Major County Sheriffs of America
www. mcsheriffs.com

November 21, 2022

Via Electronic Submission

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: Comments of the Major County Sheriffs of America Regarding "Commercial Surveillance ANPR, R111004"

The Major County Sheriffs of America (MCSA) submits the comments below in response to the FTC's request for public comment on a proposed rule addressing "commercial surveillance and data security" (R111004). The MCSA is professional law enforcement association of the 113 largest sheriff's offices representing counties or parishes with a population of 500,000 or more. Our members represent over 130 million Americans, and we provide policing, investigative, and correctional services to the nation's largest metropolitan areas. We dedicate ourselves to preserving the highest integrity in law enforcement and the elected Office of the Sheriff.

The MCSA believes commercial data privacy and security protections are critical for the safety of our citizens and for our national security. We also have a vested interest in protecting the privacy of our deputies and officers to ensure their safety and that of their family. However, any rule, regulation, or law regarding commercial data must balance individual privacy and data security interests with vital public safety and crime victim considerations, including the ability to investigate criminal activity in an increasingly digital world. The public safety and criminal justice costs associated with data regulation could outweigh any privacy and data security benefits if that balance is not struck.

Our comments to the Commission on the topic of data security and privacy are consistent with our educational efforts in both the U.S. Senate and U.S. House of Representatives where we have emphasized the significant public safety consequences that could result if the *American Data Privacy Protection Act* (ADPPA) were to be enacted as currently drafted. We support strong data privacy and security policies, but we have found that some advocates and policymakers have not considered the very real likelihood of negative impacts on criminal investigations and public safety that would result if legislation or regulations are enacted that create unreasonable barriers to law enforcement access to digital evidence.

We strongly encourage the FTC to thoroughly consider these concerns by seeking engagement from local, state, and federal law enforcement professionals – especially those in law enforcement who are routinely involved in investigating crime. No rule should be enacted in the name of consumer data privacy protection that creates a safe harbor for violent criminals, organized criminal organizations, human traffickers, child sexual predators, international and domestic terrorists, or others seeking do harm. MCSA believes there is a way to balance the legitimate interests of privacy and data security with the equally legitimate need to investigate crime and seek justice for victims. That balance cannot be achieved if law enforcement and public safety concerns are not adequately considered by the Commission.

Any regulation that ignores law enforcement concerns could render common investigative tools unavailable or extremely limited. These tools are used successfully by law enforcement agencies around the country every day to efficiently and accurately investigate violent crime, human trafficking, child sexual exploitation, fentanyl and opioids trafficking, violent extremism, carjacking, kidnapping, and threats of mass violence that are made on social media.

The tools are merely an efficient means of searching publicly available data and commercially available data. Because this data often forms the essential building blocks for generating investigative leads, especially in the early stages of a critical incident, there is simply nothing that can replace that speed and capability for investigators. It often means the difference between life and death for a crime victim.

Certain advocates grossly misconstrue how law enforcement uses investigative tools and commercially generated data to justify restrictions or prohibitions. Some falsely suggest that law enforcement uses "commercial surveillance" tools to "monitor" individuals. They baselessly assert that law enforcement exploits the personal data of ordinary citizens without any transparency, without limits, or without guardrails.

It is a 21st Century reality that digital information generated by public and private entities is relevant to most criminal investigations. If rules and regulations are not crafted carefully – keeping public safety at the forefront – the proposed rule could prevent law enforcement from obtaining crucial information in a timely, lawful manner. That would significantly jeopardize our ability to rescue victims, protect communities, and prevent bad actors from exacerbating an already historic rise in violent crime.

We urge the Federal Trade Commission to move slowly and cautiously if the Commission elects to continue with a final rule. It is no exaggeration to say that the Commission's action on this matter could weaken criminal investigations and set back law enforcement's ability to protect citizens. Investigators need lawful access to digital evidence so that we can fight the unprecedented spike in violent crime, counter technologically savvy criminals, keep children and families safe from predators, and infiltrate and stop terrorist organizations and other extremists who seek to do harm.

MCSA thanks the Commission in advance for considering our views and we stand ready to work with the Commission and all stakeholders to strike the proper balance between data privacy, data security, and public safety.