NATIONAL CONSUMERS LEAGUE
1701 K Street, NW, Suite 1200 Washington, DC 20006
Main: (202) 835-3323 Fax: (202) 835-0747 www.nclnet.org

November 21, 2022

April Tabor, Secretary of the Commission
Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Commercial Surveillance ANPR, R111004

The National Consumers League ("NCL" or "the League") strongly supports federal regulations that protect consumer data by minimizing data collection and ensuring that individuals have full control over their information, with rights to confidentiality, access, deletion, portability, and ethical use. The Federal Trade Commission ("FTC" or "the Commission") should promulgate rules that require entities that collect consumers' data to safeguard sensitive information that would cause harm if compromised. This includes information related to a consumer's location and the genetic makeup of an individual's DNA. Lastly, the FTC should give special consideration to children's data and how school systems' educational technology partners collect and use such data.

Since 1899, NCL has advocated on behalf of American consumers and workers on a myriad of issues, including data privacy. In 1992, NCL launched the National Fraud Information Center, now Fraud.org, to educate and protect consumers from scammers.[1] The League receives thousands of reports annually detailing the consequences that result from consumer data falling into the wrong hands.

[1] "About Us," *fraud.org.* https://fraud.org/about-us/

In 2015, NCL began publishing the bi-weekly #DataInsecurity Digest, delivering consumer-centered data privacy news, policy updates, and news analysis.[2] Additionally, since 2019, the League has been pushing for federal genetic privacy protections that would safeguard the genomic information that consumers provide when using commercial and direct-to-consumer DNA sequencing products.[3] These efforts on behalf of the public interest provide NCL with insight into the struggles that consumers face in the digital environment and the shortcomings of the current U.S. privacy regime.

Worryingly, a significant number of consumers appear to suffer from "data breach notification fatigue." Due to the overwhelming number and scope of data breaches affecting consumers,[4] many are ignoring breach notifications or taking inadequate data protection measures following a notification. One RAND Corporation study found that only 51% of respondents changed their password or PIN following a breach, while 22% of respondents took no action at all.[5] Another study, conducted by the Ponemon Institute, reported that 32% of respondents ignored their breach notification and took no steps to protect their information.[6]

Unfortunately, current market and regulatory environments do not incentivize enough organizations in the private sector to make data privacy a priority.[7] This is because organizations that suffer breaches know they are unlikely to lose business due to a breach. A RAND Corporation study found that almost nine out of ten respondents continued to do

---

[2] "Welcome to The #DataInsecurity Digest," *National Consumers League.* https://nclnet.org/datainsecurity-digest-sign-up/

[3] "National Consumers League Calls for Stronger Genetic Privacy Protections," *National Consumers League.* April 7, 2022. https://nclnet.org/ncl-calls-for-stronger-genetic-privacy-protection/

[4] "Over 22 billion records exposed in 2021," *Security Magazine.* February 10, 2022. https://www.securitymagazine.com/articles/97046-over-22-billion-records-exposed-in-2021

[5] "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information," *RAND Corporation.* 2016. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

[6] "The Aftermath of a Data Breach: Consumer Sentiment," *Ponemon Institute.* April 2014. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

[7] "The Uber Hack Exposes More Than Failed Data Security," *The New York Times.* Sept. 26, 2022. https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html

business with the breached company that was responsible for their personal data.[8] With numerous employers and school systems requiring their employees and students to use certain technologies, these individuals lack the agency to choose a competitor, even in the event of information compromise.

In 2021, within the United States alone, there were an estimated 22 billion records compromised and 294 million victims.[9] Given the pervasive harm resulting from poor data privacy measures and commercial surveillance practices, NCL urges the Commission to require both businesses and government agencies to minimize their data collection while providing consumers the rights to data confidentiality, access, deletion, portability, and ethical use.

Data minimization is crucial to ensuring users' privacy, especially in situations where a consumer is required to use a specific technology for employment or education. Businesses and governments should only collect the data that is necessary to execute the functions that a user requests. Companies and agencies must collect this data transparently and in a manner and volume that is consistent with what the average consumer would expect when using those services. This would prohibit the practices that companies raced to employ over the past two decades—collecting as much information about individuals as possible, including data that was not immediately (or ever) necessary.[10]

Once an entity has collected user data, they must ensure that consumers have their rights to confidentiality, access, deletion, portability, and ethical use. A right to confidentiality ensures that companies and agencies do not share user information with

---

[8] "Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information," *RAND Corporation.* 2016. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf

[9] "Identity Compromises: From the Era of Identity Theft to the Age of Identity Fraud," *Identity Theft Resource Center.* January 2022. https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf; https://www.securitymagazine.com/articles/97046-over-22-billion-records-exposed-in-2021

[10] "Real-Time Bidding: The Ad Industry Has Crossed A Very Dangerous Line," *Forbes.* October 18, 2021. https://www.forbes.com/sites/hessiejones/2021/10/18/real-time-bidding-the-ad-industry-has-crossed-a-very-dangerous-line/?sh=4d4cdef548ca

third parties unless the consumer explicitly and recently agrees to do so while a right to access guarantees that individuals can always monitor which entities have access to their data. A right to deletion provides consumers with the freedom to destroy any held data and a right to portability gives users the ability to change data facilities with ease. Lastly, a right to ethical use prohibits the use of sensitive data, such as genetic, health, demographic, and location information, for military, social surveillance, or discriminatory purposes.

Certain categories of private information, such as location and genomic data, require extraordinary safeguards due to their irreversible and invariable nature. Regarding location information, there is a primary risk resulting from its compromise, such as the threat to physical safety due to an individual's home address leaking to non-consensual parties. Additionally, there is a secondary risk resulting from assumptions that others may make about a consumer's location data, such as LGBTQ identity or the use of reproductive healthcare services.[11]

Consumers can mitigate the primary risk of a location data breach only through costly (and often inaccessible) measures, like moving to a new house. It is often impossible to alleviate the secondary risk. For example, one cannot revoke a non-consensual party's knowledge of a consumer's healthcare decisions or sexual orientation.

Similarly, an individual cannot alter the makeup of their genetics. By genotyping their DNA, consumers gain awareness of their ancestry and certain medical susceptibilities. Should unauthorized parties obtain this information, consumers have no recourse to regain security over their genome. In extreme cases, genetic data insecurity could result in discrimination (such as when attempting to obtain health insurance), social surveillance (if the consumer belongs to a marginalized ethnic group), or political persecution (should the individual be an undisclosed family member of a government oppositional figure). In

[11] "Grindr User Data Was Sold Through Ad Networks," *Wall Street Journal.* May 2, 2022. https://www.wsj.com/articles/grindr-user-data-has-been-for-sale-for-years-11651492800; "'A uniquely dangerous tool': How Google's data can help states track abortions," *Politico.* July 18, 2022. https://www.politico.com/news/2022/07/18/google-data-states-track-abortions-00045906

addition to harming the individual who provided the genetic information, unauthorized access also affects those who share DNA with that individual.

Given the proliferation of educational technology within public school systems, children's data also deserves special consideration under any federal data privacy protections. As students are often restricted to using the software and hardware that their school systems prescribe, this eliminates most economic incentives towards better data privacy as minors (or their parents) cannot choose a competitor's product. Children deserve to grow and learn in an environment safe from pervasive commercial surveillance and without the fear of data insecurity.

NCL supports FTC regulations that would safeguard consumer data privacy. The League urges the Commission to mandate data minimization practices and rights to confidentiality, access, deletion, portability, and ethical use. Federal protections should consider the invariable nature of genetic and location data, as well as the unique challenges that minors face as school systems continue to require the use of educational technology.

Sincerely,

Eden Iscil
Public Policy Associate
National Consumers League
1701 K Street, NW Suite 1200
Washington, DC 20006
Phone: (202) 835-3323 x821
Email: edeni@nclnet.org