RE: Commercial Surveillance ANPR, R111004

Submitted by New America's Open Technology Institute

November 21, 2022

Introduction

New America's Open Technology Institute (OTI) respectfully submits these comments in response to the FTC's request for public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Our comments will specifically focus on Section III. Collection, Use, Retention, and Transfer of Consumer Data, Section IV. Automated Decision-making Systems, Section V. Discrimination Based on Protected Categories, Section VI. Consumer Consent, and Section VII. Notice, Transparency, and Disclosure of part d) "How, if at All, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices that Are Prevalent?".

How, if at All, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices that Are Prevalent?

Collection, Use, Retention, and Transfer of Consumer Data

As we become increasingly aware of how corporations collect, share, and monetize our personal data at an alarming scale, we also need to recognize the persistent, structural shortcomings of the notice and consent framework in safeguarding privacy.[1] The notice and consent model of "protecting privacy" that most companies in the United States rely upon is too weak in practice to meaningfully shield individual privacy. Instead, we need comprehensive privacy regulations that will empower individuals with explicit user rights over their data, and provide strict limits on how private entities handle that data. Notice and consent is inadequate even in informing individuals about their privacy, therefore making it near impossible for users to provide meaningful consent. Few ever read the lengthy and legalistic policies attached to the products, apps, and services we use every day, which seem to stretch for pages on end. Because technology is necessary to our daily lives and it is not reasonable to expect everyday people to read dozens of pages of terms, it is no longer appropriate to say that we have willingly consented to the surveillance economy. Under a notice and consent legal framework, individuals today have no real choice in how their personal information is managed.

Transparency is important and should be further improved, but is alone insufficient. Beyond just notice and consent, users should be provided actionable rights. And further, the Commission should implement specific use restrictions, to prevent discrimination and other unfair and

[1] https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

deceptive practices. Those collecting and processing data are also in a better position than individuals to see how these tools and practices can be harmful. Additionally, entities collecting, using, sharing, and monetizing personal information must be held responsible for handling that data in a way that respects individual privacy. It is time to move away from the false promise of the notice and consent framework, and adopt a new privacy paradigm that ensures people have specific rights over their data, as well as imposes meaningful data use restrictions on companies. (Re: Question 43)

Companies also collect invasive biometric data in myriad ways. ClearviewAI, for example, has been the subject of public scrutiny for scraping publicly accessible photographs, often with names attached, from sites such as Facebook, Instagram, Venmo, and YouTube for facial recognition purposes.[2] Biometric information is the most sensitive data imaginable, and its collection, which is becoming more widespread in commercial spaces, raises significant privacy concerns. Unlike mailing addresses and passwords, our biometric information—our faces, our fingerprints, our irises, and so on—is irreplaceable and largely unchangeable. Especially over the past couple years, as the coronavirus pandemic has lingered on and public health surveillance has become more prevalent and accepted, more companies are creating and deploying new biometric surveillance tools, which are subject to little oversight and protections.[3] Now more than ever, we therefore urge the Commission to establish clear limitations on when and how private companies collect, use, share, and sell biometric data. As facial recognition and other types of biometric recognition tools become more prevalent in commercial spaces, private companies devise and deploy pandemic response tools, and some companies even monetize our sensitive biometric data, safeguards are badly needed. (Re: Question 43)

Commercial data practices are also increasingly intertwined with government data collection and law enforcement practices. Over the past few years, the media has surfaced numerous instances of U.S. government agencies circumventing Fourth Amendment requirements, and accountability more generally, by buying data from discreet commercial companies known as data brokers.[4] While we are not aware of governments' gaining voluntary access to data outside of purchases, the possibility of voluntary access without any monetary arrangement remains and should also be considered.

The practice of buying data (or gaining other voluntary access to data) means that the government circumvents the legal requirements such as court orders that would lay out parameters and particularity for the data to be obtained. Accordingly, these private sector practices are not subject to the same judicial oversight that direct government collection

---

[2] Hill, Kashmir. "The Secretive Company That Might End Privacy as We Know It". *New York Times*. January 18, 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[3] https://www.vox.com/recode/2020/7/23/21336245/clear-tsa-covid-19-screening-service-health-pass

[4] Goitein, Elizabeth. "The government can't seize your digital data. Except by buying it." *Washington Post.* April 26, 2021. https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/

otherwise would be, nor are there other oversight mechanisms (congressional or independent) in place to ensure that individuals' civil rights and civil liberties are upheld. When the government buys data (as opposed to accessing it through compelled disclosure mechanisms), there are no retention or minimization requirements or standards, no requirements that the government delete data unrelated to a certain type of investigation, and no transparency requirements—essentially, there are none of the typical democratic controls or privacy safeguards that governments require by law for intelligence collection.

The explosion of data collection by data brokers as well as behavioral profiling for the purposes of online advertising has given rise to a thriving marketplace for personal information, much of which is revealing and intimate. The commercial data broker industry is a rapidly growing multibillion-dollar economy made up of companies large and small that aggregate consumers' information into large datasets by scraping the web or buying data from other companies. This large ecosystem of companies buys, licenses, compiles, analyzes, aggregates, repackages, and sells large sets of personal information—often including very sensitive data such as location information—to anyone willing to pay for it.

A few data brokers have become notorious, such as ClearviewAI. The New York Times reported in January of 2020 that over 600 law enforcement offices around the United States had used the service in the preceding year.[5] Additional reports revealed that the FBI, U.S. Department of Homeland Security, and specifically U.S. Immigration and Customs Enforcement (ICE), had also used the company's tool.[6] But far more data brokers operate in the shadows. As far back as 2013, a U.S. Senate report detailed the threats that the data broker industry posed to consumers, finding that they "operate behind a veil of secrecy."[7]

Data brokers repackage people's personal data mostly to cater to advertisers and retail companies, who can then use it to "microtarget" consumers for online advertising—though such data is also valuable to others seeking insights into consumer behavior, such as hedge funds. The information collected and compiled into datasets can include relationship statuses, whether an individual is pregnant, which medicines an individual takes, and which businesses they frequent. Much of this data, especially location data, can be used to predict user movements, especially when combined with social network data and other analytical tools, making it valuable to advertisers and, in turn, brokers. Of all the data that brokers compile and sell, user location data are among the most sensitive and most profitable, leading to the growth of what has been called a new "location data economy."[8] The purchasers of these datasets maintain that their interest is in

[5] Ibid.
[6] Ibid.
[7] Senate Committee on Commerce, Science and Transportation. "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes". December 18, 2013. https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a
[8] Advertising market analysts BIA Advisory Services estimated that location-targeted advertising reached an estimated $21 billion in 2018, according to the New York Times. See: Valentino-DeVries, Jennifer et al.. "Your Apps

the patterns that the data reveals about consumers, rather than individual identities.[9] But those with access to the raw data could still use a unique identifier to identify a person without consent. Even without the raw data, one could easily reverse engineer location data by pinpointing a phone that regularly spent time at a certain home address, and using public records to determine who lives there.

Though these data are ostensibly collected for commerce, reporting suggests that, at least in the U.S., government law enforcement agencies are rapidly becoming major buyers. There are numerous troubling recent examples involving location data alone. In 2020, *Motherboard* revealed that a data broker named X-mode had been compiling geolocation data from a popular Muslim prayer app (Muslim Pro) and a Muslim dating app (Muslim Mingle), then selling this extremely sensitive data to the U.S. military through defense contractors.[10] Likewise, according to the *Wall Street Journal*, the Department of Homeland Security, ICE, and Customs and Border Protection have been using a commercial database from Venntel Inc. to obtain user location data to detect undocumented immigrants and monitor cell phone activity along the U.S.-Mexico border.[11] This location information—combined with other surveillance tools—has been used to track, arrest, and even deport immigrants across the country.[12] Reports also show that the U.S. Internal Revenue Service also partnered with Venntel to identify and monitor suspects in money laundering, cyber, drug, and organized crime cases.[13]

Concerningly, the practice of the state purchasing private information from data brokers has been ongoing despite rules from the U.S. Supreme Court that ban the practice. On June 22, 2018, the Court handed down its decision in *Carpenter v. US*, a landmark law enforcement data access case, ruling that under the Fourth Amendment to the U.S. Constitution, law enforcement could not compel a mobile telephone company to turn over the location of a person (for seven days or more) without first obtaining a warrant signed by a judge.[14] *Carpenter* was a narrowly written decision, and does not explicitly address U.S. intelligence agencies or other acquisitions of location data, but purchasing this data should be subject to the same oversight restrictions as other government acquisition of data. Not only does the practice of government entities buying

---

Know Where You Were Last Night, and They're Not Keeping It Secret". *New York Times.* December 10, 2018. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[9] Newman, Lily Hay. "A Simple Way to Make It Harder for Mobile Ads to Track You". *Wired*. September 21, 2019. https://www.wired.com/story/ad-id-ios-android-tracking/

[10] Cox, Joseph. "How the U.S. Military Buys Location Data from Ordinary Apps". *Vice*. November 16, 2020. https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

[11] Tau, Byron and Michelle Hackmann. "Federal Agencies Use Cellphone Location Data for Immigration Enforcement". *The Wall Street Journal*. February 7, 2020. https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

[12] Rivlin-Nadler, Max. "How ICE uses Social Media to Surveil and Arrest Immigrants". *The Intercept.* December 22, 2019. https://theintercept.com/2019/12/22/ice-social-media-surveillance/

[13] Lyons, Kim. "Congress investigating how data broker sells smartphone tracking info to law enforcement". *The Verge*. June 25, 2020. https://www.theverge.com/2020/6/25/21303190/congress-data-smartphone-tracking-fbi-security-privacy

[14] Carpenter v. United States, 585 U.S. ___ (2018).

citizens' data undermine constitutional requirements and democratic accountability, but the data that the government is buying may not even be accurate and is not subject to any oversight. While advertisers' reliance upon such information may merely result in improperly targeted ads and wasted ad dollars, some private sector uses of the data and the government's reliance upon this information can have grave implications. There are many known cases in which individuals have been denied housing due to screening companies' incorrect data, often purchased from brokers or pulled from "people search" broker websites,[15] and in which individuals have been rejected from jobs based on background checks with bad data.[16]

In order to avoid potential loopholes and mitigate the risk of future impasses to data flows internationally, it is crucial that policymakers consider not only reforms to traditional government surveillance laws, but also take swift action to close legislative loopholes and enact a comprehensive federal data privacy law. We therefore urge the FTC to consider the government's purchase and use of commercially available data as it considers commercial surveillance issues, and use its rulemaking authority to the fullest extent to close these loopholes.

Automated Decision-Making Systems

To minimize the errors made in automated systems, we recommend the FTC require evaluations of any high-risk algorithmic system before they are deployed and mitigate identified harms. Proposed pre-deployment evaluations should consider the different components and actors of the AI-system life cycle, use a clear, consensus-based definition of high-risk algorithmic systems, and assign responsibility and liability to the actors that are best suited to address potential risks.

The FTC should also use algorithmic auditing as a reliable mechanism for promoting transparency. The FTC should develop appropriate standards of practice, training and credentialing for auditors, transparency conventions, and other mechanisms that essentially turn this practice into a professional field. The creation of standards for algorithmic auditing by relevant stakeholders is important for a number of reasons. Thus far, algorithmic auditing has been carried out by a range of actors, such as investigative journalists. However, without a set of conventions to guide how these audits are conducted, it is difficult to compare, contrast, and verify the results of audits. Audits are also dependent upon human judgment, and they can therefore vary in their reliability. Standards can help combat this. (Re: Questions 53-57)

Discrimination Based on Protected Categories

If AI is not designed and monitored properly, the technology can have discriminatory consequences. For example, while these systems can help improve medical diagnostics, a study

[15] Kirchner, Lauren. "When Zombie Data Costs You a Home". *The Markup.* October 6, 2020. https://themarkup.org/locked-out/2020/10/06/zombie-criminal-records-housing-background-checks
[16] Melendez, Steven. "When Background Checks Go Wrong". *Fast Company.* November 17, 2016. https://www.fastcompany.com/3065577/when-background-checks-go-wrong

on a widely used health care algorithm showed that they can also systematically discriminate against Black people. The study found that the system failed to identify Black patients at risk for medical needs at the same rate as white patients, which resulted in Black patients being less likely to receive preventative care to improve their health. These results were particularly alarming during the COVID-19 pandemic, because Black and Brown communities are already disproportionately affected by the pandemic and AI systems may be used to help determine how to prioritize medical care if resources are scarce.

Similar to the solutions noted above, pre-deployment impact assessments and algorithmic auditing are ways to detect discrimination. Before an institution decides to implement an AI tool, it should conduct an impact assessment to evaluate the potential risks. After an AI system is deployed, it should also undergo regular audits to detect flaws or harmful consequences. Since software requires continuous updates to fix bugs and make improvements, audits need to be ongoing to stay up to date with the current version of the software. Moreover, when a system introduces new training data, audits must be updated to include an evaluation of that new data. Although audits can be costly, due process does not become less important because it is resource intensive. If an institution finds that regular audits will be too costly, they should reconsider using AI systems. The FTC should urge Internet platforms who perform audits to consider temporarily or permanently suspending systems identified with a discriminatory impact or other harmful results.

As OTI outlined in our report series exploring how internet platforms use a range of algorithmic curation practices, including ad targeting and delivery[17] and recommendation systems,[18] automated tools can generate harmful results and perpetuate historical biases in a manner that disproportionately impacts communities of color and other marginalized groups.[19] These effects can have particularly significant consequences in housing, employment, and access to financial services. Algorithms used for housing and lending decisions are (most likely) not programmed to intentionally discriminate, but can be discriminatory by their very nature, as they are trained on historical housing data in a country with a long history of housing discrimination and segregation. A plethora of existing research on this subject indicates that the offline risks and results generated by algorithmic systems are very real and can have significant consequences for already vulnerable communities. Now especially, our government should be working to address systemic racism through more equitable policy.

Consumer consent

It is OTI's perspective that it is nearly impossible for individuals to provide meaningful, effective consent, even in the case of notices being both comprehensive and easy to understand. Most

[17] https://www.newamerica.org/oti/reports/special-delivery/
[18] https://www.newamerica.org/oti/reports/why-am-i-seeing-this/
[19] https://www.newamerica.org/oti/reports/report-series-content-shaping-modern-era/

people cannot effectively weigh the costs and benefits of revealing information or permitting its use or transfer in most cases, as there is an outsized number of entities collecting, using and sharing personal data, which obfuscates any attempt at properly understanding choices. The choices however, are mostly empty, as on the one hand they decide to consent and have access to a service while on the other, they decline to consent, and then have no access to that service at all, likely without any alternatives. (Re: Question 74)

It is important to note that a simple opt-out mechanism is not enough in this context and that broader user rights are crucial generally. While outside of the purview of the FTC, it is important to have a full regime of user rights: rights to access, correct, delete, and port their data, which empowers users more than a simple opt-out mechanism. Short of this regime, opt-out mechanisms alone shift the onus to the consumer, making them alone responsible for protecting their personal information. (Re: Question 80)

Notice, Transparency, and Disclosure

The FTC's interest in protecting consumers can be achieved in part by requiring more detailed, standardized transparency reports and similar antidiscrimination audits. Better guidance for standards and procedures of reports and audits will come with a few years of reviewing transparency data and impacts of these practices on consumers.

In theory, automated content moderation tools should be easy to create and implement, as they are far more rule-bound than human beings. However, because human speech is not objective and the process of content moderation is inherently subjective, these tools are limited in that they are unable to comprehend the nuances and contextual variations present in human speech. As discussed above, these tools are limited in their ability to parse and understand variances in language and behavior that may result from different demographic and regional factors.

Two mechanisms for providing accountability around content takedown decisions that are gradually being adopted are notice and appeals. Internet platforms have begun providing notices to users who have had their content removed or accounts suspended or deleted for violating content guidelines. In addition, some platforms have introduced appeals processes so that users can seek review of content or account-related decisions.

First, we ask the FTC to encourage companies to improve the notice to users for when their content is removed, which would increase the usefulness of this notice framework. For example, in its notice to users, Facebook should specify whether the content removed was flagged and detected by an automated tool, an entity such as an Internet Referral Unit, or a user. In addition, the platform should enable users to provide more context and information during the appeals process, particularly in cases where the content was erroneously flagged or removed by an automated tool. Other platforms prefer different notice models but still could use improvement.

Reddit has a decentralized moderation, reliant on human moderators. This approach is beneficial because it is more adaptable than the auto-moderator function on the site. The automoderator provides notice to users when their content is flagged, and a similar notice system should be implemented for the human moderators who take down content.

Second, we urge the FTC to require better user controls, so that users can easily manage whether and how their data is collected and inferred, how this data is used, and how it influences the recommendations that they see. These user controls should be easy to access and understand. They should be available to all logged in users of a service. In addition, these controls should be accompanied with an explanation of how using these controls will impact a user's overall platform experience. At a minimum, these user controls should include the ability to:

- Select and change the factors (e.g. demographic information, browsing history, purchase history, ratings, interests) that a recommendation system may consider when generating recommendations for them. These settings should include the ability to completely opt out from having any of these factors considered. It should also include the ability to completely clear a user's watch, browsing, and purchase history. These controls are integral for protecting user privacy.
- Exclude certain videos, titles, channels, sellers, or items from factoring into their recommendations.
- Choose whether recommendations are influenced by a user's activity on partner or related products and websites. This should include the option to opt out entirely from having such data considered.
- Opt out of the autoplay feature on video and streaming-based services. Ideally, users should have to opt into receiving autoplay recommendations on any platform.
- Decide whether they want to receive algorithmically-curated recommendations at all. Ideally, users should have to opt into receiving such recommendations on any platform. At a minimum, users should have access to controls that enable them to fully opt out of the recommendation process. Users should have easy to use controls that let them opt out of all practices at once.

Finally,we propose the FTC require platforms to have easily comprehensible Terms of Service and publish a transparency report outlining the scope and scale of Terms of Service enforcement actions in all of the regions in which it operates. These transparency reports should provide granular and meaningful data around how the company has enforced its Terms of Service. In addition, this transparency report should be published at regular intervals (e.g. annually, quarterly, etc.). All of the data in the transparency report should be available in a structured data format (e.g. comma separated values), rather than or in addition to a flat PDF file. This is helpful to researchers who want to make use of the report data, as it simplifies the data extraction process and makes reports more accessible.

CONCLUSION

We thank the Commission for undertaking the crucial issue of commercial surveillance and for this opportunity to submit comments as the Commission considers new regulatory options related to the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. We urge the Commission to use the full extent of its rulemaking authority to curtail the unfair and deceptive practices in which many commercial entities engage. Please do not hesitate to contact David Morar (morar@opentechinstitute.org) or Lauren Sarkesian (sarkesian@opentechinstitute.org) with further questions related to these comments.

Respectfully submitted,

David Morar
Policy Fellow
New America's Open Technology Institute

Lauren Sarkesian
Senior Policy Counsel
New America's Open Technology Institute

Bailey McHale
Policy Extern
New America's Open Technology Institute, Wireless Future Project