3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

November 21, 2022

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC–5610 (Annex B)
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

To whom it may concern:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing to you regarding the advance notice of proposed rulemaking and request for comment regarding commercial surveillance and data security (Commercial Surveillance ANPR). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 133 million consumers with personal and small business financial services products. NAFCU has long been and remains a proponent of clearly defined consumer data privacy rights and robust information security standards. Lax data security practices at largely unregulated social media companies and financial technology companies (fintechs) that collect vast amounts of consumer data pose real and growing risks to NAFCU's member credit unions and their member-owners. However, the Federal Trade Commission's (FTC) pursuing a broadly applicable data privacy-related rulemaking under its nebulous authority to regulate unfair or deceptive commercial acts or practices is both an extreme example of regulatory overreach and ill-timed. Therefore, NAFCU strongly urges the FTC to abstain from all further data privacy-related rulemaking efforts until Congress passes the comprehensive federal data privacy legislation necessary to meet the challenges of the contemporary data privacy risk environment.

General Comments

The Commercial Surveillance ANPR's premise that the FTC is "*the* nation's privacy agency" is obviously flawed. Though the FTC's enforcement actions are an important component of federal data privacy regulation, many other federal agencies implement and enforce robust federal data privacy and information security standards within the bounds of their respective missions. For example, the Commercial Surveillance ANPR references FTC enforcement actions against surreptitious collectors and sellers of Social Security numbers. The collection, use, and maintenance of Social Security numbers also lie at the heart of the Financial Services Modernization Act of 1999 (GLBA), the data privacy and information security standards of which are also implemented and enforced by the National Credit Union Administration (NCUA), the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Office of the Comptroller of the Currency, among others. Similarly, the Department of Health and Human Services regulates the use, disclosure, and safekeeping of Social Security numbers and Americans' other most sensitive health data in accordance with the Health Insurance Portability and

Accountability Act of 1996 (HIPAA). To say the least, the current federal data privacy regulatory framework, even for a single type of data, is hardly the product or responsibility of a single agency.

NAFCU supports a strong NCUA and will continue to advocate for the NCUA to remain the credit union system's primary data privacy regulator. This priority is outlined in NAFCU's Data Privacy Issue Brief, which calls on Congress to enact comprehensive federal data privacy legislation that:

1. Recognizes the strengths and efficiencies of existing federal data privacy legislation and regulation and fully exempts credit unions and other federally insured financial institutions from new federal data privacy standards;
2. Expressly preempts all state data privacy legislation and regulation;
3. Vests exclusive rulemaking and discretionary enforcement authorities in covered entities' respective primary regulators;
4. Requires that all covered entities meet a robust information security standard;
5. Requires that all covered entities use uniform, easily-accessible data privacy disclosures; and
6. Establishes principles-based compliance safe harbors for covered entities taking reasonable steps to meet their data privacy responsibilities.

Regulatory Overreach

NAFCU agrees with FTC Commissioner Rebecca Kelly Slaughter's statement in the Commercial Surveillance ANPR's commentary that case-by-case enforcement is a defective regulatory strategy. Regulation by enforcement action, whether undertaken by the FTC or any other regulator, often deprives a regulated entity of reasonable notice that the regulated entity is not meeting one or more of a regulator's expectations that are not clearly codified in a relevant statute or regulation. Furthermore, because an enforcement action is, by its very nature, limited to the specific actions or inactions of a single entity or a small number of closely related entities, regulation by enforcement action does not appropriately incentivize other entities subject to the enforcing regulator's oversight. Conservative entities subject to the enforcing regulator's oversight may avoid engaging in perfectly permissible activities for fear that an enforcement action's findings could be generalized to preclude a broader set of activities. Entities engaged in activities that pose similar or even greater risks to consumers than those activities underlying an enforcement action shelter behind slight differences between their own risky activities and the details of an enforcement action's explanation and analysis.

NAFCU and its members agree that the FTC and other regulators should strive to provide meaningful regulatory clarity through the formal rulemaking processes rather than rely on blunter, less democratic means, such as an enforcement action, interpretive rule, or press release. But neither the FTC nor any other regulator should, in the name of regulatory clarity or because it is simply ill-content with the inherent limitations of its present processes, attempt to shoehorn a rulemaking into an agency authority not reasonably connected to the rulemaking.

The Commercial Surveillance ANPR bases the FTC's pursuing a broadly applicable data privacy-related rulemaking on the FTC's authority, provided by Congress under the Federal Trade Commission Act of 1914 (FTC Act), to define and root out "unfair or deceptive acts or practices in or affecting commerce." Immediately thereafter, however, the Commercial Surveillance ANPR wholly undermines its own point by listing subsequently enacted federal data privacy laws under

which the FTC enforces industry-specific federal data privacy and information security standards, including the Fair Credit Reporting Act (FCRA), the GLBA, and the Fair Debt Collection Practices Act (FDCPA). Where Congress has intended to recognize Americans' data privacy rights and for there to be robust information security standards, it is plain Congress has identified subject data, shaped technical frameworks, and selected the regulators best positioned to implement and enforce federal data privacy-related regulations within the scope of their respective missions.

Improper Timing

As FTC Commissioners Rebecca Kelly Slaughter, Alvaro M. Bedoya, and Christine S. Wilson all recognize in the Commercial Surveillance ANPR's commentary, the American Data Privacy and Protection Act (ADPPA) has, at times, enjoyed considerable bipartisan support. Though the ADPPA now appears highly unlikely to become law, the ADPPA's debate strongly suggests federal lawmakers on both sides of the aisle are increasingly interested in better protecting Americans' data privacy. When Congress ultimately passes comprehensive federal data privacy legislation, the FTC may well garner significant new data privacy-related authorities. But, rather than rely on a nebulous authority granted to it by Congress more than 100 years before many of the data and data practices the Commercial Surveillance ANPR addresses came into being, the FTC should await further Congressional action.

By pursuing a broadly applicable data privacy-related rulemaking as outlined in the Commercial Surveillance ANPR now, the FTC is marching toward an unforced error that is likely at least bi-fold. First, by anchoring its implementation and enforcement of such a rulemaking to its authority to regulate unfair or deceptive commercial acts or practices, the FTC is exposing itself to legal challenges that may delay the development of more well-founded, effective data privacy-related regulation. Second, even if such a rulemaking ultimately faces no legal challenges and can be finalized within a timely fashion, the FTC is needlessly expending federal resources before Congress clearly defines the FTC's responsibilities and authority to implement and enforce such a rulemaking. Until Congress acts further, the FTC cannot be reasonably certain that whatever data privacy-related rulemaking the FTC pursues now will ultimately meet the FTC's responsibilities under comprehensive federal data privacy legislation – or even survive its passage.

Conclusion

NAFCU strongly urges the FTC to abstain from all further data privacy-related rulemaking efforts until Congress passes comprehensive federal data privacy legislation that clearly defines the FTC's relevant responsibilities and authority. Should you have any questions or require additional information, please contact me at dbaker@nafcu.org.

Sincerely,

Dale Ross Baker

Dale Ross Baker
Regulatory Affairs Counsel