Commercial Surveillance ANPR, R111004

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

November 21, 2022

RE: ACRO comment submission on:
Federal Trade Commission (FTC): Trade Regulation Rule on Commercial Surveillance and Data Security

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research and technology organizations. Our member companies provide a wide range of specialized services across the entire spectrum of development for new drugs, biologics, and medical devices, from pre-clinical, proof of concept and first-in-man studies through post-approval and pharmacovigilance research. ACRO member companies manage or otherwise support a majority of all FDA-regulated clinical investigations worldwide. With employees engaged in research activities in 114 countries, the member companies of ACRO advance clinical outsourcing to improve the quality, efficiency, security, and safety of biomedical research.

As a condition of their research and related services, ACRO members must follow existing privacy and security laws and regulations and applicable consent processes when collecting, processing, storing, transferring, and de-identifying health and health research information. Moreover, some members are leaders in the health-related sector with respect to the development of innovative Software as a Medical Device and Clinical Decision Support Software that are supported through artificial intelligence (AI) algorithms, or more specifically, machine learning (ML) algorithms.

ACRO is pleased to provide the following feedback.

I. General comment:

In this ANPRM, FTC requests public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Specifically, the Commission invites comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning 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.

ACRO members engage in a broad range of activities related to critical medical research. These activities are conducted consistently with applicable law and provide substantial benefit to the public at large and to the health care system, by aiding in the development of new medicines and treatments, expanding public knowledge of disease, and improving overall health care. These activities provide substantial benefit, rather than creating harm to consumers. ACRO urges the Commission to avoid rulemaking that could create overlapping, burdensome, or inconsistent regulation of a health and research sector that is already strongly and effectively regulated in terms of information privacy and security and with respect to AI algorithm requirements. Further, to the extent to which additional regulation of commercial surveillance and data security practices is needed, we urge the Commission to defer to Congress, which is making progress with regard to development of comprehensive data protection and privacy legislation.

II. Specific Comments to Selected Questions Posed by the Commission:

The ANRPM requests public comment on 95 data-related Questions, which include topics of data security; consumer data collection, use, and transfer; automated decision-making systems; discrimination; consumer consent; and notice, transparency, and disclosure. ACRO's Comments pertain primarily to ANPRM Questions that relate directly or indirectly to the health-related sector as set forth below.

Section (a). To what extent do commercial surveillance practices or lax security measures harm consumers?

Question 10. *Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?*

Any rule issued subsequent to this ANPRM should provide for common exemptions and a clear narrowing of applicability. The federal Health Insurance Portability and Accountability Act (HIPAA) and a multitude of State privacy laws addressing health data include extensive, detailed, implemented, and enforceable regulatory requirements for privacy, security, and breach protections for health data. This includes broad and specific requirements for consent, collection, use, security protections, storage, retention limitations, data-sharing/transfers and data use agreements, de-identification methodologies, breach reporting, etc. On these grounds, ACRO urges the Commission to exclude health data that is already regulated from the scope of its proposed rulemaking process. Otherwise, new rulemaking could deter the important collection and use of health-related data for the development of innovative and life-saving technologies and therapies that benefit both individual consumers and society at large.

We note that HIPAA's methodological requirements for de-identification of health data set forth at 45 C.F.R. 164.514 (Methods for De-identification of PHI | HHS.gov) have stood the test of time for 20 years. In fact, the standard established – that the risk of re-identification is "very small" [at 164.514(b)(1)] – has been confirmed by the observation that, notwithstanding highly equivocal results observed during a re-identification "challenge" sponsored by the HHS Office of the National

Coordinator for Health IT (ONC,) there has been no verified report of a successful real-world re-identification attack against a de-identified data set that has been certified to the HIPAA standard. Consistent with the approach of ensuring that any new FTC rule does not impose new obligations where there are existing legal structures for health data, we encourage the FTC to make clear that data that has been de-identified consistent with the HIPAA standard would not be subject to a new rule as personal information. Having inconsistent definitions of what constitutes de-identified data, and which is therefore outside the scope of a data protection regulation, could result in the problematic situation in which data could be understood as de-identified under one regimen, such as HIPAA, but considered identifiable data under another rule.

Further, ACRO strongly urges that any potential new FTC regulation on commercial surveillance specifically exempt human subject research data from its scope. We note that all five of the States (California, Virginia, Colorado, Connecticut, and Utah) that have passed data protection laws have exempted certain data that is already protected by existing federal regulations.

All five states also have wording similar or identical to Virginia's Consumer Data Protection Act 59.1-576(C)(4) that exempts human subject research data, i.e.,

> Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R Part 46; identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by The International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use; the protection of human subjects under 21 C.F.R. Parts 6, [11], 50, and 56; or personal data used or shared in research conducted in accordance with requirements set forth in this chapter, or other research conducted in accordance with applicable law.

In addition, ACRO urges the FTC to consider and avoid impacting clinical trials and medical research to the extent those activities rely on "consumer data" as it may be defined beyond the scope of HIPAA or human subjects research data. In particular, clinical trials and drug development increasingly, appropriately and securely use Real-World Data (RWD), which comes from many sources, such as consumer health data and mobile device data. The FTC's proposed additional consumer-based regulations could create ambiguity, conflict with existing compliance practices, and otherwise hinder the ability to use this data and other types of data for meaningful outcomes as intended by the 21st Century Cures Act.

The use of consumer data is emphasized in the 21st Century Cures Act specifically in support of regulatory decision-making, such as approval of new indications for approved drugs. The Cures Act furthers this critical goal by restricting information blocking by organizations that hold patient data to make such data more portable, recognizing that interoperable health information will benefit individuals, clinicians, and researchers. This use is balanced with the established compliance requirements for privacy, confidentiality, availability, and security.

We note that the Federal Trade Commission (FTC) currently regulates many of the data sources for RWD, used for real-world evidence generation by health care companies or pharmaceutical companies. The FTC also enforces the Health Breach Notification Rule, which requires organizations not covered by HIPAA to notify their customers, the FTC, and, in certain cases, the media, of material breaches.

Question 12. *Lax data security measures and harmful commercial surveillance injure different kinds of consumers … in different sectors (e.g., health, finance, employment) … For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? … To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?*

Consistent with the previous comment, ACRO believes that any data security measures developed by the FTC should exempt data that is already subject to the full range of security and breach reporting requirements referenced above.

Section iii. Collection, Use, Retention, and Transfer of Consumer Data

Question 39: *To what extent, if at all, should the Commission limit companies that provide any specifically enumerated services (e.g., finance, healthcare, search, or social media) from owning or operating a business that engages in any specific commercial surveillance practices like personalized or targeted advertising? If so, how?*

Personalized or targeted advertising can be helpful to consumers interested in healthcare services or access to a clinical trial. For example, personalized or targeted outreach can be important for increasing the number and diversity of participants in clinical trials. To limit companies that specialize in those areas from providing helpful information to consumers through targeted advertising may reduce the effectiveness of such information for the consumer and create barriers to healthcare access or participation in innovative research opportunities. In light of this experience in the clinical research sector, ACRO would be concerned about the potential for over-reach in a proposal to impose blanket restrictions on the ownership or use of companies that provide useful personalized or targeted advertising.

Question 43. *To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, i.e., limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are* *compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?*

HIPAA/HITECH and other privacy/security laws and regulations regarding health data already have strict requirements for informed consent, data collection, retention, purpose limitations, data minimization, de-identification, data aggregation, and data sharing/transferring of health data. Again, ACRO recommends that the Commission exclude data already regulated by Federal and State laws from its proposed rulemaking.

Section iv. Automated Decision-Making Systems

Question 56. *To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps?*

The Food and Drug Administration (FDA) regulates the use of Artificial Intelligence and Machine Learning (AI/ML) algorithms in the health-related sector. This is an innovative area for developing clinical decision support software for health care professionals and to encourage advances in Software as a Medical Device. These technologies rely on medical algorithms. The Agency is monitoring the accuracy of such algorithms as part of regulatory oversight with the goal of improving healthcare. Indeed, on September 27, FDA issued the final version of its policy on Clinical Decision Support (CDS) Software as addressed in the 21st Century Cures Act of 2016 (see attached). In addition, numerous United States and international governmental and nongovernmental organizations are currently undertaking the complex work of evaluating and promulgating AI (algorithmic) risk frameworks, in order to appropriately understand and balance the benefits of risks of this critical technology. Examples in the United States include the National Institute of Standards and Technology (NIST) (which is developing a framework to identify and manage AI associated risks to individuals, organizations, and society); the Biden Administration's Office of Management and Budget (which published draft AI principles in January 2020); and the White House Office of Science and Technology Policy (which in 2021 launched an initiative to develop an "AI Bill of Rights"). In Europe, the European Commission has published a proposal for an AI Act in 2021 (which aims to foster AI technology innovation while meeting privacy, security, and human rights requirements); and the European Parliament has published a Research Study on AI in healthcare (which sets out numerous policy options to "better develop, evaluate, deploy and exploit technically, clinically and ethically sound AI solutions in future healthcare"). These among numerous other well-resourced and expertly-staffed initiatives indicate the necessity of an extremely careful and detailed approach to ensuring that addressing risks does not unnecessarily impede the valuable goals of algorithm-based technology.

Accordingly, ACRO urges that the Commission exclude algorithmic tools that are already regulated by the FDA.

Question 61. *What would be the effect of restrictions on automated decision-making in product access, product features, product quality, or pricing?*

Such restrictions may deter development of advanced automated decision-making products that could prove useful to consumers, particularly in the health and research sectors. ACRO suggests that imposing restrictions by the Commission upon such a new and developing AI/ML technology could impede innovation and reduce access to healthcare and health research.

Conclusion

In summary, ACRO advises the Federal Trade Commission to avoid creating in a new trade regulation overlapping, duplicative or even conflicting requirements for data that is already regulated by other Federal rules, including HIPAA, the Common Rule and FDA regulations.
Thank you for considering our comments.

Douglas Peddicord, Ph.D.
Executive Director