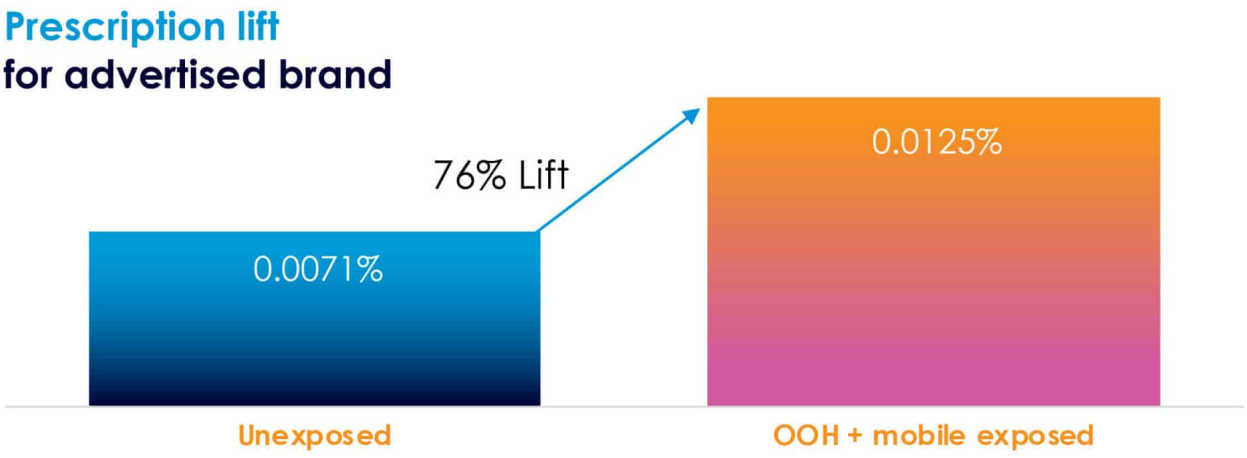


OOH drove 50% lift in consideration intent

CCO RADARProof is our campaign measurement and attribution solution that allows us to observe consumer devices exposed to an OOH campaign. In this pharma study, we learned that the campaign effectively reached the target audience and influenced their intention to consider the product. Among those exposed to the OOH campaign, consideration intent was lifted by 50%.

Visits to specialty doctors rose 20%

The data we extract from CCO RADAR products underscore the effectiveness of a combined OOH + mobile campaign to drive additional engagement. This OOH + mobile campaign drove up visits to specialist by 20% among exposed audiences.



OOH + mobile lifted conversions and drove up incremental sales

In addition, the data showed that audiences exposed to the OOH + mobile campaign helped to lift brand conversions by 76%, and pushed incremental sales up to 75%, in new patient prescriptions for the category.

Source: CCO RADAR; Kantar; Veeva Crossix, January, 2022

How can we help you?

We invite you to find out exactly what it means to GET MORE WITH US. Reach for expert help and smart, customized solutions. We're here to talk options, plan your campaign, or simply answer questions. Just fill out the form. We'll be in touch quickly.

First Name *

First Name

Last Name *

Last Name

Company Name *

Company

Job Title *

Job Title

Zip Or Postal Code *

Zip Or Postal Code

Phone Number *

Phone Number

Email *

Email

Message *

How can we help with your outdoor advertising needs?

I would like to receive Clear Channel Outdoor newsletters and updates

By submitting your information, you acknowledge our Privacy Statement and agree to our Terms of Use.

Submit

Connect with your audience. Drive measurable results. Get more with Clear Channel Outdoor.

Contact Us

About Us

Solutions

Investors

EXHIBIT I

"No Tech for ICE": Data Broker LexisNexis Sued for Helping ICE Target Immigrant Communities

RELATED

Topics

Guests

Links

Transcript

A coalition of immigrant rights organizations have sued the data broker LexisNexis for collecting detailed personal information on millions of people and then selling it to governmental entities, including Immigration and Customs Enforcement. The lawsuit alleges LexisNexis has helped create "a massive surveillance state with files on almost every adult U.S. consumer," and accuses ICE of using information collected by LexisNexis to circumvent local policies in sanctuary cities. We speak with Cinthya Rodriguez, organizer with the immigrant justice group Mijente, who explains how "one of the biggest data brokers in the world" is "getting rich off of the backs of community members," particularly among immigrant communities of color and activists.

Transcript

This is a rush transcript. Copy may not be in its final form.

AMY GOODMAN: This is *Democracy Now!* I'm Amy Goodman.

A coalition of immigrant justice groups have sued the data broker LexisNexis for collecting detailed personal information on millions of people, then selling it to governmental entities, including ICE — that's Immigration and Customs Enforcement. The lawsuit alleges LexisNexis has created a massive surveillance state with files on almost every adult U.S. consumer, and describes how law enforcement officers can surveil and track people based on information these officers would not, in many cases, otherwise be able to obtain without a subpoena, court order or other legal process. The groups also accuse ICE of using information collected by LexisNexis to circumvent local policies in sanctuary cities. The plaintiffs in the lawsuit include Organized Communities Against Deportations, Just Futures Law and Mijente.

And for more, we are joined by Cinthya Rodriguez, the national organizer with Mijente. She's joining us from Chicago.

Can you lay out this lawsuit and the significance of filing it where you are, in the state of Illinois, Cinthya?

CINTHYA RODRIGUEZ: Thank you so much, Amy. And thank you so much for having us.

So, Mijente joins this lawsuit filed by Just Futures Law, by Legal Action Chicago, alongside our friends at OCAD and the Illinois Coalition for Immigrant and Refugee Rights, because, as you shared, LexisNexis is collecting and selling the data of more than 276 million people across the country, particularly using their Accurint product. And here in Illinois, we want to bring light to how this violates privacy and consumer rights, how it's at odds with Illinois consumer protection and common law, because what we're really talking about is one of the biggest data brokers in the world, LexisNexis, and how they're getting rich off of the backs of community members by aggregating and selling our personal information, that can then lead to detention and deportations.

And I want to share that here in Cook County, Illinois, we are talking about various organizing and legal efforts that are happening to put a data broker like LexisNexis on notice. This lawsuit also follows an important hearing last month. Last month, the Cook County commissioners, spearheaded by Commissioner Alma Anaya, held the first hearing of its kind that we know of in the country that was investigating the local repercussions of this LexisNexis contract that we’re talking about, of this $22.1 million contract. So, investigating the local impacts of this contract, of ICE contracts with other data brokers, is really important. And so, during this hearing last month, the county had an opportunity to hear public testimony, witnesses — expert witnesses — that spoke about digital loopholes for sanctuary cities —

AMY GOODMAN: I wanted to go —

CINTHYA RODRIGUEZ: — and from the agency.

AMY GOODMAN: — Cinthya, to the Cook County meeting you were talking about, the recent hearing on the repercussions of ICE contracting third-party data brokers like LexisNexis, the Cook County Board of Commissioners hearing from immigrant justice advocates and community members, like Michelle Garcia, a member of the Illinois Coalition of Immigrant and Refugee Rights and Access Living. She said she used LexisNexis to search her own records and found dozens of pages of personal information on herself, family members, even other people who lived in her same apartment complex. This is what she said.

> **MICHELLE GARCIA:** LexisNexis collected 43 pages of information about me, my family and my acquaintances. It was extremely disturbing, scary and overwhelming to see everything in writing that they have collected about my life as a Cook County resident. … This information being in the hands of a third party like LexisNexis, and then potentially in the hands

> of ICE, puts my loved ones and other community members at risk. I have the privilege of citizenship. But if I were one of millions of undocumented people living in the U.S., ICE could find me within a matter of hours by searching through a report like mine. ICE is still free, has free rein to go after anyone they believe is deportable.

AMY GOODMAN: So, that's Michelle Garcia, member of the Illinois Coalition. How does LexisNexis get this information? And, of course, it goes way beyond the immigrant community in the United States, when you're talking about 250 million people. What are LexisNexis products? What are people using that tracks them?

CINTHYA RODRIGUEZ: That's right. I think one way that you can think about LexisNexis is a one-stop shop. They're a one-stop shop for data points like addresses, phone numbers, license plate information, your social media information, but also things like medical history, credit scores. Michelle also spoke during the press conference about having information on her neighbors, right? The list can go on and on. And so, we want to be clear that here we're talking about mass surveillance. Tabs are being kept, as you're sharing, on immigrant communities, communities of color, on protesters. And at the end of the day, this is affecting us all, because this is happening without consent. It's happening without people knowing, without a warrant or a subpoena or a court order.

And I also want to share that this is all really informed by research, right? We saw a Freedom of Information Act request earlier this year that revealed how, nationally, ICE agents ran over 1.2 million searches in the LexisNexis database over a seven-month period. And it's really important to understand that these searches are happening through ERO, Enforcement and Removal Operations, which is the division of ICE that focuses on arrests. And as we've shared, I live here in Cook County, in the Chicagoland area, where

the local Chicago field office ran — just themselves, ran over 13,000 of these searches.

AMY GOODMAN: "No Tech for ICE" immigrant justice advocates first exposed the multimillion-dollar contract between LexisNexis and ICE in Colorado through a FOIA that revealed the corporation was giving ICE access to real-time jail booking data from sheriff's offices in the state of Colorado. Explain the significance of this and why it puts so many people in danger.

CINTHYA RODRIGUEZ: Definitely. So, before Cook County held this hearing, Colorado was the first place where we're seeing that it was named publicly by community, that ICE is circumventing local sanctuary protections by contracting with data brokers such as LexisNexis. So, folks from the Colorado Immigrant Rights Coalition and other organizations in Colorado, and Mijente joined these groups, to expose an ICE contract from July 2021 that confirmed what we had been seeing and hearing, right? And so, this was breaking news, because in this contract language, it is explicitly stated that ICE is contracting with data brokers like LexisNexis to go around sanctuary protections. And this is happening through LexisNexis's aggregation of public and commercial data and also, as you mentioned, real-time jail data.

For many years — right? — people have fought really hard and organized for sanctuary and welcoming protections, these policies that prohibit, or seek to prohibit, information sharing and cooperation between law enforcement and ICE. But now we have this $22.1 million contract with LexisNexis that is providing back-door access to people's information and going against the spirit of sanctuary protections. So, Colorado was the first place to speak up about this —

AMY GOODMAN: We have five seconds.

CINTHYA RODRIGUEZ: — followed by Cook County. And we know that local organizing is going to continue to close these digital loopholes that make it easier for ICE to detain and deport our people.

AMY GOODMAN: And we will continue to follow this, Cinthya Rodriguez, national organizer with Mijente, working on the group’s No Tech for ICE campaign.

That does it for our show. *Democracy Now!* currently accepting applications for a people and culture manager. Learn more and apply at democracynow.org. I’m Amy Goodman. Thanks so much for joining us.

EXHIBIT J

ELECTRONIC FRONTIER FOUNDATION

Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police

This article is part of EFF's investigation of location data brokers and Fog Data Science. Be sure to check out our issue page on Location Data Brokers.

A data broker has been selling raw location data about individual people to federal, state, and local law enforcement agencies, EFF has learned. This personal data isn't gathered from cell phone towers or tech giants like Google — it's obtained by the broker via thousands of different apps on Android and iOS app stores as part of the larger location data marketplace.

The company, Fog Data Science, has claimed in marketing materials that it has "billions" of data points about "over 250 million" devices and that its data can be used to learn about where its subjects work, live, and associate. Fog sells access to this data via a web application, called Fog Reveal, that lets customers point and click to access detailed histories of regular people's lives. This panoptic surveillance apparatus is offered to state highway patrols, local police departments, and county sheriffs across the country for less than $10,000 per year.

The records received by EFF indicate that Fog has past or ongoing contractual relationships with at least 18 local, state, and federal law enforcement clients; several other agencies took advantage of free trials of Fog's service. EFF learned about Fog after filing more than 100 public records requests over several months for documents pertaining to government relationships with location data brokers. EFF also shared these records with The Associated Press.

Troublingly, those records show that Fog and some law enforcement did not believe Fog's surveillance implicated people's Fourth Amendment rights and required authorities to get a warrant.

In this post, we use public records to describe how Fog's service works, where its data comes from, who is behind the company, and why the service threatens people's privacy and safety. In a subsequent post, we will dive deeper into how it is used by law enforcement around the country and explore the legal issues with its business model.

How does the service work?

In materials provided to law enforcement, Fog states that it has access to a "near real-time" database of billions of geolocation signals derived from smartphones. It sells subscriptions to a service, which the company usually billed as "Fog Reveal," that lets law enforcement look up location data in its database through a website. The smartphone signals in Fog's database include latitude, longitude, timestamp, and a device ID. The company can access historical data reaching back to at least June 2017.

Fog's materials describe how users can run two different queries:

1. "Area searches": This feature allows law enforcement to draw one or more shapes on a map and specify a time range they would like to search. The service will show a list of all cell-phone location signals (including location, time, and device ID) within the specified area(s) during that time. The records EFF obtained do not say how large an area Fog's Area searches are capable of covering with a single query.
2. "Device searches": Law enforcement can specify one or more devices they've identified and a time range, and Fog Reveal will return a list of location signals associated with each device. Fog's materials describe this capability as providing a person's "pattern of life," which allows authorities to identify "bed downs," presumably meaning where people sleep, and "other locations of interest." In other words, Fog's service allows police to track people's movements over long periods of time.

Fog Reveal is typically licensed for a year at a time, and records show that over time the company has charged police agencies between $6,000 - $9,000 a year. That basic service tier typically includes 100 queries per month, though Fog sells additional monthly query allocations for an additional fee. For example, in 2019, the California Highway Patrol paid $7,500 for a year of access to Reveal plus $2,400 for 500 more queries per month.

Fog states that it does not collect personally identifying information (for example, names or email addresses). But Fog allows police to track the location of a device over long stretches of time — several months with a single query — and Fog touts the use of its service for "pattern of life" analyses that reveal where the device owner sleeps, works, studies, worships, and associates. This can tie an "anonymous" device to a specific, named individual.

Together, the "area search" and the "device search" functions allow surveillance that is both broad and specific. An area search can be used to gather device IDs for everyone in an area, and device searches can be used to learn where those people live and work. As a result, using Fog Reveal, police can execute searches that are functionally equivalent to the geofence warrants that are commonly served to Google.

This service could be used to determine who was near the scene of a violent crime around the time it was committed. It also could be used to search for visitors to a Planned Parenthood or an immigration law office on a specific day or everyone who attended a protest against police violence.

Image from Fog's marketing brochure, sent to North Dakota and Chino, CA, which appears to show a single location signal as viewed with Fog's service.

The basics of Fog's services are laid out in a marketing brochure which was sent to several prospective customers. The brochure explains that Fog's "unique, proprietary and patented data platform" processes data from "hundreds of millions of mobile devices" and can deliver "both forensic and predictive analytics and near real-time insights on the daily movements of the people identified with those mobile devices[.]" The materials state that Fog's collection of people's location data is "100% Opt-in. All users opt-in to location data collection," though as we will discuss later, this claim is hard to take at face value.

At the core of Fog's pitch is a series of claims about the breadth and depth of its location data. It claims to process over 250 million devices per month within the United States. (There are an estimated 301 million mobile devices nationally). According to Fog, these devices generate 15 billion signals per day, or over 5 trillion per year.

Fog Data Science's proprietary platform has been architected with massive scale in mind and provides predictive analytics and near real-time insights on how people go about their daily lives. Currently, the platform processes:

- 250 million devices each month
- 15 billion location signals each day
- 10 million fenced points of interest
- 1+ million daily events
- US and International Data

Excerpt from Fog's marketing brochure describing the properties of its dataset

EFF could not verify Fog's claims. But there is reason to be skeptical: Thanks to the nature of its data sources, it's likely that Fog can only access location data from users while they have apps open, or from a subset of users who have granted background location access to certain third-party apps. Public records indicate that some devices average several hundred pings per day in the dataset, while others are seen just a few times a day. Users who do not install many third-party apps, or who have opted out of tracking via Apple's App Tracking Transparency (ATT), may not be present in the dataset at all.

Additionally, the records EFF reviewed show that several of the agencies that worked with Fog have since canceled their subscriptions, and at least one said they were not sure if they ever used Fog to successfully solve a case. Those potential shortcomings are not a reason to underestimate Fog's invasiveness or its capability for unfettered dragnet monitoring. But it's important to understand its limits. Fog's data may be patchy and incomplete, with data about some people some of the time. But if we take Fog's claims at face value, it would mean that the company collects the location data of a majority of people in the United States on a monthly basis. This means Fog may have limits in its ability to locate any given person at a specific moment in time. But Fog's service may still be capable of identifying a significant portion of the hundreds of attendees at a protest or other sensitive location.

Example of "Pattern of Life Analysis"

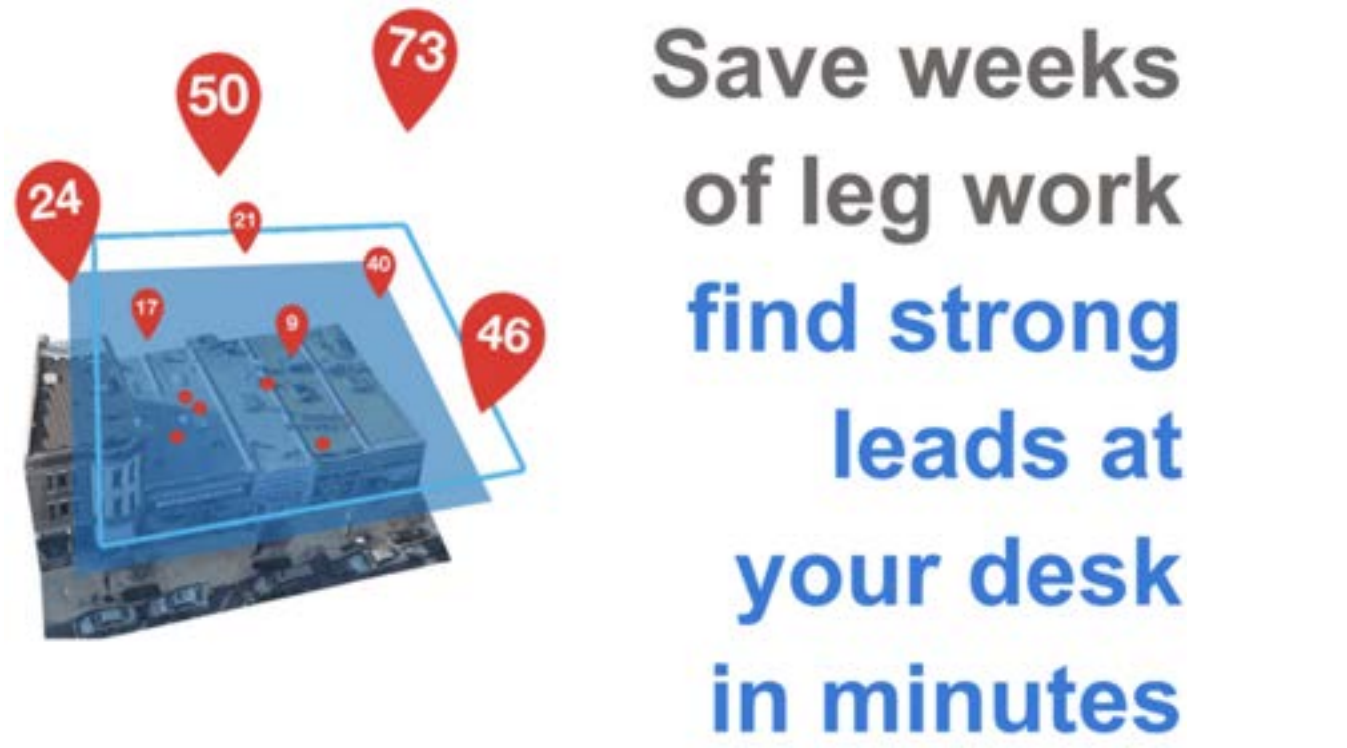
The brochure gives some insight into how Fog intends for its service to be used. It lists a series of "use cases" from the dramatic ("Human Trafficking," "Terrorism Investigations," "Counter-Intelligence") to the more mundane ("Drug Investigations," "Soft Target Protection"). It seems to be aimed at both local law enforcement and at intelligence/homeland security agencies.

The language used in the document often invokes terms used by intelligence agencies. For example, a core advertised feature is the ability to run a "pattern of life analysis," which is what intelligence analysts call a profile of an individual's habits based on long-term behavioral data. Fog Reveal is also "ideal for tipping and cueing," which means using low-resolution, dragnet surveillance to decide where to perform more targeted, high-resolution monitoring. The brochure also includes a screenshot of Fog Reveal being used to monitor "a location at the US/Mexico border," and an alternate version of the brochure listed "Border Security/Tracking" as a possible use case. As we will discuss in our next post, records show that Fog has worked with multiple DHS-affiliated fusion centers, where local and federal law enforcement agencies share resources and data.

In other materials, Fog emphasizes the convenience of its service. An email titled "Solve crimes faster: Here's how" reads:

> Find strong leads at your desk in minutes. Just type in a location, date and time, then watch app signals disclose what mobile devices were present at the crime scene. We'd love to help your department save time and money too. Let's schedule a 10-minute demo next week.

Fog's Reveal customers are given direct access to raw location data, which can be exported from the web portal into portable formats for processing elsewhere. Fog emphasizes that its license permits "processing, analysis, and sub-licensing of location data," potentially allowing law enforcement to share the data with private contractors. Fog routinely encouraged law enforcement agencies to share one license among multiple users, and some customers used Fog to run queries on behalf of other law enforcement agencies on request.



Fog claims that it only sells its Reveal service to law enforcement agencies. But Fog's materials also advertise "out-sourced analytic services" for non law enforcement customers, including "private sector security clients." An email exchange between Fog and Iowa police appears to corroborate this policy: Fog says it will not grant private companies direct access to its database, but it will perform analysis on behalf of "law firms and investigative firms." According to a brochure, this analysis may include:

- Verifiable presence at a location on a specific date and time
- Likely locations for residences, places of business and frequent activities
- Links to other individuals, places and devices
- Patterns of activity correlating to certain events, times or alibis

In other words, Fog advertises that it can use its data to surveil the private lives of individuals on behalf of private companies. The records EFF has obtained do not provide any details about specific relationships Fog has with any private-sector clients.

Where does the data come from?

The kind of data that Fog sells to law enforcement originates from third-party apps on smartphones. Apps that have permission to collect a user's location can share that data with third-party advertisers or data brokers in exchange for extra ad revenue or direct payouts. Downstream, data brokers collect data from many different apps, then link the different data streams to individual devices using advertising identifiers. Data brokers often sell to other data brokers, obfuscating the sources of their data and the terms on which it was collected. Eventually, huge quantities of data can end up in the hands of actors with the power of state violence: police, intelligence agencies, and the military.

Over the past few years, journalists have uncovered several links between private brokers of app-derived location data and the US government. Babel Street, best known for its open-source intelligence (OSINT) tools for analyzing social media and the like, sells location data as part of a secret add-on service called "Locate X." Venntel, a subsidiary of marketing data company Gravy Analytics, has sold raw location data to several different US agencies, including ICE, Customs and Border Protection (CBP), and the FBI. And broker X-Mode paid app developers around 3 cents per user per month for access to location data, then sold it directly to defense contractors.

Enter Fog Data Science. Like the other companies, Fog buys data from the private market and packages it for use by law enforcement. Unlike most others, Fog seems to target smaller agencies. Venntel has sold a year's worth of data to the Department of Homeland Security for more than $650,000; meanwhile, Fog sold its service to the sheriff of Washington County, OH, for $9,000 a year. While Venntel, Babel Street, and Anomaly 6 have made headlines for dealings with three-letter federal agencies, public records show that Fog appears to have targeted its business at local, regional, and state law enforcement. That is, Fog sells its services to police agencies that most Americans are far more likely to interact with than federal law enforcement. The records received by EFF confirm past or ongoing contractual relationships with at least 18 state and local law enforcement clients; several other agencies took advantage of free trials of Fog's service. Notes from one agency's meeting with Fog state that the company works with "50-60" agencies nationwide.

So where, exactly, does Fog's data come from? The short answer is that we don't know for sure. Several records explain that Fog's data is sourced from apps on smart phones and tied to mobile advertising identifiers, and one agency relayed that Fog gathers data from "over 700 apps." Fog officials have referred to a single "data provider" in emails and messages within Fog Reveal. One such message

explained that the data provider "works with multiple sources to ensure adequate worldwide coverage," and that a "newly added source" was causing technical issues.

But when asked about which apps or companies originate its data, Fog has demurred. Some answers implied that Fog itself might not know. In July 2020, Mark Massop responded to a point-blank question from the Chino police that "Our data provider protects the sources of data that they purchase from." Massop did say that at least two sources were *not* included in Fog's dataset: Twitter and Facebook. Separately, a Santa Clara County attorney wrote that Fog gets information from "lots of smaller apps," but not Google or Facebook.

Another document, shared in 2019 with the city of Anaheim, CA, says that Fog's portal uses "unstructured geo-spatial data emanating from open apps (Starbucks, Waze, etc.)" It's unclear whether this means that Fog actually receives data from the apps listed, or whether Starbucks and Waze are simply examples of "open apps" that could be sharing data. On Android, both Starbucks and Waze (which is owned by Google) have access to location permissions, and both apps use third-party advertising or analytics services. Waze was also mentioned in a presentation about Fog's capabilities to the Greensboro, NC police, according to Davin Hall, a former data analyst for the department interviewed by EFF. Per Hall, "Waze got brought up a lot" in the context of apps that could share data with Fog. "It got mentioned because it was a common one for people to have up while they were driving around, so it would be pinging regularly so that you could see the movement of the device actively," he said.

The document further claims that Fog's competitors all buy their data from a single source, and that Fog has a unique and privileged relationship as an "associate" of that source.

> [The use of app-based location data] for Law Enforcement and Intelligence Analysis purposes is limited to only a few carriers. Currently, these carriers purchase their source of data from an associate company of FOG Data Science. As non-associates, they are charged a much higher premium to purchase the data, thereby forcing higher prices for their products. [...]
>
> Additionally, [FOG's] direct access to, and association with, the database vendor allows it to offer low prices both per seat license and per additional query.

This implies that Fog's data provider was, to its knowledge, the sole upstream source of app-based location data for all law enforcement and intelligence clients.

Links to Venntel

Other documents suggest that the "associate company" referenced in the Anaheim document — and the source of Fog's data — is Venntel, perhaps the largest seller of location data to the government.

The most direct link comes from an email exchange with the Iowa Department of Public Safety. In response to an Iowa intelligence analyst's question about Fog's data, a Fog representative said it would ask "our data partner" for assistance. Fog then forwarded the question (including a device identifier) to a representative of Venntel, who sent back a series of screenshots illustrating how the analyst should interpret the data.

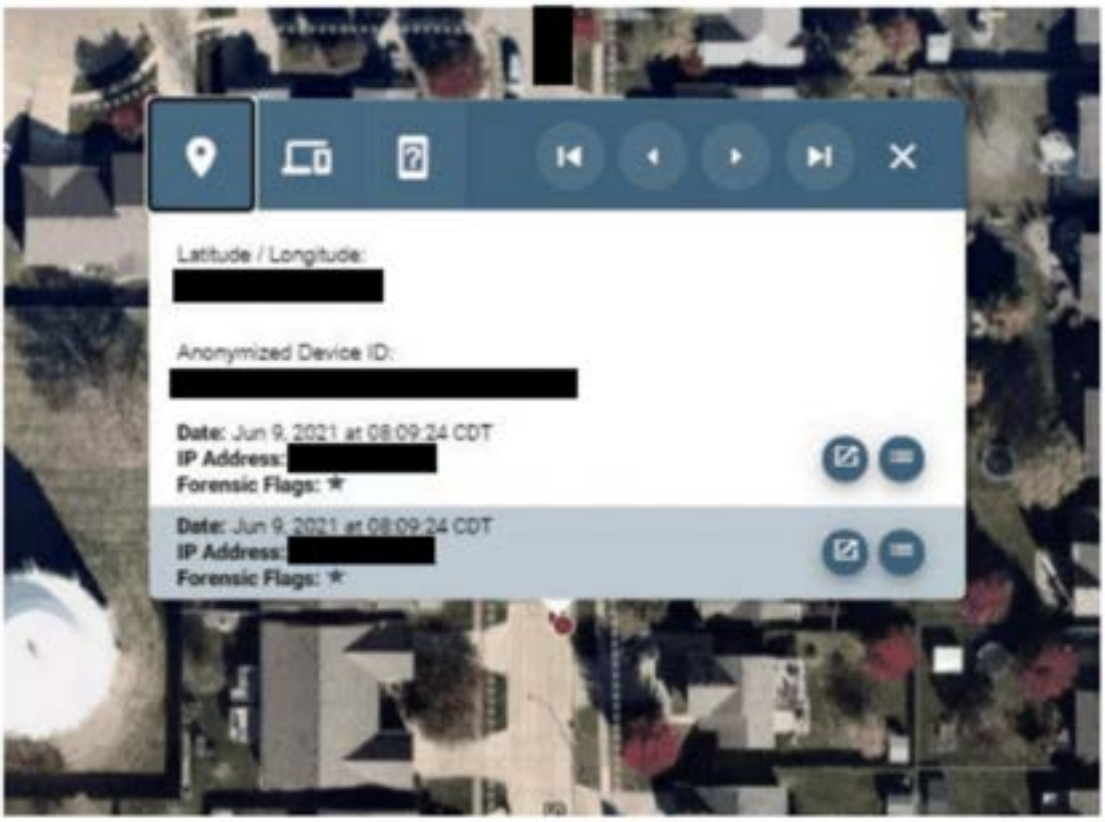
There are other links between Fog and Venntel.

The marketing materials provided by Fog to multiple law enforcement agencies are nearly identical to material that Venntel provided to DHS, according to records obtained by ACLU. The style, much of the language, and several of the graphics appear to be identical. It even appears that both companies use the same screenshot of a location in Santa Teresa, NM to illustrate their capabilities. Furthermore, both companies make identical claims about their data coverage, including that they analyze "location signals from 250 million mobile devices in the U.S." and "15+ billion daily location signals." These claims could be evidence that both companies have access to the same dataset.

Other records connect the two companies as well. One of the first records EFF received was a version of Fog's Software License Agreement (SLA) from the Missouri State Highway Patrol. A piece of text in the header—edited to be hidden in the final document, but not deleted—reads "Venntel Analytics, Inc. Event Data Licensing Agreement." .

Finally, our investigation into the code hosted at fogreveal.com turned up several literal links to Venntel. Many different URLs with the word "Venntel" in their path are referenced in the code. For example, when a Reveal user performs any geofenced device query, that query is submitted by sending a request to the url path "/Venntel/GetLocationData."

This collection of evidence suggests that Venntel is Fog's "associate," that is, the source of its data. This conclusion would be consistent with Fog's claim that its "associate" was the only source of data for other law-enforcement-facing location data brokers. Previous reporting has revealed that Venntel supplies data to other brokers, including Babel Street, which sells location data to the government through its secret "Locate X" service.



EFF has redacted this screenshot to remove potentially identifiable information.

Records released to EFF also give us new information about how Venntel works. The screenshots appear to be taken from Venntel's own web-based portal. It has previously been reported that Venntel lets users search for devices in a specific area, then perform deep dives on specific devices. This functionality parallels Fog Reveal's "area search" and "device search" capabilities. To our knowledge, this is the first time the public has been able to see what Venntel's user interface looks like. The interface is similar to Fog's, though the visual style is slightly different. Venntel's interface also appears to display more information than Fog's does, including an IP address associated with each signal. You can read more about how Fog Reveal likely operates in our deep dive into its code.

Consent and Identifiability

In marketing materials and emails, Fog has reassured prospective customers that its data is "100% opt-in" and that "no PII [personally-identifiable information] is ever collected." But records obtained by EFF and the nature of precise, individualized location data shows that the data is incredibly personal and can easily identify people.

First, Fog's assertion that the people in its database have "opted in" rests on a legal fiction of consent that EFF, courts, and members of Congress have repeatedly criticized because it fails to adequately protect people's privacy. Modern smartphones require user consent before allowing certain kinds of data, including location, to be shared with apps. However, phones do very little to limit how the data is used after that permission is obtained. As a result, every permission is an all-or-nothing proposition: when you let a weather app access your location in order to see a five-day forecast, you may also give it the ability to sell, share, and use that data for whatever other purposes it chooses. In the United States, often the only legal limits on an app's use of data are those it places on itself in a privacy policy. And these policies can be written so vaguely and permissively that there are, functionally, no limits at all.

In other words, even if a user consents to an app collecting location data, it is highly unlikely that they consent to that data winding up in Fog's hands and being used for law enforcement surveillance.

Fog's second claim, that its data contains no personally identifying information, is hard to square with common understandings of the identifiability of location data as well as with records showing Fog's role in identifying individuals.

Location data is understood to be "personally identifying" under many privacy laws. The Colorado Privacy Act specifically defines "identified individuals" as people who can be identified by reference to "specific geolocation data." The California Privacy Rights Act considers "precise geolocation data" associated with a device to be "sensitive personal information," which is given heightened protections over other kinds of personal information. These definitions exist because location data traces can often be tied back to individuals even in the absence of other PII. Academic researchers have shown over and over again that de-identified or "anonymized" location data still poses privacy risks.

Fog's data can allow police to determine where a person sleeps, works, or worships; where they go to get lunch, or health care, or to unwind on a Friday night. Tying a location trace to a real identity is often more of a mild inconvenience than a serious barrier to police. Fog's own literature clarifies this: in a PowerPoint presentation shared with Chino, CA, it explains, "While there is no Pll data provided, the ability to identify a location based on a device's signal strength can provide potential identifications when combined with other data that agencies have access to." After attending a meeting with Fog representatives, a St. Louis County officer summarized: "There is no PI linked to the [device ID]. (But, if we are good at what we do, we should be able to figure out the owner)."

Furthermore, Fog's data is directly tied to "hashed" advertising identifiers, and multiple records show how Fog has helped its customers use "device searches" to track devices with specific ad IDs. A phone's ad ID is available to anyone with access to the device, and ad IDs shared widely among app developers, advertising companies, and data brokers of all stripes. Once an agency has access to a target's ad ID, they can use Fog to search for a detailed history of that person's movement.

Emails between Fog and the California Highway Patrol indicate that Fog did not believe the Carpenter v. U.S. decision—which held that law enforcement need a warrant to access cell site location information (CSLI)—applied to their service, and therefore no warrant was required to access the app-based location data that Fog sells. But as we have discussed, Fog's data is acquired and sold without meaningful consent and can frequently be used to track individuals just as effectively as CSLI. We discuss the legal issues with Fog and what we know about how agencies have treated the law in a subsequent post.

A perfect storm

The market for app-derived location data is massive. Dozens of companies actively buy and sell this data with assistance from thousands more. Many of them put raw data up for sale on the open market. And at least a handful of companies sell this kind of data to the federal government. Despite this, Fog Data Science is the only company EFF is aware of that sells individualized location data to state and local law enforcement in the United States.

Fog's product represents a direct and uniquely modern threat to our privacy. Its business is only possible because of a cascade of decisions by tech platforms, app developers, lawmakers, and judges, all of whom have failed to adequately protect regular users. Apple and Google have designed their mobile operating systems to

support third-party tracking, giving brokers like Fog essential tools like the ad identifier. Thousands of app developers have monetized their software by installing invasive tracking code on behalf of data brokers and ad tech. Congress has repeatedly failed to pass even basic privacy protections, allowing a multibillion dollar data broker industry to operate in the open. And courts have failed to clarify that a person's Fourth Amendment rights aren't diminished just because they're carrying a smartphone that can transmit their location to apps and data brokers.

Fog Reveal can be used to harm vulnerable people and suppress civil liberties. Fog's area searches can let police perform dragnet surveillance on attendees of peaceful protests, religious services, or political rallies. Some of Fog's customers already have a history of doing so by other means: an investigation by ACLU revealed how California Highway Patrol used helicopters with high-tech surveillance cameras to capture zoomed-in video of attendees at peaceful demonstrations against police violence.

Fog's service is especially dangerous in the wake of the Supreme Court's *Dobbs* decision. Many states have criminalized abortion, giving state and local police license to unleash their surveillance powers against people seeking reproductive healthcare as well as the professionals that provide it. Fog Reveal lets an officer sitting at a desk draw geofences around abortion clinics anywhere in the world, then track all devices seen visiting them.

Finally, Fog's service is ripe for abuse. The records we received indicated that some agencies required warrants to use Fog in some circumstances but did not show that law enforcement placed any limits on individual officers' use of the technology, nor that they conducted routine oversight or auditing. It is possible that officers with access to Fog Reveal could misuse it for personal ends, just like some have misused other investigative tools in the past. In June, news broke that a US Marshal is being charged for allegedly using a different geolocation surveillance service in 2018 that was then sold by a prison payphone company — Securus — to track "people he had personal relationships with as well as their spouses." (The US Marshals have previously contracted with Fog as well.) It's possible that officers could similarly misuse Fog to surveil people they know.

How to protect yourself

The good news, if any, is that it is relatively straightforward to protect yourself from Fog's surveillance. Fog relies on data gathered by code embedded in third-party apps. That means you can cut off its supply by revoking location

permissions to any apps that you do not completely trust. Furthermore, turning off location services at the operating system level should prevent Fog and other app-based data brokers from accessing your location data at all. (This does not always prevent location data from being gathered by other actors, like your cellular carrier. You can read more about avoiding a range of threats to privacy in one of EFF's Surveillance Self-Defense guides.)

There is no evidence that Google Maps, Apple, or Facebook provide data to Fog, and emails from Fog representatives and its customers state that Fog does not gather data from Google or Facebook. While there are other reasons to restrict Google's access to your location, it does not appear as though data shared exclusively with one of these map providers will end up in Fog's database.

Finally, evidence suggests that Fog's service relies on using advertising identifiers to link data together, so simply disabling your ad ID may stymie Fog's attempts to track you. One email suggests that Apple's App Tracking Transparency initiative — which made ad ID access opt-in and resulted in a drastic decrease in the number of devices sharing that information — made services like Fog less useful to law enforcement. And former police analyst Davin Hall told EFF that the company wanted to keep its existence secret so that more people would leave their ad IDs enabled.

You can reset or disable your ad ID by following the instructions here.

Fog and its customers have spent years trying to remain in the shadows. Its service cannot function properly otherwise. Exposed to the light of day, Fog's product becomes clear: an all-seeing eye that invades millions of Americans' privacy without warrant or accountability.

Read more about Fog Data Science:

- *Press release: Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation*
- *What is Fog Data Science? Why is the Surveillance Company so Dangerous?*
- *How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale*
- *Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data*
- *Fog Data Science Puts our Fourth Amendment Rights up for Sale*
- *How Ad Tech Became Cop Spy Tech*

LAWFARE

EXHIBIT K

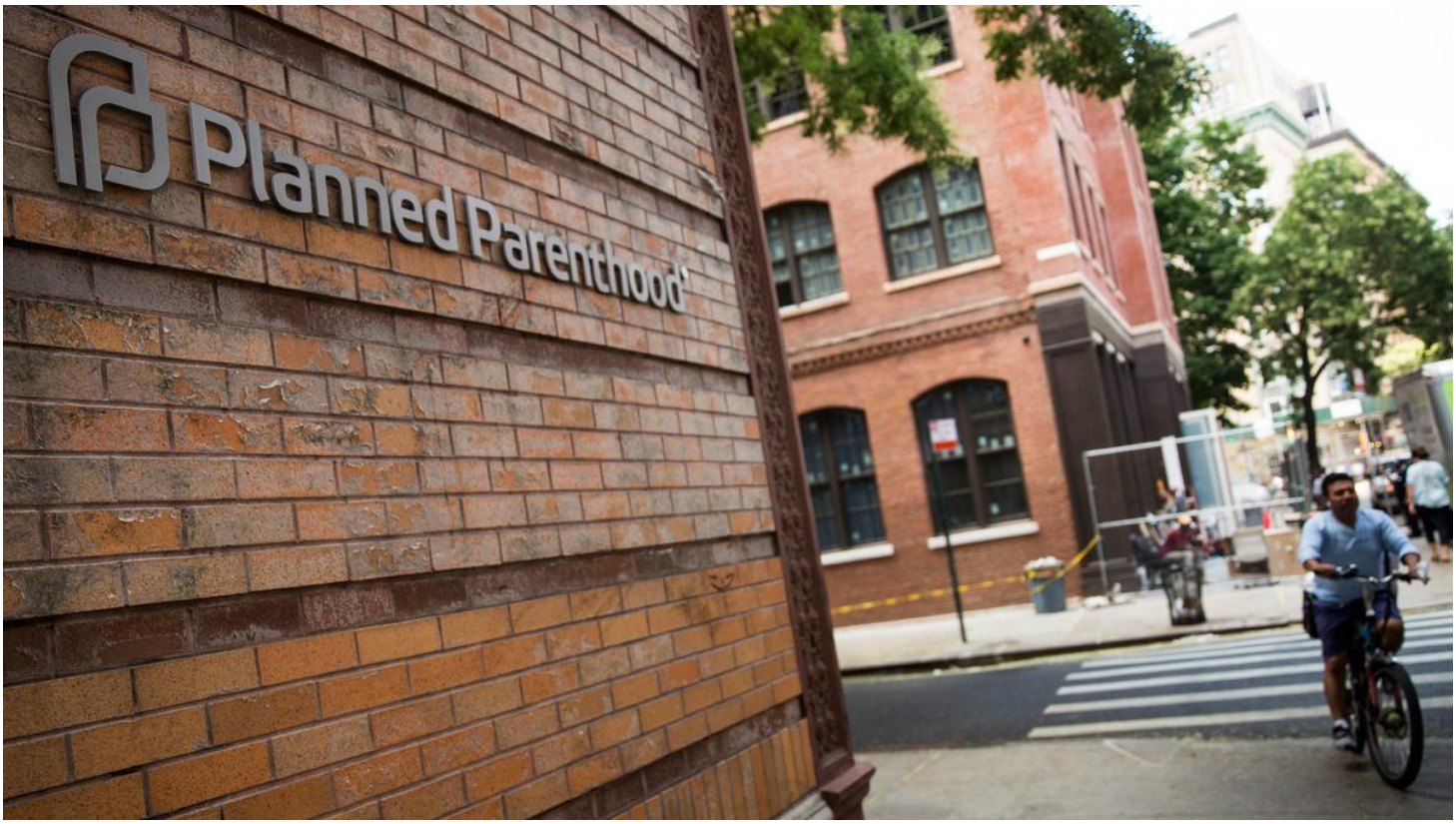
Cybersecurity & Tech | Surveillance & Privacy

The Data Broker Caught Running Anti-Abortion Ads—to People Sitting in Clinics

Justin Sherman

Monday, September 19, 2022, 8:31 AM

In 2015, a data broker helped anti-abortion groups target women in clinic waiting rooms. The Massachusetts attorney general decided to act.



A reproductive health clinic. (Source: Carrie Mumah, https://tinyurl.com/ynjum8wk)

In July, the House Oversight Committee sent letters to data brokers SafeGraph, Digital Envoy, Placer.ai, Gravy Analytics, and Babel Street as well as five personal health apps interrogating their collection and sale of people's reproductive health information. Before that, Sen. Elizabeth Warren, D-Mass., wrote letters to SafeGraph and Placer.ai about their sales of location data pertaining to abortion clinics—after which both companies pledged to stop making that information available for sale.

Amid intensifying conversations about the post-*Dobbs v. Jackson Women's Health Organization* privacy environment in the United States, particularly for those with the capacity to become pregnant, these congressional letters are hardly the first time data brokers have been accused of exploiting the data of pregnant people. Recently, the Federal Trade Commission (FTC) announced a lawsuit alleging that data broker Kochava sold location information linked to specific devices that could trace individuals' movements to reproductive health clinics and other sensitive locations—information that also could "be used to identify medical professionals who perform, or assist in the performance of, abortion services."

But data brokers have been under scrutiny for similar conduct since long before *Dobbs*. In 2017, the Massachusetts attorney general reached a settlement with the data broker Copley Advertising—which surveilled women and other people visiting abortion clinics, geofenced advertising around those clinics, and then enabled anti-abortion organizations to run anti-abortion ads to people sitting in clinic waiting rooms. The settlement ensured that the company would not use geofencing technologies near Massachusetts health care facilities again. For policymakers, legal scholars, and citizens trying to evaluate data privacy and data brokerage risks following the overturning of *Roe v. Wade*, this harmful collection and monetization of health information underscores how data privacy laws focused on these harms are sorely needed—and how state attorneys general may be able to punish or even preempt these abuses.

Data Broker Running Anti-Abortion Ads to People in Clinic Waiting Rooms

Copley Advertising, LLC, according to the settlement agreement, was a company that provided geofencing technology and advertising services to its clients. Specifically, its technology

> generally encompasses the process of identifying whether an internet-enabled device, such as a smartphone, enters, exits, or is present within a geographic area through the use of any information stored, transmitted, or received by the device, including but not limited to latitude, longitude, GPS (Global Positioning System), information, IP (Internet Protocol) address, wireless Internet access information, so-called Bluetooth technology, Near-Field Communication ('NFC') information, or device identification information.

Copley Advertising would "tag" smartphones or other devices entering or leaving an area and then would run advertisements on certain device applications—which would run for up to 30 days—based on that location information.

In 2015, Copley Advertising and its one owner and employee John Flynn provided these capabilities to Bethany Christian Services, an anti-abortion, Michigan-based, evangelical Christian organization that provides adoption services—though until 2021, not to LGBTQ+ parents—and whose website features articles about women deciding to not get an abortion. According to the settlement with the Massachusetts attorney general, Copley Advertising geofenced medical facilities for Bethany Christian Services, including reproductive health clinics, in New York City; Columbus, Ohio; Richmond, Virginia; St. Louis, Missouri; and Pittsburgh, Pennsylvania. It then enabled Bethany Christian Services to run ads to devices within a geofenced area—including abortion clinic waiting rooms.

The ads were titled "Pregnancy Help," "You Have Choices," and "You're Not Alone," among others. People who clicked on the ad were "taken straight to a landing page or webpage complete with pregnancy options information and access to a live mobile chat with a Bethany pregnancy support specialist"—in other words, an individual who could try to talk or possibly manipulate the person out of receiving an abortion. Copley Advertising also provided these kinds of services to RealOptions, an anti-abortion, so-called crisis pregnancy center network in California, though the settlement did not provide details about the services that Copley provided to RealOptions. In both cases, the purpose was to enable the anti-abortion organizations to target "abortion-minded women" who "were either close to or entered the waiting rooms of women's reproductive health clinics."

Flynn stated to the Massachusetts attorney general that it would be possible for him to "tag all the smartphones entering and leaving the nearly 700 Planned Parenthood clinics in the U.S."

The Massachusetts Attorney General's Preemptive Action

In 2017, the Massachusetts attorney general entered into a settlement agreement with Copley Advertising and Flynn. While Copley Advertising, according to the settlement, had not provided this kind of geofencing service in Massachusetts, the attorney general believed it would be unlawful for the individual to do so under Massachusetts General Law Title XV, Chapter 93A § 2, which makes illegal "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." This is because, according to the settlement, this kind of geofencing "intrudes upon a consumer's private health or medical affairs or status and/or results in the gathering or dissemination of private health or medical facts about the consumer without his or her knowledge or consent."

Copley Advertising and Flynn denied breaking any law and went a step further to "deny that they engaged in any wrongdoing." Despite that claim, Copley Advertising and Flynn entered into an agreement with the state that they would not geofence, "either directly or indirectly through others, the Vicinity of any Medical Center located in Massachusetts to infer the health status, medical condition, or medical treatment of any person." Vicinity was defined in the settlement text as "a distance of 250 feet from the Perimeter of a Medical Center." A medical center was defined as "any facility that provides mental or physical health care, treatment, counseling, or therapy by or under the authority or supervision of licensed health care professionals," including hospitals, urgent care facilities, health clinics, and family planning clinics. Interestingly, the category of "Retail Store Pharmacy" was excluded from this definition, "even if such Retail Store Pharmacy administers vaccinations, performs blood pressure screening, provides drug prescription counseling, or engages in other such health care activities."

Zooming out for a moment, there are just five states in the U.S. with consumer privacy laws, as neatly summarized by the International Association of Privacy Professionals:

- California—California Consumer Privacy Act, signed 2018, effective January 1, 2020; California Privacy Rights Act, signed 2020, fully operative January 1, 2023

- Colorado—Colorado Privacy Act, signed 2021, effective July 1, 2023
- Connecticut—Connecticut Data Privacy Act, signed 2022, effective July 1, 2023
- Virginia—Virginia Consumer Data protection Act, signed 2021, effective January 1, 2023
- Utah—Utah Consumer Privacy Act, signed 2022, effective December 31, 2023

What the Copley Advertising case demonstrates, however, is that state attorneys general do not necessarily need a state consumer data privacy law on the books to act against exploitative data collection and use. Certainly, strong privacy laws are needed in the United States—ideally, a comprehensive federal privacy regime for all residents—and added resources and authorities for punishing privacy violations and data abuses would go a long way to preventing and mitigating harm against individuals. In the meantime, state attorneys general can nonetheless look to existing legislation on consumer protection and unfair or deceptive acts or practices to approach companies with specific settlement agreements to stop their harmful behaviors. Indeed, the Massachusetts attorney general did exactly that—even though the recent phone-tracking and ad-targeting did not occur within Massachusetts itself.

Policy Implications

Much of the policy conversation about data brokers and abortion- and pregnancy-related information has focused on direct sales of that information. This is certainly an area for concern. The United States' federal health privacy law, the Health Insurance Portability and Accountability Act (HIPAA), applies only to a few kinds of "covered health entities," such as hospitals, and does not apply to a range of companies that might also collect individuals' health information—including data brokers, mobile apps, internet service providers, and social media platforms. These noncovered entities are therefore free to collect, sell, license, or share this information as they see fit. Further, the sale of health- and pregnancy-related data is of great concern in a policing context, because law enforcement does not require warrants to purchase information on Americans—ranging from location data to specific information on people's medical-related conditions and activities. Law enforcement organizations enforcing laws that criminalize abortion, particularly at the state level, could exploit this

vector of data gathering as well, in addition to surveillance mechanisms like following individuals, tailing vehicles, monitoring state border crossings, using facial recognition technology, and deploying license plate readers.

This case study underscores that data brokers' exploitation of health data is also concerning in a post-*Dobbs* environment. If data brokers, advertisers, and many other companies can legally collect, analyze, and monetize individuals' health information without substantial or any restrictions, they can enable anti-abortion actors to target people with advertisements. Those advertisements could include misinformation. Journalistic reporting and academic scholarship have underscored the ways that anti-abortion "crisis pregnancy centers" spread misinformation about abortions and pregnancy that endanger pregnant people's health. Data brokers could also enable anti-abortion groups to run outright coercive advertisements to people who are recently pregnant or visiting care facilities—using language, content, or even direct communication (like through a chat box) that intimidates individuals and interferes with their ability to make decisions freely and safely about their own body. Running an ad to someone sitting in an abortion clinic waiting room can itself signal to the person that an unknown third party, or a known anti-abortion actor, is aware of their location, which is also fear-inducing.

Fundamentally, this kind of surveillance is also invasive. Citizens do not reasonably have any knowledge of third-party companies that quietly surveil their locations and then monetize the data on the open market. The argument made by the Massachusetts attorney general underscores this point. Even if consumers were aware this was happening, it does not mean they understand how companies and other actors are using their data—and it does not change the fact that those companies and actors can use the data to harm people.

American policymakers and privacy scholars alike must push for stronger, short-term controls on data brokerage practices that invade individuals' privacy and place their health, bodily autonomy, and physical safety at risk. This could include, for example, outright bans on non-HIPAA-covered entities' surveillance and sale of Americans' health conditions, whether related to pregnancy or concerning mental health conditions, HIV/AIDS status, surgical histories, and current drug prescriptions. Waiting for a comprehensive privacy law only continues to leave individuals at risk. The danger to pregnant people is in and of itself reason to act, yet failure to legislate around data brokers also continues to pose risks to elderly Americans and those with Alzheimer's, survivors

of domestic and intimate partner violence, and other vulnerable communities. In the interim, states can pass their own data broker regulations, and state attorneys general should take note of this example from Massachusetts—where the government did not have to wait for harm to occur in its own state to act.

Understanding the full scope of data brokerage practices around health data, from surveillance to data sales to enabling targeted advertising, will only better inform regulatory responses and calibrate the most urgent places for immediate reform.

Justin Sherman

@jshermcyber

Read More

Justin Sherman is a contributing editor at Lawfare. He is also the founder and CEO of Global Cyber Strategies, a Washington, DC-based research and advisory firm; a senior fellow at Duke University's Sanford School of Public Policy, where he runs its research project on data brokerage; and a nonresident fellow at the Atlantic Council.

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

EXHIBIT L

For Release

FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices

Agency Seeks Public Comment on Harms from Business of Collecting, Analyzing, and Monetizing Information About People

August 11, 2022

Tags: Consumer Protection | Bureau of Consumer Protection | Big Data | Online Advertising and Marketing | Privacy and Security | Children's Privacy | Consumer Privacy | Data Security | Tech

Note: The FTC hosted a virtual news conference on the ANPR announcement. View the webcast.

The Federal Trade Commission today announced it is exploring rules to crack down on harmful commercial surveillance and lax data security. Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Mass surveillance has heightened the risks and stakes of data breaches, deception, manipulation, and other abuses. The FTC's Advance Notice of Proposed Rulemaking seeks public comment on the harms stemming from commercial surveillance and whether new rules are needed to protect people's privacy and information.

Give Feedback

"Firms now collect personal data on individuals at a massive scale and in a stunning array of contexts," said FTC Chair Lina M. Khan. "The growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent. Our goal today is to begin building a robust public record to inform whether the FTC should issue rules to address commercial surveillance and data security practices and what those rules should potentially look like."

The business of commercial surveillance can incentivize companies to collect vast troves of consumer information, only a small fraction of which consumers proactively share. Companies reportedly surveil consumers while they are connected to the internet – every aspect of their online activity, their family and friend networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details.

Companies use algorithms and automated systems to analyze the information they collect. And they make money by selling information through the massive, opaque market for consumer data, using it to place behavioral ads, or leveraging it to sell more products.

The FTC is seeking comment on a wide range of concerns about commercial surveillance practices. For example, some companies fail to adequately secure the vast troves of consumer data they collect, putting that information at risk to hackers and data thieves. There is a growing body of evidence that some surveillance-based services may be addictive to children and lead to a wide variety of mental health and social harms.

While very little is known about the automated systems that analyze data companies collect, research suggests that these algorithms are prone to errors, bias, and inaccuracy. As a result, commercial surveillance practices may discriminate against consumers based on legally protected characteristics like race, gender, religion, and age, harming their ability to obtain housing, credit, employment, or other critical needs.

Other concerns stem from the ways in which companies make commercial surveillance difficult to avoid. Some companies require people to sign up for surveillance as a condition for service. Consumers who do not wish to have their personal information shared with other parties may be denied service– or required to pay a premium to keep their personal information private. After consumers sign up, companies may change their privacy terms going forward to allow for more expansive surveillance. Companies increasingly employ dark patterns or marketing to influence or coerce consumers into sharing personal information.

In the last two decades, the FTC has used its existing authority under the FTC Act to bring hundreds of enforcement actions against companies for privacy and data security violations. These include cases involving the sharing of health-related data with third parties, the collection and sharing of sensitive television viewing data for targeted advertising, and the failure to implement reasonable security measures to protect sensitive personal data such as Social Security numbers.

The FTC's past work, however, suggests that enforcement of the FTC Act alone may not be enough to protect consumers. The FTC's ability to deter unlawful conduct is limited because the agency generally lacks authority to seek financial penalties for initial violations of the FTC Act. By contrast, rules that establish clear privacy and data security requirements across the board and provide the Commission the authority to seek financial penalties for first-time violations could incentivize all companies to invest more consistently in compliant practices.

Information about how to submit comments on the FTC's Advance Notice of Proposed Rulemaking is included in the Federal Register notice. The deadline for submitting comments will be 60 days after the notice is published in the Federal Register in the coming days. Submitted comments will be posted to Regulations.gov.

The public will also have an opportunity to share their input on these topics during a virtual public forum on September 8, 2022.

The Commission voted 3-2 to publish the notice in the Federal Register. Chair Khan, Commissioner Rebecca Kelly Slaughter and Commissioner Alvaro Bedoya issued separate statements. Commissioners Noah Joshua Phillips and Christine S. Wilson voted no and issued dissenting statements.

Press Release Reference

FTC to Host Forum on September 8 on Commercial Surveillance and Lax Data Security Practices

Contact Information

Media Contacts

Juliana Gruenwald Henderson
Office of Public Affairs
202-326-2924

Peter Kaplan
Office of Public Affairs
202-326-2180

Staff Contacts

James Trilling
Bureau of Consumer Protection
202-326-3497

Peder Magee
Bureau of Consumer Protection
202-326-3538

Olivier Sylvain
Bureau of Consumer Protection
202-326-3046

EXHIBIT M

SCHAKOWSKY, ESHOO, WYDEN, BOOKER INTRODUCE BILL TO BAN SURVEILLANCE ADVERTISING

Newsroom

Press Releases

Photos

Articles by Jan

Videos

September 18, 2023 | Press Release

Full text of Bill (PDF) | Summary of Bill (PDF)

WASHINGTON – Today, U.S. Representatives Jan Schakowsky (IL-09) and Anna G. Eshoo (CA-16) and U.S. Senators Ron Wyden (D-OR) and Cory Booker (D-NJ) introduced the *Banning Surveillance Advertising Act,* legislation that prohibits advertising networks and facilitators from using personal data to target advertisements. The bill also prohibits advertisers from targeting ads based on protected class information such as race, gender, and religion, and personal data purchased from data brokers. The bill allows targeting based on broad location connected to a recognizable place, such as a municipality, and explicitly allows contextual advertising, which is advertising based on the content a user is engaging with.

“For far too long, online platforms have used surveillance advertising to capitalize on consumers’ private information. This exploitative online business model weaponizes Americans’ data by, for example, targeting consumers recovering from eating disorders with diet ads or retraumatizing those suffering from a pregnancy loss. Sensitive information consumers never chose to disclose – like their behavior, medical history, or sexual orientation – has been put up for auction, literally. The Banning Surveillance Advertising Act will help safeguard consumers online by removing the financial incentive for companies to exploit consumers' personal information. I am proud to join Representative Eshoo, Senator Booker, and Senator Wyden to stop this poisonous and unscrupulous practice,” **said Representative Jan Schakowsky.** “I remain committed to passing a bipartisan, comprehensive consumer data privacy law, and I believe a ban on surveillance ads should be a part of any such piece of legislation. I look forward to continued discussion with Energy and Commerce members on both sides of the aisle in order to achieve this outcome.”

“The ‘surveillance advertising' business model is premised on the unseemly collection and hoarding of personal data to enable ad targeting. This pernicious practice allows online platforms to chase user engagement and increase their revenue at the expense of our safety and security. It is at the root of disinformation, discrimination, voter suppression, privacy abuses, and so many other harms. The surveillance advertising business model is broken," said **Representative Anna Eshoo.** “I'm proud to partner with Representative Schakowsky and Senators Wyden and Booker on legislation to ban this toxic business model that causes irreparable harm to consumers, businesses, and our democracy.”

“The first place to start in holding companies accountable is to attack the business model so many of the big tech companies depend on. If you take away the incentive to hoover up users’ personal data, you make it much harder to target them both with objectionable content and take a sledgehammer to the incentive to design platforms in a way that can be harmful – especially for kids and teens. That’s exactly what this legislation does,” **said Senator Ron Wyden.**

“Surveillance advertising is an exploitative and invasive practice that undermines Americans’ privacy,” **said Senator Cory Booker.** “We should not have to choose between using the internet and sacrificing our most personal and sensitive data. This legislation will protect our privacy, hold companies accountable for exploiting consumers, and make the internet safer for all users.”

The *Banning Surveillance Advertising Act* is supported by leading public interest organizations, academics, and companies with privacy-preserving business models.

"Identifying, tracking, discriminating, sorting, targeting, delivering harmful and hateful content, and manipulating online users lies at the heart of all that is toxic about today's digital world. Surveillance advertising drives discrimination and compounds inequities, it destroys democratic institutions and rights, strengthens monopoly power of Big Tech platforms, and is harmful to children, teens, families, and communities. If enacted, the Banning Surveillance Advertising Act would significantly curtail this business model and would be an important first step in building a better digital world," **said Katharina Kopp, Ph.D., Director of Policy for the Center for Digital Democracy.**

"The endless collection of personal data to micro-target ads is the very core of Big Tech's toxic business model and a powerful driving force behind the rise of extremism and misinformation, in addition to a myriad other societal harms. Industry's incentive to engage in massive data collection and retention in pursuit of surveillance advertising has resulted in record profits for Big Tech, but comes at great cost to our personal privacy, security and the health of our democracy. The Banning Surveillance Advertising Act will not only protect consumers from this exploitative business practice, but also mitigate Big Tech's unchecked harms as we face a growing environment of online manipulation and disinformation. We thank Reps. Eshoo and Schakowsky, and Sens. Wyden and Booker for their leadership, and call on Congress to advance this legislation with urgency," **said Nicole Gill, Executive Director and Co-Founder of Accountable Tech.**

"The Internet has no longer become an open place of discovery, let alone one where advertisers can reach users or consumers based upon the merits of their service or product. Instead we are all increasingly subject to content coming at us based on predictions of what will outrage or arouse us, which at scale is disastrous for both democracy and any competitive market. The Banning Surveillance Ads Act will assist American consumers, citizens and businesses by ensuring that the Internet works for us all, rather than disorient or polarize us**," said Ramesh Srinivasan, Ph.D., Professor and Director of the University of California's Digital Cultures Lab, author of Beyond the Valley.**

"The best way to address the harm of Big Tech is to target their surveillance driven business model, rather than push for misguided censorship. The Banning Surveillance Ads Act smartly takes aim at the harmful business model that incentivizes Big Tech platforms to seek engagement at all costs, and it avoids the pitfalls of other legislation that raises significant civil liberties and First Amendment concerns. Fight for the Future is glad to endorse this bill," **said Evan Greer (she/her), director, Fight for the Future.**

"We know that social media companies too often prioritize boosting engagement over beating extremism. Our research highlights how these companies' tools directly amplify antisemitic, extremist and racist content, though they have the power and the capability to deamplify hate. We applaud the Banning Surveillance Advertising Act, championed by Rep. Eshoo, which could help break the cycle and ultimately, make the internet safer," **said Jonathan Greenblatt, CEO and National Director, Anti-Defamation League.**

"Banning surveillance ads is essential if we want to address the disinformation crisis. Big Tech's practice of targeting those most vulnerable to messaging has upended elections, harmed children and super charged hate and division. And tech companies reap the profits, while the rest of society pays the price. That's why lawmakers need to step in and ban surveillance ads for good," **said Vicky Wyatt, Campaign Director at Ekō.**

###

Issues: Consumer Protection Privacy Online Protection

OFFICE **LOCATIONS**

Washington DC Office
2408 Rayburn HOB
Washington, DC 20515
Phone: (202) 225-2111

Skokie District Office
4500 Oakton Street
Skokie, IL 60076
Phone: (773) 506-7100

Fax: (202) 226-6890

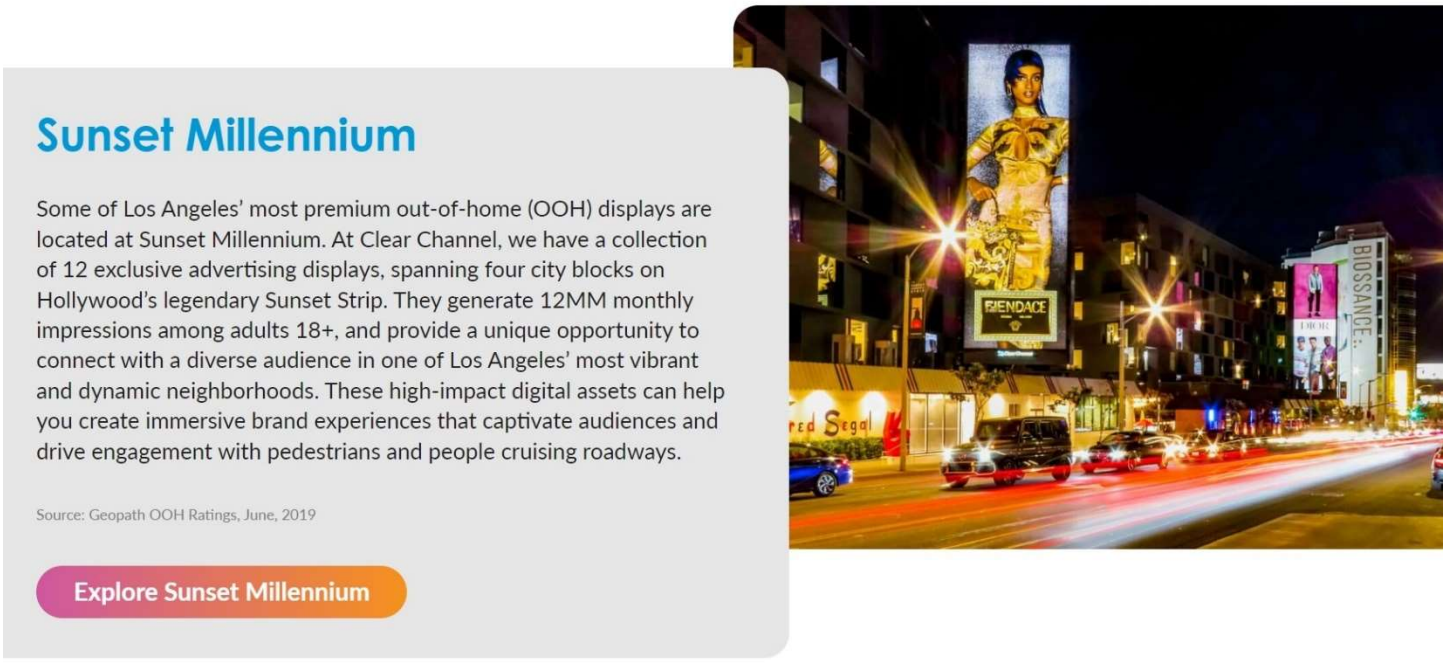
Fax: (202) 226-6890

EXHIBIT N

Images of Existing Digital Billboards in City of LA & Nearby Cities

A small sample of some of the existing digital billboards in LA area cities.

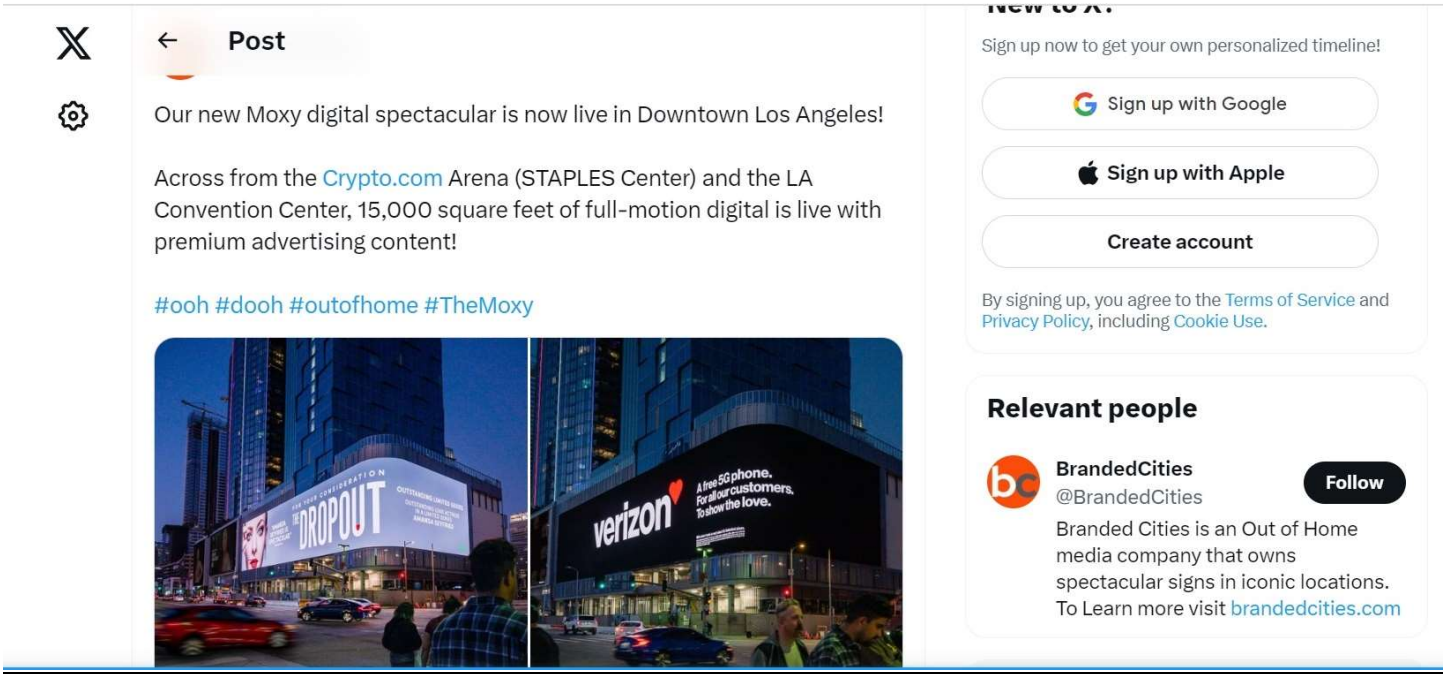
West Hollywood



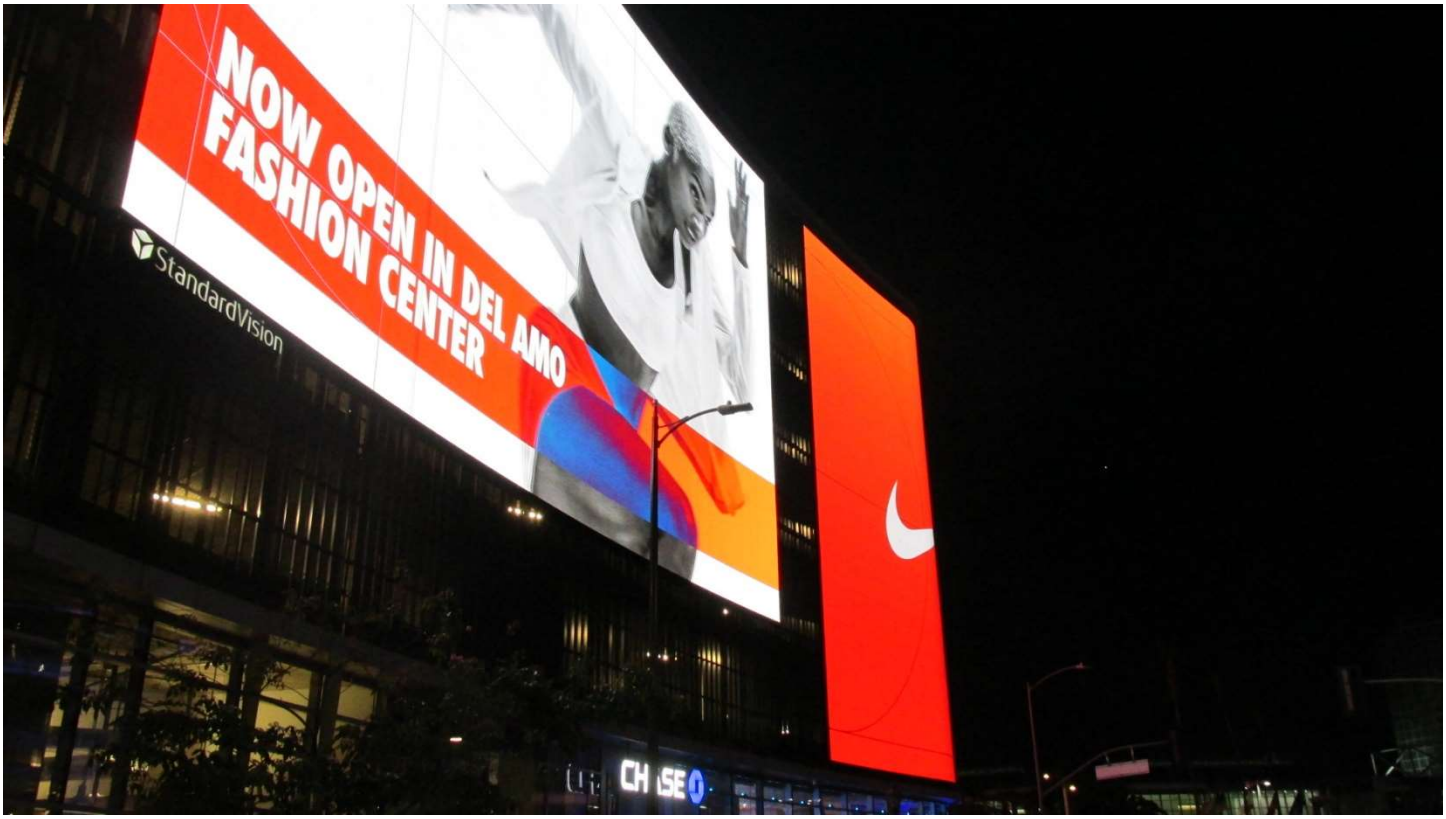
Clear Channel web page highlights "high-impact" digital assets on Sunset Strip.

Digital billboards on Sunset Strip.

Los Angeles



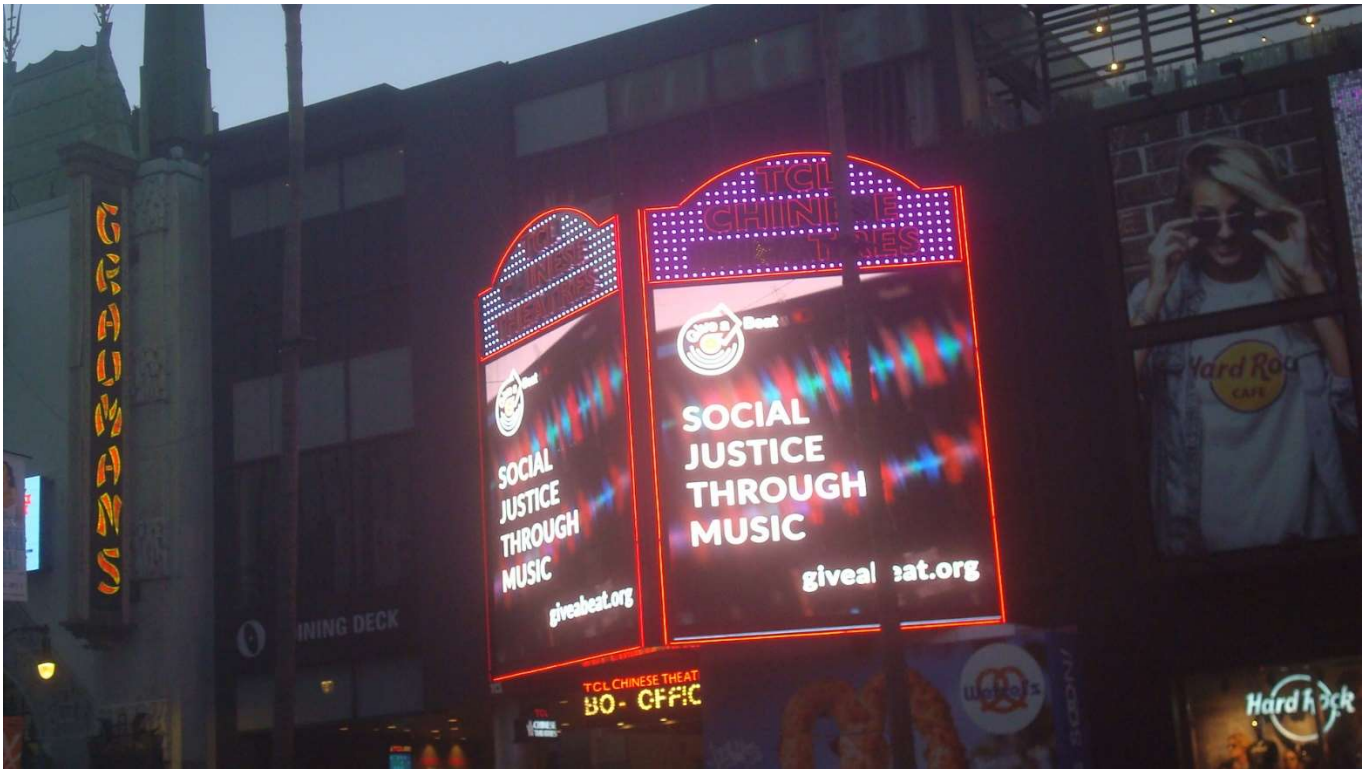
Branded Cities post on X featuring its 15,000 sq. ft. digital billboard near LA Convention Center.



Standard Vision digital billboard near LA Convention Center.

Hollywood

Hollywood theater marquee converted to digital billboard.



Digital billboard adjacent to Chinese Theater in Hollywood.

Inglewood

Wow Media digital billboard near Florence and La Brea in Inglewood.