

October 21, 2022

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Comments of the Taxpayers Protection Alliance

Re: Trade Regulation Rule on Commercial Surveillance and Data Security
Document ID: FTC-2022-0053-0001

The Taxpayers Protection Alliance (TPA), a non-partisan advocacy organization representing millions of taxpayers and consumers, writes today to the Federal Trade Commission (FTC) in response to its request for comment on the prevalence of data security practices, which practices harm consumers, and whether the Commission should pursue regulatory alternatives concerning the ways private companies collect and utilize data. We appreciate the opportunity to comment on behalf of our members and supporters.

Firstly, TPA wants to caution the Commission not to create any new constitutional “rights” that do not exist. The Constitution – and the Bill of Rights – were written as restrictions on governmental authority. The provisions spelled out there do not limit private actors. In much the same way that a mother may dictate what type of speech she’ll allow at her dinner table, private companies have broad leeway to operate as they see fit on the platforms which are their property. The government – on the other hand – does not have the same right to impose such restrictions.

So too should it be so with regards to privacy regulation. The Commission begins its request for comment on this issue thusly:

Whether they know it or not, most Americans today surrender their personal information to engage in the most basic aspects of modern life. When they buy groceries, do homework, or apply for car insurance, for example, consumers today likely give a wide range of personal information about themselves to companies, including their movements, prayers, friends, menstrual cycles, web-browsing, and faces, among other basic aspects of their lives.

While this is all true and may indeed make certain consumers uncomfortable, this data collection is a product of voluntary associations. A citizen conducting business, buying products, or just browsing the web does so freely and with the option to just as freely discontinue doing so at any moment. At this time, that same citizen does not have the option to disassociate with the government. This is fundamentally why their interactions ought to be viewed differently in the eyes of the law and in the eyes of a regulatory body such as this Commission.

It is also important to note that – fundamentally – this data collection is just a modern iteration of common business practices. Any successful entrepreneur or businessman conducts market research to ensure that his or her product has demand and determine what – if any – improvements can be made. For example, retailers have used consumer programs to harvest individual data for the purposes of more effectively offering products and services to meet their customers’ needs.

Data collection practices as described by the Commission in its overview of this advanced notice of proposed rulemaking follows in that same tradition. The key difference is that this latest version is on a much broader scale and using more sophisticated technology. At its roots, however, this is just an innovative way of conducting market research.

Such data collection methods breed innovation and competition. Just like a business conducts research to improve its marketing and its products, so too does a modern tech company collect data to create a better experience for users. This can range from giving browsers a more relevant ad experience – showing them products and services that might interest them – to creating new products or services based on what is most popular in existing ones.

The FTC’s stated mission is to “protect the public from deceptive or unfair business practices.” While technology may be new and –admittedly – many in the general public may not understand the methods through which companies are collecting this data, there is very little deceptive or unfair about it. It is the latest development in the quest of private companies to improve their business model, for consumers. This is a feature, not a bug, of the free enterprise system.

Consumers value privacy differently. Some may indeed take an absolutist approach to their privacy, not desiring any entity – governmental or corporate – to access any of their information. However, others may *want* their data to be used to give them a more custom experience and to be able to find relevant information online more easily.

If public policy is tailored towards the former group, the experiences and liberties of the latter will be harmed in the process. The Commission, while considering this issue, must avoid catering to the lowest common denominator and let consumers – individually and personally – decide what’s right for them.

The best use of the Commission’s time and energy on this front would be to focus on fraud prevention, as opposed to dictating terms of services. Given the FTC’s stated mission, actual instances of deception should fall more squarely into the Commission’s purview than concern about excessive data collection.

Another important consideration is that risks will be inherent in this – or any other – process. Nothing emanating from the federal government should act as a one-size-fits-all solution to every privacy concern ever voiced. There will be tradeoffs with every conceivable proposal. Regulations targeted at eliminating all possible risk will severely

limit consumer choice, also known as competition, and potentially halt life-altering innovations. The Commission should recognize that there exists an acceptable level of risk, and that the solution to that risk is consumer vigilance and education – not government intervention.

The Commission should also strive to avoid pre-empting the role of Congress in crafting any policy directed at data privacy. Uncertainty acts as a drain on economic growth and innovation. Any lasting solution on data privacy should flow through the halls of Congress. A broad policy emanating from this Commission – as well-intentioned as it may be – will be subject to a regulatory Ping-Pong of sorts, where companies will not be sure how their business practices will be regulated one year to the next as the administration changes hands. Congress, as designed by the Constitution, is slower to implement sweeping changes to existing policy.

The Commission also notes that data security is an important part of this advanced notice of proposed rulemaking. This is an area of more paramount importance than regulating data collection practices.

The FTC can assist in this effort in several ways. The first is to instill reasonable oversight measures to ensure no undue pressure is exerted on companies to turn over private information to governments without following all proper legal channels. This is one of the first, most basic steps necessary to safeguard the information that is collected from hostile actors – foreign or domestic.

The FTC can also relax existing antitrust actions and postures to better allow the sharing of best practices across the industry. Businesses in this space have a shared interest in ensuring malware and other dangerous technologies do not work their way into the market. Experts from various companies can share information to improve safety for consumers across the economy.

Unfortunately, the FTC has its sights set on such information sharing as a “deceptive or unfair” practice, despite the clear consumer benefits such sharing would have. Companies barring potentially malicious actors from their app stores, or insistence on having vendors use verifiably safe payment processing systems and security protocols are commonsense precautions. They should not fall into the FTC’s crosshairs.

Finally, and most simply, the Commission should allow and encourage the market to reward companies that meet the privacy standards deemed best by consumers. Companies will respond to market forces, which is why FTC must remain focused on deterring fraud above micromanaging privacy practices. If consumers prefer a service that affords a little more privacy, they will – in the absence of other obfuscating forces – flock to services that provide that. If they prefer services that are more customized to their needs because they’ve given some of their data over, they will patronize businesses and companies that provide that for them. This is the invisible hand of the economy at work. Government entities like the FTC need only sit back and watch it work.

The digital ecosystem has been able to grow and thrive with minimal intervention by government actors. TPA, along with the millions of taxpayers and consumers we represent, are excited to see the next steps in the years to come. We are glad the FTC has recognized the growing importance in this space and have sought comment from the public on how best to proceed. We thank you in advance for your thoughtful consideration of the principles and recommendations outlined above.

Sincerely,

David Williams
President

Patrick Hedger
Executive Director

Dan Savickas
Director of Tech Policy