A HOOVER INSTITUTION ESSAY

A Gig Surveillance Economy

ELIZABETH E. JOH

Aegis Series Paper No. 2108

Introduction

Eighteen years ago, the *New York Times Magazine* reported on a proposed online project aimed at protecting the country's forty-seven thousand strategic facilities, including oil pipelines, power stations, and dams. How do you protect such a vast network of sites vulnerable to sabotage, with limited government resources and personnel? The answer: pay freelance "spotters" eight to ten dollars an hour to check pictures sent to their home computers in order to answer the question, "Do you see a person or vehicle in this image?"[1] A confirmed positive sighting would prompt a law enforcement response in "less than 30 seconds."[2] This is an early version of a phenomenon identified and discussed in this essay: a gig surveillance economy.

Massive amounts of our personal information are out there for willing buyers. Nearly every aspect of our online activity is subject to collection, analysis, and sale. In the physical world, our movements and faces are easily captured and can be identified with increasing accuracy. Some of this information has been retrieved through illegal means, but much of it has been procured lawfully. For law enforcement agencies, purchasing information rather than collecting it directly provides another advantage. Direct government collection of data traditionally considered unprotected—such as public movements—draws questions about whether that information deserves heightened legal protection when collected at a mass scale. But by purchasing that same information in the private market, the government can sidestep these controversies. Government purchase of information already collected by a third party does not today implicate individual Fourth Amendment protections.[3]

When the government acts as a buyer in the private marketplace of personal information, however, it also shapes the market's response. The government is not just another customer. Because of its size, the government can be a profoundly influential one, sometimes in unexpected ways. Its very existence as a customer for information may give rise to new forms of surveillance capitalism that extend beyond the purchase of already-captured information.[4]

One such consequence is the rise of gig surveillance work, defined here as short-term, freelance, temporary surveillance that generates data later sold for profit.[5] This gig surveillance economy (a) mimics the temporary, platform-mediated work we see in rideshares and food and package delivery; (b) involves information collection with cheap and networked tools; and (c) requires no specialized skills.

Gig surveillance work requires few changes to the existing political economy of temporary, on-demand, freelance labor.[6] Uber and DoorDash drivers are pervasive; why not equip them with license plate readers? Instacart and Postmates shoppers are everywhere; why not give them body cameras? Most of us willingly identify pictures online as part of CAPTCHA tests;[7] why not offer payment for the same task? And while the need for gig surveillance work may one day be rendered obsolete with the introduction of smart cities[8] and other forms of automated surveillance built into our infrastructure, in the short term it fills a need and raises concerns about policy and law that have yet to be addressed. Every element necessary for gig surveillance work already exists, and conditions are ripe for its flourishing. The production of surveillance data is already a by-product of conventional gig work. What we can expect is the further development of gig work for the sake of surveillance itself. This essay describes gig surveillance work, what potential legal and policy questions it raises, and what it means for the further entrenchment of government reliance on the private information market.

Origins

The emergence of gig surveillance work should not surprise us. We can identify many institutional and cultural factors that facilitate low-wage, on-demand, temporary workers' assumption of the task of mass surveillance for the information marketplace.

Well before the introduction of the internet, platforms, and artificial intelligence, private policing services flourished in the United States to complement and sometimes to rival public policing.[9] Public police departments with uniformed officers emerged relatively late in American history, with the first urban departments established by the mid-1800s. In the era before these "new" police became the norm, private alternatives such as constables performed criminal-justice services that defied easy public or private categorization.[10] Victims of stolen property, for instance, could turn to constables for help—for a fee.[11] Even after public police departments arose, private services for crime control did not disappear. Businesses and individuals alike could turn to private police services for extra protection or personalized services. That remains true today. The numbers of those employed in private security services far exceeds the rolls of public police departments.[12]

Private investigation has often been associated with some special set of skills, acquired either through experience or training. To be sure, there are tens of thousands of low-paid, low-skilled security jobs in the United States, but there are also scores of highly skilled private security experts (often formerly from the ranks of public police[13]). Corporate private investigation departments can sometimes match or even exceed the resources of public police departments. Target, for example, maintains its own forensics lab in its Minneapolis headquarters.[14]

In addition to private for-profit investigators, the American experience of crime control has also been characterized by bands of volunteers motivated by self-protection (neighborhood watches) or for the protection of vulnerable groups (Guardian Angels).[15]

Like private investigators, volunteer groups have been helpmeets or hindrances to the public police, particularly when private actions go beyond self-help into vigilantism.[16] Today, private companies have inserted themselves into the culture of defensive self-help. Networked devices such as Ring doorbell cameras,[17] Flock neighborhood license plate readers,[18] and the Citizen crime-reporting app produce surveillance information for private purposes but also for police departments, which can access this data by request or through prearranged partnerships.[19]

In sum, the resort to private sources of crime prevention and investigation is not new, and in fact predates professional urban police departments. These private arrangements are now also enhanced by the wide availability of products that vastly increase the amount and scope of information that can be collected.

Incentives

The history of private resources for security and policing would not by itself augur the emergence of freelance surveillance work. Identifying the other incentives for a gig surveillance economy requires us to look elsewhere. The characteristics of gig work and the rise of networked surveillance devices provide the additional incentives for the rise of a gig surveillance economy.

First, there is ubiquity of gig work itself: temporary, freelance, platform-distributed jobs on demand. These gigs include not just package and food delivery, clerical tasks, shopping, and warehouse stocking, but also online jobs such as audio transcription and survey completion.[20] While unskilled, low-wage work is not new, the gig economy is distinct because of its organization. Gig companies provide online platforms or smartphone apps that match prospective customers to potential workers for jobs. These companies supply the verification and reputational checks for trustworthiness in these arm's-length transactions. Thus, while there have long been cars for hire, companies such as Uber and Lyft provided the technological means to match customers and drivers for rideshares at a large scale.

Ever since the first Amazon Mechanical Turk worker bid for a job in 2005 and the first Uber driver picked up a passenger in 2011, the gig or "sharing" economy has grown dramatically.[21] Recent studies have estimated that perhaps as many as fifty-five million people in the United States engage in gig work of some kind—amounting to about a third of the workforce.[22] There are literally tens of millions of Americans who are already used to temporary, on-demand piecework that usually requires little skill or experience, and whose organization is mediated by gig work companies.

This very large workforce has two features that are relevant to a gig surveillance economy. First, one of the chief characteristics of gig work is its precarity.[23] Because of its on-demand nature, gig work fluctuates in both availability and compensation.[24] This leads some gig workers to offer their services to many companies at the same time. Food delivery workers

sign up for assignments with not just Postmates, but Instacart and DoorDash as well. Rideshare drivers may work for Uber and Lyft. The ad hoc nature of gig work can mean that its workers are caught in an anxious cycle of always looking for more piecework to add on.

A second relevant feature of the gig economy is that its workers are already inured to surveillance. That surveillance arises both from the gig companies and their customers. Gig workers may find all aspects of their performance monitored: location, speed, keystrokes, delivery metrics, and so on.[25] Amazon warehouse workers, for example, can expect algorithms to manage staffing based upon which "muscle-tendon groups" would lead to repetitive motion disorders.[26] Likewise, gig workers find their reputational rankings subject to constant surveillance and manipulations by customers. Gig workers can thus find themselves in "surveillance loops," where they are "constantly watched, not just by the platform itself . . . but also by clients."[27] Thus, surveillance is already an embedded feature of gig work.

Another structural incentive for the arrival of a gig surveillance economy is the nature of surveillance today: cheap, networked, ubiquitous, and normalized. Gig workers would not have to adapt to radically different work, but rather adjust to already-existing social and market conditions, each of which is worthy of further discussion.

The first relevant aspect of the current surveillance market is that the necessary tools for gig surveillance work exist already. License plate readers and body cameras are a commonplace part of the surveillance landscape. Not only are they tools for the police, but they are also offered as off-the-shelf consumer products. Homeowners can buy Ring's motion-sensitive livestreaming doorbell cameras for less than a hundred dollars.[28] A group of neighbors can install and operate a Flock license plate reader system for around twenty-five hundred dollars per camera, per year.[29]

These commercially available surveillance products are becoming ever more capable of identification and detection. Software updates can continuously augment the capabilities of much surveillance hardware. Body cameras can be updated with facial recognition.[30] License plate readers can match cars to watch lists in real time with artificial intelligence.[31]

And these data-gathering tools are pervasive. They can be installed everywhere—not just on street corners, but on homes, businesses, vehicles, and bodies. Every cell phone is a camera that can be connected to the cloud. DNA sampling may be nothing more than collecting literal garbage: discarded cups and silverware.[32] Data-storage costs are now low enough that storing all data collected is both practical and desirable.[33]

What is more, few of these surveillance tools require specialized skills. Police officers using body-worn cameras, for instance, may require some training, but these products are typically sold to police department customers for their ease of use.[34] The most popular brand of police body camera assumes that a patrol officer can simply use the device, return it at the

end of a shift, and then upload data to a cloud storage service where software like automated transcription and video analysis can then be applied.[35] Rank-and-file police officers do not have to become information technology or artificial intelligence specialists. Body cameras can thus increase the reach of police surveillance without demanding additional expertise.

Yet another feature of the commercial surveillance market is that it has further entrenched the normalization of ubiquitous and pervasive surveillance. Surveillance by private and public actors constitutes a routine aspect of ordinary transactions and communications. Millions of homeowners have internet-connected doorbell cameras.[36] Our cell phones can be accurately described as "universal personal surveillance" devices.[37] And the COVID-19 pandemic accelerated the use and acceptance of technologies such as facial recognition as work and school took place remotely.[38]

Although there certainly exist robust critiques from the scholarly and policy community about increasing mass surveillance, the reality is more complicated. Surveys suggest that people in the United States are worried about government tracking of their location through their digital devices[39] and employer surveillance in the workplace.[40] And yet tens of millions of Americans also purchase home surveillance devices. Our experience with surveillance also shows that social and political forces are as important as the technologies themselves when new surveillance modes are introduced. The rapid adoption of body cameras by American police departments in the 2010s, for instance, was less the result of technological developments than the cultural and institutional pressures for greater accountability that arose after the fatal shooting of Michael Brown by a Ferguson, Missouri, police officer in 2014.[41]

Finally, another important aspect of the current surveillance market relates to one particular and influential customer: the government. The collection of location data drawn from ordinary cell phone apps for uses such as games and shopping is a multibillion-dollar industry in the United States.[42] That location data can be used to identify movement patterns and habits of individuals for criminal investigations, national security purposes, and immigration enforcement.[43] The federal Department of Homeland Security, for instance, has purchased access to location data collected by Venntel, Inc., for immigration enforcement purposes.[44]

While the Supreme Court's 2018 decision in *Carpenter v. United States* concluded that government acquisition of historical cell phone location data usually requires a warrant,[45] government agencies have avoided these restrictions through the purchase, rather than direct collection, of personal information already captured by others.[46] The federal government has also taken the legal position that the purchase of information already collected by a third party is constitutionally distinct from asking a court for permission to collect it.[47] Buying access to the enormous pool of faces, license plates, movements, and other products of commercially available mass surveillance aids in

criminal investigations, immigration enforcement, and other government purposes. For local governments, access to databases of license plates or faces could generate revenue, including fines and fees for uninsured drivers[48] or individuals with outstanding tickets and citations.

In sum, many political and economic incentives have encouraged the emergence of gig surveillance work. The gig or sharing economy has created an enormous class of temporary, piecemeal, and often low-skilled workers. The nature of the gig economy today—focusing on reputation and performance management—means that gig workers become both agents and objects of surveillance. In addition, the commercial surveillance market now provides ever-cheaper tools of increasing accuracy that create ever-larger tranches of detailed information about people's patterns, habits, and identities. And there is every reason to think that temporary surveillance work as an end in itself will grow and grow as a sector of the economy.

Observations about a Gig Surveillance Economy

So what does gig surveillance work look like? There are at least two versions that already exist. Much of the conventional gig economy already collects surveillance data as an incidental matter. The following examples show how the existing gig economy easily becomes a gig surveillance economy by focusing on the data collection as its own profitable product.

The first type indiscriminately collects surveillance data; we can refer to this as mass surveillance gig work. Automated license plate reader (ALPR) data serves as a good example. While the police use license plate readers themselves, so do private companies. The Digital Recognition Network (DRN) is a commercial database of ALPR scans that is available to individuals, companies, and law enforcement agencies. Over the last ten years, DRN has created a "crowdsourced" database from thousands of cameras attached to the vehicles of repossession agents.[49] For fifteen thousand dollars, a repossession agent can install a license plate reader system and also obtain access to the DRN database.[50] This ALPR setup allows individual repossession agents to passively scan every license plate that they happen to pass by. The system benefits both DRN and the drivers; access to the database allows repossession agents to receive alerts if they have scanned the plate of a car marked for repossession, while the passively scanned plates with location and time stamps add to the DRN database.[51] In 2019, there were more than six hundred of these data-collecting "affiliates" who are paid monthly as part of DRN's "revenue share programs" for the license plate scans they collect.[52] DRN's customers include law enforcement agencies, insurance companies, and even individual users, who can pay to look up a license plate for as little as twenty dollars.[53]

Mass surveillance gig work would expand this model so that anyone could become a piecework collector of surveillance information for ALPR databases. This would not supplant

the existing ALPR economy but enhance it. Commercially available software such as OpenALPR can transform almost any internet-connected camera into a license plate reader for less than one hundred dollars.[54] Homeowners could be encouraged to earn passive income by selling license plate reader data that they collect from their home security cameras. Platforms could incentivize delivery drivers to install ALPR systems on their cars to collect data passively while performing their delivery gigs. Those same drivers could also be persuaded to wear body cameras to record information to be sold to private and public customers alike.

If this first potential model assumes an open-ended model of data collection, a second type of gig surveillance work would address individualized requests from gig clients; we can refer to this as focused surveillance gig work. Just as Amazon's "Turkers" perform online piecework for specific clients, targeted surveillance temp work could also be offered as a personal service. This too could take a variety of forms: jobs for obtaining video surveillance at specific addresses, collecting particular license plate scans, or even retrieving discarded trash containing genetic material from an individual.

None of these gig jobs require special investigatory skills; all can be outsourced cheaply. In this way, these focused surveillance gig jobs share only a surface similarity to traditional private investigation. Moreover, in the arm's-length transactions of the gig economy, individual surveillance gig workers may have no idea for whom or for what purpose they are collecting the information.

There is already a market and a service dedicated to this focused surveillance gig work. The Premise Data Corporation pays users of its app around the world to engage in small surveillance tasks.[55] While some of this work, like obtaining market information on competitors, is aimed at commercial clients, other forms appeal to government entities. Such tasks include collecting data on Wi-Fi signals and photography of sensitive locations such as mosques, banks, and cafes.[56] Business proposals prepared by Premise for the US military suggest ways in which their app could be used to be "responsive to [a] commander's information requirements."[57] The company claims to have six hundred thousand users who contribute data from around the world, including from Iraq, Afghanistan, Syria, and Yemen.[58] Premise app workers are not told for whom their tasks are being completed, although the company's policies disclose that some of its clients may be governments.[59]

While Premise has marketed itself as a gig work app for foreign intelligence, the same model could be used domestically by law enforcement. Police departments, for instance, could outsource surveillance work cheaply.[60] Gig surveillance work might accomplish some policing tasks cheaply and surreptitiously in ways that uniformed police officers could not. Gig workers could crowdsource surveillance of suspected areas of criminal activity or monitor suspected persons.

In neither model of gig surveillance work hypothesized here—mass surveillance or focused work—is the Fourth Amendment likely to pose much restraint on the government as a client. First, if the government purchases surveillance data of public activity voluntarily retrieved by gig workers and then aggregated by a platform, it is likely to justify the warrantless acquisition of that data as unprotected by the Fourth Amendment, as it has in similar previous instances.[61] Second, although privacy and civil liberties advocates have argued that the Supreme Court's imposition of a warrant requirement for cell phone location data in *Carpenter* should extend to other instances where highly personal information can be inferred from mass data collection,[62] thus far the federal agencies that have purchased this information distinguish the government's direct collection of location information from its purchase from commercial data brokers.[63] Third, gig surveillance work, which would involve the voluntary sharing (by the gig worker) of data (such as photography in public places) to a third party (the platform) for sale, does not fit neatly into existing Fourth Amendment doctrine.

In *Carpenter* itself, the Supreme Court distinguished but did not overturn two lines of cases that complicate the consideration of gig surveillance work. First are the Supreme Court decisions that have found no constitutional protections for physical movements in public because such activity is "voluntarily conveyed to anyone who want[s] to look."[64] Second are the cases finding no Fourth Amendment protections for information "voluntarily turn[ed] over to third parties."[65] Finding these two groups of cases not wholly applicable, the Supreme Court developed a new rule and a warrant requirement for the collection of historical cell phone location information.[66]

A commercial gig surveillance platform could solicit jobs for the public surveillance of specific persons or groups. Once aggregated, that information might give rise to inferences about long-term habits that might implicate *Carpenter*'s concerns: information that is "detailed, encyclopedic, and effortlessly compiled."[67] But whether courts would draw that conclusion is uncertain.

If the government were to solicit directly gig surveillance work for specific places and persons, a private gig worker might qualify as "an instrument or agent of the Government."[68] When the government directs or encourages a private party to engage in a search or seizure, courts may treat that activity no differently than if the government had performed the act itself.[69] Such a transformation of a private search into a public one, however, assumes that the collection of data itself qualifies as a Fourth Amendment search or seizure.[70] With gig surveillance work, however, the government-as-client may solicit tasks such as license plate scans and monitoring of public places and facts; such data collection by itself would not necessarily count as a "search" for Fourth Amendment purposes, even if the government retrieved the information itself.

Doctrinal uncertainty is unlikely to be countered by a robust legislative response, at least in the short term. The current state of federal and state regulation of mass surveillance by

the government is tepid. Despite the increasing use of technologies such as license plate readers and facial recognition by law enforcement agencies throughout the United States, no comprehensive national legislation exists regarding their use. The already-existing market for locational data collected through apps and then sold to private and public agencies is a billion-dollar industry operating with few legal constraints. A gig surveillance economy is likely to face the same dearth of regulations.

This means that potentially troubling aspects of the emerging gig surveillance economy would arise unchecked. First, unlike those who volunteer to the police information they happen to find by chance, gig surveillance workers would be incentivized to conduct as much surveillance as possible. That is the nature of gig work. An open market for piecemeal surveillance offering low wages but requiring no specialized skills would have a wide pool of workers. That by itself could dramatically expand surveillance of the public.

Second, if some forms of gig surveillance simply involve passively collecting any available information, such as license plate data, then gig surveillance workers would also possess near-total discretion about where and against whom to conduct surveillance. Left to their own discretion, gig surveillance workers incentivized to collect as much data as possible are unlikely to seek it in ways that spread surveillance burdens evenly. This may increase surveillance in low-income neighborhoods while avoiding wealthier ones in which such activities are more difficult or impossible. Like police discretion, gig work discretion would raise questions about discrimination and accountability with none of the regulatory checks imposed on the police.[71]

Other market incentives could further expand the scope of gig surveillance. To be sure, the internet has already introduced crowdsourced investigations conducted by private individuals without financial incentives. The federal investigation of the January 6, 2021, attack on the US Capitol, for instance, has been aided by thousands of volunteer sleuths willing to pore over online clues left in livestreams, pictures, and videos documenting the event.[72] Financial incentives would amplify participation. Consider bounties—in the form of bonuses or revenue sharing—for every "hit" for a wanted person or vehicle positively identified by a gig worker. Such financially incentivized data collection—with little regulation, supervision, or training—is likely to heighten the potential for abuse, mistakes, and overreach that we have seen in the use of surveillance technology by law enforcement officials.[73]

Finally, gig surveillance work will broaden the availability of government customers. While the average local police department may not have the funds to purchase a tranche of location information obtained by cell phone data brokers,[74] they can solicit surveillance work if it is cheap and on demand. Surveillance technology typically follows a familiar pattern. Initially, a new technology is prohibitively expensive to use except by some federal law enforcement agencies or the military. Eventually these tools become cheaper and often more sophisticated. Local police departments then emerge as eager customers,

whether through their own initiative or because federal grants incentivize the purchase of these new tools. Gig surveillance work can thus accelerate the accessibility of large amounts of data to a wider range of police departments.

Local police department use of gig surveillance work raises significant challenges. Regulating the direct use of surveillance tools such as license plate readers by police departments has proven difficult for local governments.[75] City councils and local communities may not know how to address gig surveillance work effectively. The companies providing these surveillance tools may also impose conditions of secrecy that hamper efforts to increase transparency and accountability.[76] As these services grow and grow, we might see demands for transparency by local governments in their oversight of police budgets and by defendants seeking the details of the surveillance acquired in their individual cases.[77]

Conclusion

The existing gig work economy—delivery work, rideshare drivers, online task work, and the like—already collects enormous amounts of surveillance data that is usually incidental to or integrated into gig tasks. But the gig work economy has also facilitated *gig surveillance work*: where surveillance is itself the gig worker's objective. The platform-mediated, temporary structure of conventional gig work that matches customers to workers is perfectly suited to the intentional collection of personal information, either indiscriminately or focused on particular persons. Moreover, surveillance tools that are enabled by artificial intelligence and connected by the internet are also increasingly cheap and require little skill to use. Examples of gig surveillance work already exist in the cases of license plate readers and foreign intelligence surveillance. This particular economy will only become more robust as the private sector realizes the profitability of temporary work to collect data as an end in itself. We can thus identify some of the law and policy issues that such a market produces, particularly as cheaply gathered personal information would appeal to law enforcement agencies of all types and sizes. Gig surveillance work expands the already-vast market for data available for purchase by the government, and thus raises important questions about transparency, accountability, and unbounded discretion in policing.

ACKNOWLEDGMENTS

Thanks to Jack Goldsmith and the participants in the Hoover Institution's 2021 National Security, Technology, and Law Working Group conference for their comments and suggestions.

NOTES

1 Matthew Brzezinski, *2003: The 3rd Annual Year in Ideas; The Homeland-Security Neighborhood Watch*, N.Y. Times Mag., Dec. 14, 2003, at 75.

2 *Id.*

3 *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (Kennedy, J., dissenting) ("The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party." (citing United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979))); *id.* ("This is true even when the records contain personal and sensitive information.").

4 *See* Shoshana Zuboff, The Age of Surveillance Capitalism (2019) (The Definition) (defining surveillance capitalism as "[a] new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales").

5 This essay focuses on the implications of a gig surveillance economy for the government as a client. There are certainly questions that arise for private clients, including individuals and corporations, but they are not addressed here.

6 *See, e.g.*, Sarah A. Donovan et al., Cong. Research Serv., R44365, What Does the Gig Economy Mean for Workers? (2017) (summary) ("The gig economy is the collection of markets that match providers to consumers on a gig (or job) basis in support of on-demand commerce."); Elka Torpey & Andrew Hogan, *Working in a Gig Economy*, U.S. Bureau of Lab. Statistics Career Outlook (May 2016), https://www.bls.gov/careeroutlook/2016/article/what-is-the-gig-economy.htm (noting that while "there is no official definition of the 'gig economy,'" a gig can be defined as "a single project or task for which a worker is hired, often through a digital marketplace, to work on demand").

7 Josh Dzieza, *Why CAPTCHAs Have Gotten So Difficult*, The Verge (Feb. 1, 2019), https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence (noting CAPTCHA is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart").

8 "Smart cities" typically refers to the introduction of information technologies that are embedded into the structure of a city and that help improve efficient delivery of city services and communications. *See generally* Vito Albino et al., *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*, 22 J. Urb. Tech. 3 (2015).

9 *See, e.g.*, Alana Semuels, *Private Detectives Filling Gaps Left by Police Budget Cuts*, L.A. Times (Feb. 20, 2013), https://www.latimes.com/world/la-xpm-2013-feb-20-la-fi-private-detective-20130220-story.html.

10 *See, e.g.*, Elizabeth E. Joh, *The Forgotten Threat: Private Policing and the State*, 13 Ind. J. Global Legal Stud. 357, 362 (2006).

11 *See, e.g.*, David R. Johnson, Policing the Urban Underworld: The Impact of Crime on the Development of the American Police 48–50 (1979).

12 *See, e.g.*, Seth W. Stoughton, *The Blurred Blue Line: Reform in an Era of Public & Private Policing*, 44 Am. J. Crim. L. 117, 128–29 (2017).

13 *See, e.g.*, J. David Goodman, *Bratton Gives Revolving Door One More Spin*, N.Y. Times (Dec. 23, 2013), https://www.nytimes.com/2013/12/24/nyregion/bratton-tries-to-untangle-his-corporate-ties.html.

14 John Colapinto, *Stop, Thief!*, New Yorker (Aug. 25, 2008), https://www.newyorker.com/magazine/2008/09/01/stop-thief.

15 *See generally* Wesley G. Skogan, *Community Organizations and Crime*, 10 Crime and Just. 39 (1988).

16 In the 2013 trial of George Zimmerman for the fatal shooting of Trayvon Martin, an African American teenager living in Miami Gardens, Florida, considerable attention was paid to Zimmerman's role in his local organized neighborhood watch. *See* Michael Muskal & Tina Susman, *Rules for Neighborhood Watch Discussed in George Zimmerman Trial*, L.A. Times (June 25, 2013), https://www.latimes.com/nation/la-xpm-2013-jun-25-la-na-nn-george-zimmerman-neighborhood-watch-20130625-story.html.

17 Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, Wash. Post (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach.

18 Ella Fassler, *Neighborhood Watch Has a New Tool: License-Plate Readers*, OneZero (Nov. 11, 2020), https://onezero.medium.com/neighborhood-watch-has-a-new-tool-privately-owned-license-plate-readers-302f296abb27.

19 *See, e.g.*, Jamie Siminoff, *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*, Ring Blog (Aug. 28, 2019), https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map.

20 *See, e.g.*, Alana Semuels, *The Internet Is Enabling a New Kind of Poorly Paid Hell*, Atlantic (Jan. 23, 2018), https://www.theatlantic.com/business/archive/2018/01/amazon-mechanical-turk/551192/.

21 European Parliamentary Research Service, *Data Subjects, Digital Surveillance, AI and the Future of Work*, at 27, PE 656.305 (Dec. 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf [hereinafter *Data Subjects*].

22 *See, e.g.*, Nandita Bose, *U.S. Labor Secretary Supports Classifying Gig Workers as Employees*, Reuters (Apr. 29, 2021), https://www.reuters.com/world/us/exclusive-us-labor-secretary-says-most-gig-workers-should-be-classified-2021-04-29/.

23 *See, e.g.*, Alexia Fernández Campbell, *The Recession Hasn't Ended for Gig Economy Workers*, Vox (May 28, 2019), https://www.vox.com/policy-and-politics/2019/5/28/18638480/gig-economy-workers-wellbeing-survey (noting that in a recent survey, workers who said gig work was their main source of income were "the most likely to report financial distress, and the least likely to have health insurance, paid time off, unemployment benefits, and basic labor protections"); Kimiko de Freytas-Tamura, *Food Delivery Apps Are Booming. Their Workers Are Often Struggling*, N.Y. Times (Nov. 30, 2020), https://www.nytimes.com/2020/11/30/nyregion/bike-delivery-workers-covid-pandemic.html.

24 *See, e.g.*, Shelly Steward, *Five Myths about the Gig Economy*, Wash. Post (Apr. 24, 2020), https://www.washingtonpost.com/outlook/five-myths/five-myths-about-the-gig-economy/2020/04/24/852023e4-8577-11ea-ae26-989cfce1c7c7_story.html ("The dynamic pricing systems used by Uber, Lyft, and other platforms make not only job availability, but the rate of pay, unpredictable.").

25 *See, e.g.*, Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 Cal. L. Rev. 735, 742 (2017) ("Punch clocks have given way to thumb scans, key cards may soon give way to Radio Frequency Identity (RFID) tags, and internet browser histories are often scrutinized closely.").

26 Annie Palmer, *Jeff Bezos Says Amazon Needs to Do a Better Job for Employees in His Final Shareholder Letter as CEO*, CNBC (Apr. 15, 2021), https://www.cnbc.com/2021/04/15/jeff-bezos-releases-final-letter-to-amazon-shareholders.html.

27 *Data Subjects*, *supra* note 21.

28 Sam Wollaston, *I Spy: Are Smart Doorbells Creating a Global Surveillance Network?*, Guardian (June 26, 2021), https://www.theguardian.com/lifeandstyle/2021/jun/26/i-spy-are-smart-doorbells-creating-a-global-surveillance-network.

29 Flock Safety, *How Much Does a Flock Safety Camera Cost?*, Flock Safety Blog, https://www.flocksafety.com/blog/faq-items/how-much-does-a-flock-camera-cost-for-your-neighborhood (last visited Aug. 23, 2021).

30 *See* Andrew Westrope, *Wolfcom Embraces Body Cam Face Recognition despite Concerns*, GovTech (Mar. 20, 2020), https://www.govtech.com/biz/wolfcom-embraces-body-cam-face-recognition-despite-concerns.html (describing a facial recognition–enabled body camera that is in development).

31 *See, e.g.*, IntelliVision, *Explore the Advanced Features of Our License Plate Recognition Technology* (June 10, 2020), https://www.intelli-vision.com/2020/06/10/explore-the-advanced-features-of-our-license-plate-recognition-technology (listing advanced features).

32 Paige St. John, *The Untold Story of How the Golden State Killer Was Found: A Covert Operation and Private DNA*, L.A. Times (Dec. 8, 2020), https://www.latimes.com/california/story/2020-12-08/man-in-the-window (discussing police identification of Golden State Killer Joseph DeAngelo after "enlisting help of a garbage truck driver to snatch DNA-bearing items from his trash can").

33 *Cf.* John Villasenor, *Recording Everything: Digital Storage as an Enabler of Authoritarian Governments*, Brookings 8 (2011), https://www.brookings.edu/wp-content/uploads/2016/06/1214_digital_storage_villasenor.pdf.

34 *See, e.g.*, Axon Body 3 [Camera], https://www.axon.com/products/axon-body-3 (last visited Aug. 23, 2021) (featuring testimonial: "The device is easy to operate.").

35 *See, e.g.*, Axon Dock Security, https://global.axon.com/security/dock (last visited Aug. 23, 2021) (describing Axon product that provides for "intuitive" uploading of data from Axon body cameras to cloud storage service).

36 Ring's vice president of public policy also stated in a 2020 written response to US senators that while Ring does "not disclose the specific numbers of devices sold . . . there are millions of customers who have purchased a Ring device." Letter from Brian Huseman, vice president of public policy, Ring, to Senators Wyden, Van Hollen, Markey, Coons, and Peters (Jan. 6, 2020), https://www.documentcloud.org/documents/6603014-Response-Letter-on-Ring-1-6-2020.html#document/p2/a545936.

37 Christopher Mims, *Body Cameras for All: One Way to Avert Lawsuits*, Wall St. J. (Jan. 4, 2015), https://www.wsj.com/articles/keywords-body-cameras-for-all-one-way-to-avert-lawsuits-1420419535.

38 Janna Anderson et al., *Experts Say the "New Normal" in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges*, Pew Res. Ctr. (Feb. 18, 2021), https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges.

39 Byron Tau, *Most Americans Object to Government Tracking of Their Activities through Cellphones*, Wall St. J. (Nov. 25, 2020), https://www.wsj.com/articles/most-americans-object-to-government-tracking-of-their-activities-through-cellphones-11606305601.

40 Mary Madden & Lee Rainie, *Americans' Attitudes about Privacy, Security and Surveillance*, Pew Res. Ctr. 19 (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance.

41 *See, e.g.*, Elizabeth E. Joh, *Beyond Surveillance, Data Control and Body Cameras*, 14 Surveillance & Society 133 (2016).

42 Byron Tau, *Treasury Watchdog Warns of Government's Use of Cellphone Data without Warrants*, Wall St. J. (Feb. 22, 2021), https://www.wsj.com/articles/treasury-watchdog-warns-of-governments-use-of-cellphone-data-without-warrants-11614003868.

43 *See id.*

44 Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=article_inline.

45 Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (holding that government acquisition of cell site location information is a Fourth Amendment search that typically requires a warrant supported by probable cause).

46 Tau & Hackman, *supra* note 44.

47 *See id.* ("Because location information is available through numerous commercial ad exchanges, government lawyers have approved the programs and concluded that the Carpenter ruling doesn't apply.").

48 *See* Ella Fassler, *Oklahoma Quietly Launched a Mass Surveillance Program to Track Uninsured Drivers*, OneZero (Apr. 6, 2021), https://onezero.medium.com/oklahoma-quietly-launched-a-mass-surveillance-program-to-track-uninsured-drivers-471bb4e5701a.

49 Joseph Cox, *This Company Built a Private Surveillance Network*, Motherboard (Sept. 17, 2019), https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn.

50 *Id.*

51 *Id.*

52 Digital Recognition Network, *Become an Affiliate* (Sept. 13, 2019), https://web.archive.org/web/20190913144119/https://www.drnrecovery.com/affiliates/become-an-affiliate.

53 *See* Cox, *supra* note 49.

54 *See, e.g.*, Josh Kaplan, *License Plate Readers Are Creeping into Neighborhoods across the Country*, Slate (July 10, 2019), https://slate.com/technology/2019/07/automatic-license-plate-readers-hoa-police-openalpr.html.

55 Byron Tau, *App Taps Unwitting Users Abroad to Gather Open-Source Intelligence*, Wall St. J. (June 24, 2021), https://www.wsj.com/articles/app-taps-unwitting-users-abroad-to-gather-open-source-intelligence-11624544026.

56 *Id.*

57 *Id.*

58 *Id.*

59 *Id.*

60 To understand how cheaply this could be done, consider that a Premise user in Afghanistan is typically paid twenty-five cents per task. *Id.*

61 Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-by-Moment Geolocation Cellphone Data to Track People*, BuzzFeed News (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation (quoting DHS attorney Chad Mizelle's memo as stating: "the government's acquisition of that information is not a 'search' under the Fourth Amendment").

62 *See, e.g.*, Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, Brennan Ctr. for Justice (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data.

63 *See id.*; Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It*, Wash. Post (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases (arguing the "practice of buying Americans' data has become routine, effectively hollowing out both *Carpenter* and privacy safeguards enacted by Congress"). *But see* Tau, *supra* note 42 (reporting on IRS memo warning that courts may apply *Carpenter*'s warrant requirement to GPS data sold to government by marketing firms).

64 Carpenter v. United States, 138 S. Ct. 2206, 2215 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

65 *Id.* at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

66 *Id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

67 *Id.* at 2217.

68 *See* Skinner v. Railway Labor Exec. Ass'n, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government. . . . Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved 'in light of all the circumstances.'") (internal citations omitted) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

69 *See, e.g.*, U.S. v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997) (noting that the Sixth Circuit treats a private party as a government agent when police have "instigated, encouraged or participated in the search" and the private party "ha[s] engaged in the search with the intent of assisting the police in their investigative efforts") (quoting United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985)).

70 *See, e.g.*, U.S. v. Walther, 652 F.2d 788, 791 (9th Cir. 1981) ("A wrongful search or seizure by a private party does not violate the fourth amendment. However, where a private party acts as an 'instrument or agent' of the state in effecting a search or seizure, fourth amendment interests are implicated.") (internal citations omitted) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)).

71 *See, e.g.*, George L. Kelling, "Broken Windows" and Police Discretion, National Institute of Justice Research Report (1999) (noting that research on the "ubiquity of discretion" in policing has heavily influenced police practice and culture).

72 *See, e.g.*, Sarah Parvini & Melissa Gomez, *On Social Media, Amateur Digital Sleuths Try to Help Track Violent Capitol Rioters*, L.A. Times (Jan. 17, 2021), https://www.latimes.com/california/story/2021-01-17/amateur-social-media-sleuths-track-violent-capitol-rioters; David Yaffe-Bellany, *The Sedition Hunters*, Bloomberg (June 7, 2021), https://www.bloomberg.com/features/2021-capitol-riot-sedition-hunters (noting that the FBI has "also relied on the crowdsourcing efforts of [online] sedition hunters").

73 *See, e.g.*, Christine Hauser, *Aurora Police Chief Apologizes after Officers Handcuff Children on the Ground*, N.Y. Times (Aug. 5, 2020), https://www.nytimes.com/2020/08/05/us/aurora-police-black-family.html?smid=url-share (reporting mistaken license plate reader match led to car stop and handcuffing of family including four children); Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html?smid=url-share (reporting what may be the "first known account of an American being wrongfully arrested based on a flawed match from a facial recognition algorithm").

74 *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

75 *See, e.g.*, Mailyn Fidler, *Local Police Surveillance and the Administrative Fourth Amendment*, 36 Santa Clara High Tech. L. J. 481, 512 (2020) ("As of August 2020, fourteen local government entities—thirteen cities and one county—have passed laws formalizing administrative control over police use of sophisticated investigative technologies.").

76 *See, e.g.*, Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. Rev. Online 101 (2017).

77 *See generally* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 Stanford L. Rev. 1343 (2018).

hoover.org

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

The preferred citation for this publication is Elizabeth E. Joh, *A Gig Surveillance Economy*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2108 (November 10, 2021), available at https://www.lawfareblog.com/gig-surveillance-economy.

About the Author

ELIZABETH E. JOH

Elizabeth E. Joh is the Martin Luther King Jr. Professor of Law at the University of California–Davis School of Law. She has written widely about policy, technology, and surveillance. Her scholarship and commentary have appeared in leading legal and news publications. She previously clerked for the Honorable Stephen Reinhardt on the Ninth Circuit Court of Appeals.

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