July 26, 2022

The Honorable Joseph R. Biden Jr.
President of the United States
1600 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Mr. President,

We send this letter to urge the White House to ensure that proposed comprehensive federal privacy legislation does not become a tool to undercut the ability of law enforcement across this country to protect the American People. In the knowledge that misguided proposals by some to “defund the police” should instead be efforts to improve policing practices, we now must overcome schemes to hamstring law enforcement by crippling its most effective digital analysis tools.

To acknowledge the “elephant in the room”, this letter is not addressing anything related to the impact of the Supreme Court’s Dobbs decision, such as possible rules about geo-location data and the like. That is a different topic for a different day. Instead, we write due to concerns about proposed anti-law enforcement language in the “American Data Privacy and Protection Act” (ADPPA), now pending in the House of Representatives.

Unfortunately, today criminals have abundant resources, sophisticated technology, and stolen data to support their broad, nefarious efforts. Law Enforcement -- and private sector fraud prevention groups – need similarly effective tools to counter and prevent criminal activity. As proposed, the ADPPA ties the hands of our law enforcement professionals and prevents them from protecting American taxpayers from fraud, waste, abuse, and the continued victimization of our most vulnerable populations. The ADPPA is not in the best interest of the American people, but instead empowers transnational criminal groups, fraudsters, human traffickers, and even pedophiles by taking away law enforcement’s most powerful and effective investigative tools: data and data analysis from public – private partnerships.

Background:

Federal, state, and local law enforcement agencies nearly all use private sector data-centric services for crime prevention and investigation. There are two or three leading providers of these services, which all share the following characteristics:
• They collect and use publicly available information such as government records (no privacy interest).
• They supplement those public records with other data, including regulated data such as federal regulated credit header information (GLBA-regulated) and drivers’ license data (DPPA-regulated).
• The services all acquire their data indirectly rather than directly from individuals; and
• The services are all provided not only to law enforcement but also to private sector customers who use them to prevent identity theft, stop fraud and generally protect American consumers.

These services do NOT contain privacy-centric behavioral data such as purchasing history, web search history, or geo-location data.

Concerns

The proposed ADPPA bill in Congress undercuts the effectiveness of these critical public-private partnership investigative tools. While the bill continues to evolve, it currently:

• Penalizes any company or services that acquires consumer data indirectly, letting criminals completely opt out of such services and empowering them to prohibit future data collection. This approach is a gift to fraudsters, pedophiles, terrorist and others who would wish to hide their dangerous activities from law enforcement.
• Fully regulates even publicly available data if it is combined with other data sets – a provision included in this bill even though all critically important law enforcement tools used today use such combined data sets.
• Limits authorization for using data to prevent or investigate “illegal activity” to solely illegal activity deemed to “directly harm another person”. The bill thus picks a subset of illegal activity that can be addressed with important investigative tools, hamstringing law enforcement efforts to investigate other illegal activity, from money laundering to ransom ware to fraud against government agencies such as unemployment, tax or relief agencies.
• Purports to exclude from its scope services performed “on behalf of” government agencies, knowing that this exclusion is pointless because the critical services used today do not involve data uses by agents acting “on behalf of” law enforcement but are services provided TO law enforcement professionals (and to corporate anti-fraud departments).
We are not in opposition to the concept of a federal privacy law, but we feel strongly that any such laws should not seek to undercut the effectiveness of law enforcement.

Our concerns are very real. Already in the past year, pressure and threats from certain Congressional offices resulted in the decision by U.S. utility providers to stop sharing customer sign-up data, known as NCTUE files, with law enforcement or private sector fraud departments. Congress never took a vote on this issue and no law exists limiting law enforcement use, but it was accomplished through back-channel pressure, with the result being the services used to protect our country are now less accurate and timely than they otherwise would be.

In short, the ADPPA should not be a backdoor ploy to pick and choose which laws can be enforced. Please let Congress know that a national privacy law should not be used to hurt law enforcement, particularly now when surging violent crime rates and transnational criminal groups hurt all Americans.

Sincerely,

Larry Cosme
National President
Federal Law Enforcement Officers Association