Right on CRIME **Testimony**

July 19, 2022

Digital Dragnets:

Examining the Government's Access to Your Personal Data.

Testimony before the United State House of Representatives Committee on the Judiciary

by Brett Tolman, Executive Director

Thank you for the opportunity to testify today. My name is Brett Tolman, and I am the Executive Director of Right on Crime, a conservative organization dedicated to the promotion of criminal justice policies that promote public safety, individual liberty, and whole communities. I have previously served as the United States Attorney for the District of Utah, as an Assistant United States Attorney, and as Chief Counsel for Crime and Terrorism for the United States Senate Judiciary Committee. The past decade I have also worked in private practice as the founder of the Tolman Group, focusing on government reform, criminal defense, and internal corporate investigations, and previously as a Shareholder and Chair of the White Collar, Corporate Compliance and Government Investigations Section of the law firm of Ray Quinney & Nebeker, PC.

I am encouraged by the Committee's decision to hold a hearing to address concerns around law enforcements' warrantless access to commercially available "bulk data." These concerns are valid, and I share them.

The Fourth Amendment protects against warrantless searches and seizures.[1] It specifically protects:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment affords Americans an expectation of privacy with respects to their person and property, such that if law enforcement wishes to gain access to their personal records, they must first establish probable cause to secure a warrant which they make available to the individual subject to search.[2] The Supreme Court has ruled that a person's expectation to privacy under the Fourth Amendment follows them, not a place.[3] It ruled in *U.S. v. Jones* that "reasonable expectation of privacy in the whole of their physical movements."[4]

But what about an individual's digital footprint? Is there a reasonable expectation of privacy attached to bulk records containing an individual's digital record? Yes, and as such, the Fourth Amendment demands a warrant predicate access to this information.[5] [6]

The constant evolution of technology, and the digital footprints that individuals generate as a result, expose opportunities for end runs around the Fourth Amendment's privacy guarantees. Therefore, use of

[1] https://www.law.cornell.edu/constitution/fourth_amendment
[2] https://supreme.justia.com/cases/federal/us/389/347/
[3] Id.
[4] United States v. Jones, 565 U.S. 400 | Casetext Search + Citator
[5] https://casetext.com/case/smith-v-maryland#p740
[6] https://casetext.com/case/united-states-v-jones-1419#p406

technology by the government upon its citizens must be subject to constant scrutiny. The Supreme Court ruled in *Carpenter v. U.S.* that an "individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell site location information]" and that "[a]llowing government access to cell-site records contravenes that expectation" despite "records [having been] generated for commercial purposes."[7]
To that end, I am critical of the law enforcement practice of purchasing databases in bulk, which they then mine, or dare I say search, for incriminating information against unwitting citizens as violating the expectation of privacy guaranteed under the Fourth Amendment. This access by law enforcement of an individual's digital records and movements is purchased, rather than obtained via warrant as required by the Fourth Amendment. Americans' personal data is sold to law enforcement, unbeknownst to them, and for the purpose of investigating or surveilling them. This is a violation, plain and simple.

Congressional attention and oversight concerning the lack of transparency and basic information relating to law enforcement's access to an individual's digital movements must persist to ensure the rights of citizens are not sacrificed on the alter of technological innovation.

Last July, I testified before the Members of the Subcommittee on Crime, Terrorism, and Homeland Security regarding the lack of oversight and privacy concerns around law enforcement's use of facial recognition technology.[8] I noted my discomfort around the sources of the photos used in this practice. In addition to drawing on pictures secured through the criminal justice process, the government utilizes millions of photos of law-abiding individuals collected for driver's licenses and passports.[9] Private technology companies that contract with law enforcement harvest billions of photos posted by unsuspecting users on platforms such as Facebook, YouTube, and even Venmo.[10] This collection and data grab amounts to an unprecedented invasion of privacy that places enormous, undue control in the hands of the government and Big Tech, two entities not always known for their light touch or responsible use of power.

Mass surveillance compounds the issues surrounding mass collection. Walking out the door in the morning can be an exercise in skipping from one security or traffic camera to another, or one cell tower to another. Sending a text, making a call, or using an app can be subject to review by a government actor. In gaining access to this data, as Justice Roberts noted in *Carpenter*, law enforcement "achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[11] Just because law enforcement collects the data from a third party that maintained the same for commercial purposes, does not negate one's reasonable expectation of privacy when that data tracks their movement and location.[12]

Inevitably, law enforcement will default to reliance on unfettered access to digital records from third parties if permitted to bypass a warrant. They may do so touting laudatory uses, such as identifying missing persons, but a right abused for any reason is still an abuse and its expansion in use is inevitable.

Our Founding Fathers deliberately and prudently enshrined in the Bill of Rights proscriptions on the wanton search of Americans as a necessary bulwark for freedom. It is hard to square these notions and

[7] https://casetext.com/case/carpenter-v-united-states-67
[8] https://www.texaspolicy.com/wp-content/uploads/2021/07/2021-07-12-T-Tolman-ROC-Facial-Recognition-Hearing-US-HOR.pdf
[9] https://www.gao.gov/assets/gao-16-267.pdf
[10] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[11] https://casetext.com/case/carpenter-v-united-states-67
[12] Id.

protections with the unfettered access to digital records that can instantaneously reveal an individual's identity, location, communications, movements, and associations.

In addition to the Fourth Amendment concerns, there is a conversation to be had around the implications that such access to private information will have on the public's trust of law enforcement. Americans have long prided themselves on our ability to refuse the government unless it has legitimate cause to interfere with our liberty. Our police, at least in the absence of reasonable suspicion of wrongdoing or additional judicial process, are supposed to rely on the consent of the citizenry in their interactions. The unfettered power to mine personal information, with little public awareness or transparency, stands this principle on its head. Questions posed to an individual by law enforcement about their personal information become merely rhetorical. Law enforcement has already accessed all the information needed to track them. Americans are placed in a position where they must choose between the convenience and necessity of technology against their right to privacy from government surveillance.

Furthermore, we cannot ignore the risk that access to commercially available digital records without a warrant will be used to target certain Americans. Consider the chilling effect if the government could sidestep the probable cause necessary to obtain a warrant from the court, and simply purchase the data necessary to target an American or groups of Americans for surveillance. What protections are in place to ensure that targets are not politically motivated, or otherwise motivated in support of an agenda having nothing to do with public safety? This practice grossly lacks the necessary transparency and accountability.

Not long ago, I was tasked with leading the effort in the Senate to reauthorize the USA PATRIOT Act. We heard similar assurances years ago, by those leading the Department of Justice and the FBI about FISA and those surveillance authorities not being turned against honest Americans. We have seen how that worked out as outlined in the recent, and disturbing, Inspector General reports.

None of this is to say that there is not a legitimate purpose for access to digital records in order to guard against real threats to safety and security. However, in a country that values and ensures freedom from government intrusion, we must ensure access is transparent by predicating the same upon the acquisition of a warrant. One needs only to look no further than Russia's and China's unconscionable and unfettered control over the digital footprint of its citizenry, where no expectation of privacy exists, to appreciate the limitations the Fourth Amendment places upon government agencies in America.

It is unrealistic to expect law enforcement officials to permanently deny themselves access to information that is increasingly prevalent in the commercial sector and which has such powerful capacity to improve public safety. While I harbor a conservative's healthy skepticism of government, I respect members of law enforcement and will always seek to support them and their mission to keep us all safe. However, acknowledging there are credible uses for digital surveillance and voicing support for law enforcement is not the same as writing a blank check for power and then looking the other way.

Significant restraints might be necessary for privacy protections to catch up to the rapidly advancing capabilities of technology. As it stands, it is difficult to see how the regular, widespread access to commercially available, personal information can meet the high standards of our Constitution and its protection of civil liberties or the norms inherent in a democratic society. If one considers such access creating the ability to find a needle in a haystack, it seems entirely reasonable to demand the police to first

establish probably cause relevant to the needle they are looking for, rather than allow the purchase of all the haystacks in the off chance it contains a needle.

Americans deserve transparency as to the nature of law enforcements access to data held by third parties containing information for which they had a reasonable expectation to believe was private. We should have particular reticence when it comes to the collection of data obtained without a warrant. This is a pressing issue pertaining to all Americans' fundamental rights. As someone who has spent a great deal of time working on legislation in this arena and someone who fundamentally believes that smaller government is better government, I am encouraged that the Committee is concentrating its focus on these concerns today. I expect that its resolution will require many conversations, careful balancing of tradeoffs, and potentially difficult decisions. I look forward to contributing however I can to that effort today. Thank you once again, for the opportunity to present these concerns to the members of this Committee.

ABOUT THE AUTHOR

Brett L. Tolman is the founder of the Tolman Group and the executive director for Right on Crime. He is dedicated to state and federal policy and advocacy, especially on criminal justice reform. Prior to entering private practice, Tolman was appointed by President George Bush in 2006 as the United States Attorney for the District of Utah and held that office for nearly 4 years from 2006-2009. As U.S. Attorney for Utah, he was responsible for cutting-edge cases addressing such issues as international adoption fraud, mortgage fraud, international marriage fraud, sex and human trafficking, terrorism, and breaches of national security. In 2009 he handled the prosecution of Brian David Mitchell, the convicted kidnapper of Elizabeth Smart. From 2008-2009 he was selected by Attorney General Michael Mukasey to serve as special advisor to the attorney general on national and international policy issues affecting United States attorneys and the Department of Justice. Prior to his appointment as U.S. Attorney, Tolman served as chief counsel for crime and terrorism to the United States Senate Judiciary Committee. During his career, Tolman has testified multiple times in the United States Congress and assisted in drafting and passing many pieces of legislation affecting state and federal criminal justice systems. These include the First Step Act of 2018, the Corrections Act, the Sentencing Reform Act, the Justice for All Act of 2004, Protection of Lawful Commerce in Arms Act (2005), the Violence Against Women and Department of Justice Reauthorization Act of 2005, the USA Patriot Improvement and Reauthorization Act of 2005, and the Adam Walsh Protection and Safety Act (2006). He is a frequent contributor on Fox News, CNN, MSNBC, NewsMax and No Spin News with Bill O'Reilly.

About Right On Crime

Right On Crime is a national initiative of the Texas Public Policy Foundation supporting conservative solutions for reducing crime, restoring victims, reforming offenders, and lowering taxpayer costs.

Right On CRIME

901 Congress Avenue | Austin, Texas 78701 | 512.472.2700 | www.RightOnCrime.com