A HOOVER INSTITUTION ESSAY

Understanding Police Reliance on Private Data

FARHANG HEYDARI

Aegis Series Paper No. 2106

National Security, Technology, and Law

Introduction

Law enforcement investigations have always depended on information from private actors, including victims, witnesses, and informants. But modern technology and big data have transformed this analog process into an automated, digital one. What was once a practice of targeted data collection has turned into bulk data gathering—GPS and cell-site location information, biometric databases, license plate locations, and more.

This shift has elevated the role that private entities play in the investigative process. From the tech giants that transmit and store our communications and internet browsing history, to the data brokers that aggregate public records into detailed individual dossiers, private companies make decisions that can make or break criminal investigations. These choices include whether to oppose or accede to a government request for information, what data to collect, and how frequently it's deleted. Over time, these private decisions have come to define many aspects of our rights and liberties.

The growing role of private entities in law enforcement data collection mirrors the growth of private influence across the entire criminal system. Although most commonly associated with formal outsourcing, including private prisons and police, private influences pervade every stage of the criminal system. Private security guards make huge numbers of arrests; private surveillance devices and watch groups provide law enforcement with an array of critical information; proprietary technologies produce evidence admitted against the accused; algorithms influence bail and sentencing determinations; incarceration and alternatives-to-incarceration programs are administered by private entities.

Many of these private influences have been fiercely criticized. There is robust scholarship documenting the inherent difficulties with governing private actors in the criminal system. These critiques range from lack of transparency and legal accountability for private actors, to their perverse financial incentives. This criticism has been so sustained that many now instinctively oppose any role for private actors in the criminal system.

Although there is merit to these concerns, blanket opposition to any role for private actors in the criminal system is not a sound policy-making approach. For one thing, it is impractical. Government will always need the private sector—to outsource production of certain goods (e.g., vehicles, body cameras), to provide information relevant to investigators, and more. But more importantly, as discussed below, public actors can raise many of the same concerns as private actors, and there are even occasions when private actors can help moderate the harmful impact of public actors.

The challenge is for policy makers to distinguish beneficial private influences from harmful ones. In this paper, I suggest one way for policy makers to approach this task: focusing on the private entities with the closest relationship—contractual, financial, and otherwise—to law enforcement, for these entities have fewer incentives to guard against law enforcement overreach.

This paper has three parts:

Part I examines the debate around privatization in the criminal system, arguing that private actors are not as uniformly problematic as the privatization debate would suggest. Indeed, public actors can exhibit the same flaws, and private actors can sometimes mitigate the harm caused by the criminal system.

Part II turns to law enforcement's access to the private data market, arguing there can be benefits to law enforcement accessing sensitive data through private actors.

Part III suggests that in order to realize these benefits and guard against harms, regulators should focus on private entities that have particularly close relationships with law enforcement. These entities are least likely to push back against law enforcement and instead are more likely to become a private extension of law enforcement. Requiring these entities to register and to provide insight into their collection practices is an important step toward a more effective regulatory structure.

I. Private Influences on the Criminal System

Private actors and entities play key roles at every stage of the criminal process.[1]

Often these influences take the form of formal privatization—government contracting out for goods and services. For example, private companies under contract with federal, state, and local governments operate prisons, jails, immigrant detention centers, halfway houses, drug treatment facilities, and many other aspects of the corrections systems. In the process, these companies make important policy decisions, from those relating to internal discipline to the fees they charge incarcerated individuals.

But there are also many ways in which private entities influence the criminal system without any formal privatization. Consider the impact of a member of the public calling the police. The country has seen countless viral videos of individuals calling the police on people of color who are going about their daily lives—walking their dogs, shopping in a deli, barbequing in the park, watching their child play soccer, boating, and generally existing in public spaces.[2] The consequences of any particular call can be emotional trauma, arrest, or even death for the target of the call. But at scale, calls for service have an even more dramatic impact. Big retailers like Walmart generate a volume of calls that can turn police into a private security force.[3] Studies have shown that calls to police in gentrifying neighborhoods generate more arrests for offenses like loitering and disorderly conduct, and more proactive policing for drug and alcohol offenses.[4] Such enforcement can inflame tensions, exacerbate gentrification, and make longtime residents feel unwelcome.[5] None of this is "privatization" per se, but these private actions have profound consequences on the criminal system.

The influence of private actors on the criminal system has fierce critics. Opposition is particularly sustained around the broader prison-industrial complex, including privatized bail, detention, probation, and more.[6] But there is also widespread criticism of private police, the privatization of prosecutorial services, and the increasingly influential role of policing technology companies.[7]

The critiques of privatization are varied, but many focus on the governance difficulties that arise when private actors operate in the criminal system. These critiques typically fall into four categories:

1. Unlike public officials, private actors are not *democratically accountable* to the public.

2. Private actors are not *transparent* because traditional mechanisms of government transparency—open records and sunshine laws, notice-and-comment procedures, and criminal discovery rules—do not impose the same obligations on private actors.

3. Private actors are more difficult to hold *legally accountable*, primarily because constitutional rules do not apply to them.[8]

4. A private actor's *profit motives* will distort decision making in a way that harms the public.

Although these concerns are valid in particular contexts, an automatic opposition to *all* private influences is overbroad in two directions:

First, public actors are subject to many of the same governance concerns as private entities.

Consider, for example, the influence of profit motives and financial incentives on public actors in the criminal system. Although public officials do not have shareholders, they too have financial incentives that can distort their decisions. Government addiction to fines, fees, and asset forfeiture is a clear example. As of 2017, ten million people owed more than $50 billion for everything from traffic fines to court fees.[9] In some places, fines and fees account for most of the local budget,[10] plugging shortfalls and helping local leaders avoid tough budget choices.[11] Forfeiture laws have allowed law enforcement to seize and retain billions of dollars from people suspected of criminal activity without bringing formal charges.[12] Because forfeiture funds are generally spent outside of the budgeting process, they can fund a variety of off-the-books initiatives and splurges.[13] As a result, fines, fees, and forfeiture opportunities can dictate enforcement priorities.[14] In short, government actors can be as susceptible to profit motives as their private counterparts.

Second, there are ways that private actors might actually improve the public system, such as by increasing transparency and improving the legal accountability of the system.

Consider, for example, concerns around policing transparency. Private entities are not subject to formal transparency mechanisms such as open records laws, but the private sector has improved police transparency in important ways. For example, although we now take for granted that police will report crime data, this only became a reality after the federal government called for investment and partnerships with the private sector to make crime mapping technology widely available.[15] Body cameras followed a similar course, with strong federal support from the Obama administration and private industry stepping in to fill the gap. It's hard to imagine these tools being developed or widely adopted without private industry. Private companies have also built features that automatically create documents or audit trails, making those documents Freedom of Information Act ready. And the very presence of private actors can bring transparency to government conduct. There are private groups that organize court-watching or cop-watching efforts to bring greater visibility to how the criminal system functions.[16] These are examples of private influences facilitating government transparency.

Privatizing aspects of the criminal system can also promote legal accountability. Most private sector actors in the criminal system are at-will employees, meaning that many public sector hurdles to discipline such as union contracts and civil servant protections—well-documented obstacles to individual accountability in the policing and prisons context—do not apply. The private sector can also be more responsive to market pressures because customers can choose to take their business elsewhere (an option members of the public do not always have with their local police or prosecutors, for example).[17] Finally, some private industries have implemented their own accountability mechanisms, such as ethics boards and whistleblower protections.[18] These mechanisms are particularly prominent around emerging technologies, where government regulation is notoriously slow.[19]

In short, although there are reasons to be wary of the role of private actors in the criminal system, a knee-jerk opposition to any reliance on private actors goes too far. Public officials are vulnerable to many of the same concerns raised by privatization, such as a lack of transparency and financial motives. And there are times when private actors can improve the governance of public actors.

These lessons are directly applicable to law enforcement's reliance on privately held data.

II. Law Enforcement's Access to the Private Data Market

Like the role of private actors in the criminal system generally, their role in law enforcement data collection is complex.

Many scholars and advocates have raised important concerns about the dangers of law enforcement's access to the private data market. Unbeknownst to most of us, private entities of all sorts collect and store vast amounts of our personal data. By tapping into these reservoirs of data, law enforcement can obtain far more information about us than they could possibly capture directly, and they do so without many traditional constitutional safeguards.[20] This expansive access presents grave risks to individual privacy and security against government overreach. History demonstrates that this overreach is likely to be directed toward the same racial and ethnic groups that bear the brunt of overpolicing. There is also concern these tools will be turned against journalists, political dissidents, and others engaged in protected First Amendment expression.

I am sympathetic to many of these arguments. In my view, they present a compelling argument for comprehensive regulation of law enforcement access to electronic data. As law enforcement increasingly relies on the private data market, legal asymmetries between privately and publicly collected data make less and less sense. The Supreme Court acknowledged as much in the context of location information derived from our cell phones. In *Carpenter v. United States*, the Court established a warrant requirement for location tracking via private cell-site location data.[21] In doing so, it began to move toward parity for data directly obtained by law enforcement and data obtained from private third parties.[22] Some jurisdictions have begun legislating this type of parity by limiting law enforcement's access to data whether initially collected by a policing agency or a private entity. In Utah, for example, government entities may not use privately captured automated license plate reader (ALPR) data without a warrant or court order, unless the private entity retains ALPR data for 30 days or fewer.[23]

Although there is much more one could say about the need for improved governance around law enforcement data collection via private actors, in this section, I outline circumstances under which private actors might actually bring certain governance benefits. In particular, I consider the possibilities of (1) separation-of-powers benefits, (2) transparency benefits, and (3) distributional benefits.

A. Separation-of-Powers Benefits

When law enforcement maintains its own databases, there are few barriers to accessing the data. Querying a government-maintained warrant database, a DNA database, or a license-plate reader database, for example, does not require judicial authorization. When law enforcement has direct access to camera infrastructure, they can monitor the cameras in real time, run advanced analytics like facial recognition, and store the data indefinitely. The results of unfettered law enforcement access to its own databases are well documented—officers have accessed the data for personal purposes; used it to target racial, ethnic, and political minorities; and so on.[24]

But when private entities are the data custodians, they can act as guardians, creating something akin to separation-of-powers protections that other branches of government have largely abdicated.[25] Particularly since the Snowden revelations about the National Security Agency, the largest technology companies have pushed back against law enforcement data requests. Apple famously opposed court orders to hack its iPhones in connection with the terrorist shooting in San Bernardino.[26] Other companies require warrants rather than subpoenas before turning over customer data.[27] Microsoft challenges secrecy orders attached to search warrants.[28]

B. Transparency Benefits

Closely related to potential separation-of-powers benefits are transparency benefits. When law enforcement maintains its own database, the public is often left with little information about the contents of the database or how law enforcement uses it. Take law enforcement fusion centers. Growing out of the perceived information-sharing failure of the 9/11 attacks, there are now about eighty of these centers across the country.[29] Their role is to aggregate and disseminate data among law enforcement agencies. What we know about these centers comes out in dribs and drabs, often from confidential documents and whistleblowers. Because these centers largely operate in the dark, it should be no surprise that they have repeatedly targeted people based on political ideology.[30]

When law enforcement is forced to turn to private data holders, there at least is potential for greater transparency. Google, Facebook, and other companies voluntarily publish semiannual reports on the breadth of law enforcement requests they receive—these are insights we'd never have if law enforcement was left to its own devices. Ring now publishes the content of all law enforcement video requests—obviating the need for cumbersome open records requests. Axon builds audit trails into its Tasers and body cameras—though the onus remains on communities to request this information. (Of course, as I discuss in more detail in the final section, there are times when policy makers must do more to force transparency from private actors.)

C. Distributional Benefits

A third potential advantage of private databases is that these can be less likely to replicate law enforcement biases. Take DNA databases as an example. Government-operated DNA databases are generated from individuals who encountered law enforcement—mostly people arrested for or convicted of a felony but also victims and people who plead to low-level misdemeanors.[31] These databases replicate the biases that exist in policing generally. Although there is little public data on the demographic profiles of these databases, scholars estimate that DNA profiles from Black people are collected at two to three times the rate of white people.[32]

But because private databases are sourced differently than law enforcement databases, they do not necessarily reflect these same law enforcement biases. For example, the nearly 30 million DNA profiles contained in Ancestry.com's and 23andMe's commercial databases actually have a disproportionate share of the country's white population—the same folks who are less likely to be captured in public (criminal) DNA databases.

Similar dynamics exist in other contexts. Although most law enforcement agencies run facial recognition searches against mugshot databases—which reflect the racial and socioeconomic disparities in criminal enforcement—private facial databases are often sourced from the internet and social media, which capture wide swaths of the population. As another example, law enforcement's license plate databases are populated in part by data generated from readers on police patrol vehicles. These vehicles spend a disproportionate amount of time in minority neighborhoods.[33] But when private individuals or associations purchase ALPRs, they target their own wealthier and whiter neighborhoods.

• • •

I do not suggest that these benefits are universal among private databases; nor do I argue that commercial databases do not come with their own downsides. But instead of automatically eschewing private data markets or embracing them, policy makers should regulate in ways that account for the complex interplay between the public and private spheres, avoid regulatory gaps, and take the best of both systems.

III. Focusing Governance on Law Enforcement Enablers

There is no shortage of companies that sell and share data with law enforcement. Some have made a business out of the practice (Venntel, Vigilant Solutions, Flock Safety). Others share information with law enforcement only in response to legal demands (Facebook, Google). And others fall somewhere in between (Ring). As described in the first part of this paper, these private actors give rise to real governance concerns, but as explained in the second part, there are also potential benefits. The question then, is how can policy makers distinguish the beneficial aspects from the harmful ones?

There is no simple or single answer to this calculus, but this section suggests a few guiding principles focused on improving governance.

A. Focus on Entities with Close Law Enforcement Ties

Although there are many aspects of law enforcement data collection that warrant close attention from regulators, when it comes to the role of private actors, lawmakers should begin with those entities that have particularly close relationships with law enforcement.

Financial incentives can shape the data private entities gather and the circumstances under which they share data with law enforcement. Thomson Reuters, for example, has profited enormously from selling law enforcement access to its CLEAR database.[34] This relationship with law enforcement encourages the company to collect more data in CLEAR, and to enhance its search capabilities. Motorola Solutions, in its effort to provide "the only end-to-end public safety ecosystem,"[35] continues to expand the data services it offers—including its recent acquisition of the nation's largest shareable database of vehicle location information,[36] its incorporation of facial recognition search technologies, and its "own exclusive database" of facial images.[37] Companies with such close relationships to law enforcement are incentivized to reduce points of friction and make data collection and access as seamless as possible.

In contrast, private entities that do not profit directly from law enforcement operate with different incentives. Although these companies have their own profit motives to harvest our data, they have less reason to build their data collection practices and access policies around law enforcement needs. Google, for example, while profiting tremendously from user data, does not sell access to law enforcement. Google turns over the data of tens of thousands of users a year, but it does so in response to specific legal process. This process is far from perfect, and Google could do more to oppose overly broad requests, but at least Google creates points of friction to minimize the user data it shares and files transparency reports.[38] These processes are a far cry from the bulk collection and access that Thomson Reuters provides. And when companies do not rely on police coffers for revenue, they can push back on law enforcement requests: Apple, referenced earlier, used its refusal to comply with the FBI's request to hack iPhones as a marketing opportunity.[39]

In short, private entities with close relationships to law enforcement are not incentivized to perform separation-of-powers functions and are more likely to serve as an extension of law enforcement.[40] They are likely to take steps toward reducing friction and accommodating law enforcement at every turn. This is where regulators should focus their attention.

B. Operationalizing This Line

But how to operationalize this line? How to define those entities with sufficiently close ties to law enforcement to warrant additional regulatory scrutiny?

The web of law enforcement data collection is complicated, and any regulation must account for this complexity. Entities large and small share data with law enforcement. Some do so to make a profit while others do not. Some share data they own; others share data owned by others.

Although it might sound simple enough to regulate all entities that provide access to or share data with law enforcement agencies, this definition would sweep in entities that provide data in response to legal process, such as a local business that responds to a subpoena or warrant. The key is to target those instances of law enforcement access to privately held data that are most susceptible to abuse.

To that end, policy makers ought to focus on two types of entities:

First, lawmakers should include private entities that provide law enforcement with access to data under a formal contractual arrangement or in exchange for compensation. These entities include some of the most invasive examples of law enforcement access to the private data market, including large data brokers that aggregate public information into individual dossiers (Thomson Reuters, LexisNexis); bulk purchasing of cell phone location information (Venntel); access to massive troves of geotagged license plate reads (Vigilant Solutions, NVLS); and access to a variety of biometric databases, including faces (Clearview AI), iris scans (BI2 Technologies), and DNA profiles (DNASolves).

It is important to expansively define the types of contracts and compensation that qualify. There are many vendors that provide law enforcement with free access to a product on a trial basis not under formal contracts, but under more general memorandums of understanding and terms of service.[41] There are vendors that receive compensation in the form of user data added to their database, rather than financial compensation.[42]

Second, lawmakers should include private entities that facilitate law enforcement access to “crowdsourced” data—that is, data provided by private individuals and aggregated or shared by a third-party entity. Law enforcement has long relied on private individuals to conduct surveillance and share information, but private entities have recently augmented this process. Crime Stoppers offers cash rewards for information and claims to have contributed to over 800,000 arrests, including over 14,000 homicides.[43] Technology companies offer members of the public (and businesses) ways to install sophisticated surveillance equipment and share the captured data directly with law enforcement. Flock Safety allows homeowners’ associations and other private entities to purchase ALPRs and to share the data they generate in bulk with local law enforcement. Ring has created a service (Neighbors Public Safety Service) by which law enforcement agencies can request video from community members. In these cases, neither Ring nor Flock is selling directly to law enforcement and often lack any formal contractual relationship. And yet, policy makers would do well to understand the types of lateral surveillance devices in use in their communities, and how law enforcement accesses that data.

To avoid overregulation, lawmakers should consider certain exemptions. For example, they might exempt entities that share only in response to mandatory legal process (search warrants, national security letters). This regulation could also exempt entities whose financial relationship with law enforcement falls below a minimum dollar threshold. A threshold exemption would avoid sweeping in small entities or individuals that take subpoena or witness fees for responding to government requests and has precedent in a variety of other contexts.[44]

C. Requiring Registration

How a jurisdiction ultimately regulates entities with close law enforcement ties will depend on the political realities of that jurisdiction. In this section, I suggest modest registration requirements designed to provide policy makers with a fuller understanding of how law enforcement uses the private data market.[45] A registration requirement would not substantively restrict law enforcement's use of the private data market, but would move its use into public view, allowing policy makers and communities to determine whether greater regulation is warranted.

Data providers with sufficiently close ties to law enforcement should be required to register and disclose at least the following sorts of information:

- The entity's name and contact information, including information on any subsidiaries or parent corporation with access to the data at issue

- A description of the data the entity collects, stores, or transfers

- A description of the source of the data and how it is obtained

- Whether the entity has a direct relationship with the subjects of the data (or whether the data is obtained via a third party) and whether (and how) the subjects of the data had the opportunity to opt out at the time of collection

- Whether the entity applies any analytic tools to the data, including AI or machine-learning based algorithms

- A list of all government agencies with which the entity has shared data and the nature of that data
- Total revenue from data sharing with government agencies, including both direct compensation from government entities and private funding on behalf of government entities
- The terms under which the data was shared, including whether the data was shared in response to legal process, under contract, or in exchange for compensation
- A copy of any contract or terms of service under which data is shared with law enforcement
- The entity's data security practices, including whether the entity has suffered any data breaches

A robust registration statute would, of course, include additional provisions, such as requirements to state the relevant information "in a concise, transparent, intelligible and easily accessible form, using clear and plain language,"[46] and penalties for failure to comply (such as civil liability or a private right of action).[47]

Conclusion

Law enforcement's collection of electronic data remains woefully underregulated. This is particularly so when private third parties are involved. As courts continue to play catch up, there is a desperate need for regulators to enter the fray. In this paper I suggest a modest first step—rather than turning away from any involvement by private actors, or leaving them entirely unregulated, I suggest a registration process that aims to bring transparency to those private entities that are most likely to serve as an extension of law enforcement.

ACKNOWLEDGMENTS

My sincerest thanks to the participants of the Hoover Institution's National Security, Technology, and Law Working Group for their thoughtful feedback. In particular, thanks to Barry Friedman, Jack Goldsmith, and Andrew K. Woods.

NOTES

[1] The arguments in this section are part of a broader forthcoming project. *See* Farhang Heydari, *The Private Role in Public Safety*, 90 Geo. Wash. L. Rev. (forthcoming 2022).

[2] *See* Chan Tov McNamarah, *White Caller Crime: Racialized Police Communication and Existing While Black*, 24 Mich. J. Race & L. 335, 337–41 (2019) (collecting examples).

[3] Seth W. Stoughton, *The Blurred Blue Line: Reform in an Era of Public & Private Policing*, 44 Am. J. Crim. L. 117, 139 (2017).

[4] *See, e.g.*, Brenden Beck, *Policing Gentrification: Stops and Low-Level Arrests during Demographic Change and Real Estate Reinvestment*, 19 City & Community 245, 249 (2020); Olatunde C.A. Johnson, *Unjust Cities? Gentrification, Integration, and the Fair Housing Act*, 53 U. Rich. L. Rev. 835, 846 (2019).

[5] *See* Devon W. Carbado, *Blue-on-Black Violence: A Provisional Model of Some of the Causes*, 104 Geo. L.J. 1479, 1495 (2016).

[6] *See, e.g.*, Angela Y. Davis, *Are Prisons Obsolete*? 84–85 (2003); Patrice A. Fulcher, *Hustle and Flow: Prison Privatization Fueling the Prison Industrial Complex*, 51 Washburn L.J. 589, 599 (2012); Sharon Dolovich, *State Punishment and Private Prisons*, 55 Duke L.J. 437, 449 (2005); Ahmed A. White, *Rule of Law and the Limits of Sovereignty: The Private Prison in Jurisprudential Perspective*, 38 Am. Crim. L. Rev. 111, 144 (2001); Chris Weaver & Will Purcell, Comment, *The Prison Industrial Complex: A Modern Justification for African Enslavement?*, 41 How. L.J. 349, 353 (1998).

[7] Regarding privatization of police, *see, e.g.*, Heidi Boghosian, *Applying Restraints to Private Police*, 70 Mo. L. Rev. 177 (2005). *But see* Elizabeth E. Joh, *Conceptualizing the Private Police*, 2005 Utah L. Rev. 573, 596. Regarding privatization of prosecution, *see, e.g.*, Roger A. Fairfax, Jr., *Outsourcing Criminal Prosecution?: The Limits of Criminal Justice Privatization*, 2010 U. Chi. Legal F. 265 (2010). *See also* Benjamin Levin, *Criminal Employment Law*, 39 Cardozo L. Rev. 2265, 2314 (2018).

[8] The private search doctrine, for example, allows law enforcement to conduct a warrantless search when a warrant would normally be required, merely because a private party has already conducted the search. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109 (1984). The third-party doctrine allows law enforcement to access information about us that has been exposed to third parties. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979).

[9] Karin D. Martin et al., *Shackled to Debt: Criminal Justice Financial Obligations and the Barriers to Re-entry They Create*, *in* New Thinking in Community Corrections 5 (Jan. 2017), https://www.ncjrs.gov/pdffiles1/nij/249976.pdf. *See generally* Neil L. Sobol, *Charging the Poor: Criminal Justice Debt & Modern-Day Debtors' Prisons*, 75 Md. L. Rev. 486 (2016).

[10] *See generally* Mike Maciag, *Addicted to Fines: Small Towns in Much of the Country Are Dangerously Dependent on Punitive Fines and Fees*, Governing (Aug. 19, 2019), https://www.governing.com/archive/gov-addicted-to-fines.html.

[11] *See, e.g.*, John D. King, *Privatizing Criminal Procedure*, 107 Geo. L.J. 561, 562 (2019); Brief for the American Civil Liberties Union et al. as Amici Curiae Supporting Petitioners at 7, *Timbs v. Indiana*, 139 S. Ct. 682 (2019) (No. 17-1091).

[12] *See generally* Dick M. Carpenter II et al., Institute for Justice, Policing for Profit: The Abuse of Civil Asset Forfeiture (2nd ed. 2015); *see also* Leonard v. Texas, 138 S. Ct. 1448 (2017) (Thomas, J., dissenting from denial of certiorari).

[13] *See, e.g.*, Carpenter, *supra* note 12, at 7, 39–41; Marian R. Williams et al., Inst. for Justice, Policing for Profit: The Abuse of Civil Asset Forfeiture 15–20 (1st ed. 2010).

[14] David Pimentel, *Forfeitures Revisited: Bringing Principle to Practice in Federal Court*, 13 Nev. L.J. 1, 31 (2012); *see also* U.S. Dep't of Justice, Investigation of the Ferguson Police Department 4–5 (Mar. 2015); Alexandra Natapoff, Punishment without Crime: How Our Massive Misdemeanor System Traps the Innocent and Makes America More Unequal at chpt. 5 (2018).

[15] *See* Erik Luna, *Transparent Policing*, 85 Iowa L. Rev. 1107, 1164–65 (2000).

[16] *See* Jocelyn Simonson, *The Criminal Court Audience in a Post-Trial World*, 127 Harv. L. Rev. 2173, 2177–200 (2014). *See generally* Jocelyn Simonson, *Copwatching*, 104 Cal. L. Rev. 391 (2016).

[17] *See* Jody Freeman, *Private Parties, Public Functions and the New Administrative Law*, 52 Admin. L. Rev. 813, 818–19 (2000); *see also* Alexander Volokh, *Privatization and the Elusive Employee-Contractor Distinction*, 46 U.C. Davis L. Rev. 133, 149–151 (2012).

[18] Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. Rev. 54, 108 (2019); *Axon AI Ethics Board*, https://www.axon.com/company/ai-and-policing-technology-ethics (last visited Aug. 6, 2021).

[19] *E.g.*, *Axon AI Ethics Board*, *supra* note 18.

[20] *See, e.g.*, Orin S. Kerr, *Buying Data and the Fourth Amendment* (Hoover Working Group on Nat'l Sec., Tech., and Law, Aegis Series Paper) (forthcoming 2021); Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third-Party Rights in Mass, Suspicionless Searches of Consumer Databases* (Hoover Working Group on Nat'l Sec., Tech., and Law, Aegis Series Paper) (September 23, 2021).

[21] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[22] *Id.* at 2217 ("Whether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements. . . ."); *id.* ("Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location.").

[23] Automatic License Plate Reader System Act, Utah Stat. tit. 41, § 6a-2005(4) (2014). ALPRs are devices that capture the times, location, and image of every license plate that passes within their view. *See generally* The Axon AI & Policing Ethics Bd., Second Report of the Axon AI & Policing Technology Ethics Board: Automated License Plate Readers (Oct. 2019).

[24] *See, e.g.*, Van Buren v. United States, 141 S. Ct. 1648 (2021); Joanne Cavanaugh Simpson & Marc Freeman, *South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors. Is That Legal?*, South Florida Sun Sentinel (June 26, 2021), https://www.sun-sentinel.com/local/broward/fl-ne-facial-recognition-protests-20210626-7sll5uuaqfbeba32rndlv3xwxi-htmlstory.html; Sam Stanton et al., *More Than 1,000 California Police Accessed Background Check Database for Personal Use*, Sacramento Bee (Nov. 14, 2019), https://www.sacbee.com/news/investigations/article237091029.html; Sadie Gurman, *Across US, Police Officers Abuse Confidential Databases*, AP (Sept. 28, 2016), https://apnews.com/article/699236946e3140659fff8a2362e16f43.

[25] *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 Stan. L. Rev. 99, 105 (2018) ("By entrusting our data processing and communications to a handful of giant technology companies, we've created a new generation of *surveillance intermediaries*: large, powerful companies that stand between the government and our data and, in the process, help constrain government surveillance.") (emphasis in original).

[26] Apple Inc's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance, *United States v. in the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, 5:16-cm-00010 (C.D. Cal. filed on Mar. 3, 2016), https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf.

[27] Ring, for example, requires formal legal process or certain exigent circumstances before turning over customer videos. *See Ring Law Enforcement Guidelines*, https://support.ring.com/hc/en-us/articles/360001318523-Ring-Law-Enforcement-Guidelines (last visited Aug. 6, 2021).

[28] *E.g.*, First Amended Compl. for Declaratory Judgment, *Microsoft Corp. v. U.S. Dep't of Justice*, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 2:16-cv-00538).

[29] U.S. Dep't of Homeland Security, Fusion Center Locations and Contact Information, https://www.dhs.gov/fusion-center-locations-and-contact-information (last visited Sept. 7, 2021) (listing 80 "primary" and "recognized" fusion centers).

[30] *See, e.g.*, Will Parrish & Jason Wilson, *Revealed: Anti-terror Center Helped Police Track Environmental Activists*, The Guardian (Oct. 2, 2019), https://www.theguardian.com/us-news/2019/oct/02/oregon-pipelines-protests-monitoring-police-anti-terror-unit; Curtis Waltman, *DAPL Fusion Center Reports Illustrate Everything Wrong with Fusion Centers*, Muckrock (Aug. 9, 2017), https://www.muckrock.com/news/archives/2017/aug/09/dapl-threat-assessment-ii/; *Documents Show Boston's "Antiterrorism" Fusion Center Obsessively Documented Occupy Boston*, Privacy SOS (May 25, 2014), https://privacysos.org/blog/documents-show-bostons-antiterrorism-fusion-center-obsessively-documented-occupy-boston; Amanda Peacher, *Why Is the State of Oregon Conducting Intelligence Work?*, OPB (Apr. 26, 2016), https://www.opb.org/news/article/oregon-department-of-justice-intelligence.

[31] *See, e.g.*, Jordan Smith, *Orange County Prosecutors Operate "Vast, Secretive" Genetic Surveillance Program*, The Intercept (July 3, 2021), https://theintercept.com/2021/07/03/orange-county-prosecutors-dna-surveillance.

[32] *See* Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 Cal. L. Rev. 1847, 1851 (2020).

[33] *See* Dave Maass & Jeremy Gillula, *What You Can Learn from Oakland's Raw ALPR Data*, Elec. Frontier Found. (Jan. 21, 2015), https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data.

[34] *See* Drew Harwell, *ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations*, Wash. Post (Feb. 26, 2021), https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data (pricing the Immigration and Customs Enforcement contract for CLEAR access at $21 million).

[35] Motorola Solutions, Law Enforcement Radio Technology and Software, https://www.motorolasolutions.com/en_us/solutions/law-enforcement.html (last visited Aug. 6, 2021).

[36] Ben Miller, *Motorola Solutions Buys Major License-Plate-Reading Company*, Govtech Biz (Jan. 14, 2019), https://www.govtech.com/biz/motorola-solutions-buys-major-license-plate-reading-company.html.

[37] Motorola Solutions, Vigilant FaceSearch Identity Matching and Verification (Dec. 2020), https://www.motorolasolutions.com/content/dam/msi/docs/products/license-plate-recognition-systems/reaperhd-mobile-lpr-system/vigilant-facesearch-fact-sheet.pdf.

[38] *See, e.g.*, Brief for Google LLC as Amicus Curiae Supporting Neither Party Concerning Defendant's Motion to Suppress Evidence from a "Geofence" General Warrant at 11–12, *United States v. Chatrie*, No. 3:19-cr-00130 (E.D. Va. Dec. 23, 2019) (describing "a [three]-step anonymization and narrowing protocol" for when Google responds to a geofence warrant); Google LLC, Global Requests for User Information, https://transparencyreport.google.com/user-data/overview?hl=en (last visited Aug. 6, 2020).

[39] Apple Inc., Privacy, https://www.apple.com/privacy/government-information-requests/ (last visited Aug. 6, 2020).

[40] For example, since Apple has refused to cooperate with the FBI, other law-enforcement aligned companies like GrayKey and Cellebrite, which rely on law enforcement for revenue, have stepped in to offer their own hacking services. *See* Thomas Brewster, *An Israel-U.S. Merger Creates an Apple Hacking Powerhouse for the Feds*, Forbes (Jan. 14, 2020), https://www.forbes.com/sites/thomasbrewster/2020/01/14/an-israel-us-merger-creates-an-apple-hacking-powerhouse-for-the-feds/?sh=4ffd8d361579.

[41] *See, e.g.*, Clearview, Inc., Clearview Terms of Service, https://staticfiles.clearview.ai/terms_of_service.html (last visited Aug. 6, 2020).

[42] Elec. Frontier Found., Street-Level Surveillance, https://www.eff.org/pages/iris-recognition (last visited Aug. 6, 2020) ("The vendor BI2 offered these sheriffs free three-year trials of its stationary iris capture devices to be used in inmate intake facilities. . . . The scans will be added to BI2's private database, which already has close to a million iris scans collected from over 180 law enforcement jurisdictions across the country.").

[43] Crime Stoppers USA, Current Statistics, https://www.crimestoppersusa.org (last visited Sept. 3, 2021).

[44] Examples include certain conflict-of-interest laws (*e.g.*, 42 C.F.R. § 50.603), state and federal lobbying rules (*e.g.*, Section 4(a)(3) of the Lobbying Disclosure Act (LDA)), and more.

[45] California and Vermont have taken this approach with data brokers. *See, e.g.*, Cal. Civ. Code § 1798.99.80 (2019); Vt. Stat. Ann. tit. 9, § 2430 (2018). The FTC has called for one at the federal level. *See* Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[46] *See* General Data Protection Regulation 2016/679, art. 12, cl. 1, 2016 O.J. (L 119) 39 (EU).

[47] *See, e.g.*, Vt. Stat. Ann. tit. 9, § 2430 (2018).

The views expressed in this essay are entirely those of the author and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

hoover.org

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Farhang Heydari, *Understanding Police Reliance on Private Data*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2106 (October 7, 2021), available at https://www.lawfareblog.com/understanding-police-reliance-private-data.

About the Author

David Kidd/Government Technology

FARHANG HEYDARI

Farhang Heydari is the executive director of the Policing Project and an adjunct professor of law at New York University School of Law. He has previously taught courses at Columbia Law School. Before joining the Policing Project, he was a civil rights litigator at Neufeld, Scheck & Brustin LLP.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams/national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION