Received: 10 October 2022 | Revised: 15 June 2023 | Accepted: 4 August 2023

DOI: 10.1111/lasr.12681

ARTICLE

Law & Society REVIEW

Surveillance deputies: When ordinary people surveil for the state

Sarah Brayne[1] | **Sarah Lageson**[2] | **Karen Levy**[3]

[1]Department of Sociology, University of Texas at Austin, Austin, Texas, USA

[2]School of Criminal Justice, Rutgers University, Newark, New Jersey, USA

[3]Department of Information Science, Cornell University, Ithaca, New York, USA

Correspondence
Sarah Brayne, Department of Sociology, University of Texas at Austin, Austin, TX, USA.
Email: sbrayne@utexas.edu

Abstract

The state has long relied on ordinary civilians to do surveillance work, but recent advances in networked technologies are expanding mechanisms for surveillance and social control. In this article, we analyze the phenomenon in which private individuals conduct surveillance on behalf of the state, often using private sector technologies to do so. We develop the concept of *surveillance deputies* to describe when ordinary people, rather than state actors, use their labor and economic resources to engage in such activity. Although surveillance deputies themselves are not new, their participation in everyday surveillance deputy work has rapidly increased under unique economic and technological conditions of our digital age. Drawing upon contemporary empirical examples, we hypothesize four conditions that contribute to surveillance deputization and strengthen its effects: (1) when interests between the state and civilians converge; (2) when law institutionalizes surveillance deputization or fails to clarify its boundaries; (3) when technological offerings expand personal surveillance capabilities; and (4) when unequal groups use surveillance to gain power or leverage resistance. In developing these hypotheses, we bridge research in law and society, sociology, surveillance studies, and science and technology studies and suggest avenues for future empirical investigation.

INTRODUCTION

In 2020, Amazon announced that over 10 million users had joined its "Neighbors" app (Huseman, 2021). The app is integrated into the company's home surveillance devices, including the popular "Ring" doorbell camera—a video-enabled device that enables users to view, speak with, and record their front door area as well as the people who visit it. When a person purchases and installs

Sarah Brayne, Sarah Lageson and Karen Levy have noted equal authorship on this article.

a Ring doorbell, they are automatically enrolled in the Neighbors app, which enables users to post videos of "suspicious" activities and crimes (including the theft of Amazon packages from their doorsteps; Molla, 2020) and to view similar content posted by other users within five miles of their location. Although these "surveillance as a service" devices are marketed to, purchased, and installed by civilians, the state regularly seeks access to their data (West, 2019). The content collected by Ring cameras is shared directly with more than 2000 police departments across the United States through a combination of subpoenas, warrants, court orders and memorandums of understanding between municipalities or homeowners' associations and local law enforcement agencies (Lyons, 2021). Most often, that content is shared with the state by users who volunteer it to police (Gilliard, 2021; Haskins, 2021). Ring and Neighbors thus represents a convergence of interests among consumers, the state, and one of the largest and most powerful technology companies. Homeowners can protect their property; police have access to previously difficult-to-reach surveillance content; Amazon profits.

Ring exemplifies the phenomenon of what we term *surveillance deputization*: when ordinary people use their labor and economic resources to engage in surveillance activities on behalf of the state. Our analysis of the historical development and contemporary forms of surveillance deputization demonstrate that the phenomenon shows no signs of abating, as states continue to implore people to watch and report on one another. Despite its prevalence, sociolegal scholarship has rarely examined surveillance deputization as a coherent phenomenon, and it remains an underspecified mechanism of state power. The case of surveillance deputization illustrates broader forces at play, including neoliberal privatization of state functions, the cultivation of risk and fear, and the interplay between law, technology, and privacy. It also sheds new light on core themes and debates in law and society literature, including legal consciousness, legal mobilization, and legal ambiguity—concepts which consider how ordinary people make sense of ambiguous and rapidly changing legal and quasi-legal contexts. Therefore, we articulate a theoretical framework of surveillance deputization rooted in a law and society approach, describing how it functions, what motivates participation, its implications, and how it intersects with state and corporate interests. We offer four hypotheses about its dynamics and implications: (1) the interest convergence hypothesis; (2) the legal institutionalization hypothesis; (3) the technological mediation hypothesis; and (4) the social stratification hypothesis.

Our hypotheses draw upon several key themes in the law and society literature. First, surveillance deputization represents a case in which ordinary people must contend with both an ambiguous legal environment and a new suite of technological capabilities. Future law and society scholarship might continue to examine this interplay between lay people's understanding of law and legal rights as they implement new tools that in turn support functions typically relegated to the state. Our hypotheses also invoke concepts of legal mobilization, when both private companies and private individuals actively leverage surveillance to obtain quasi-legal outcomes or aid in legal processes, exposing unclear meanings of the law in the digital, platformed age. Finally, our analysis directly engages law and society scholarship with studies of technology. As we show, the networked, data-intensive technologies that have become the infrastructure of everyday life—like smartphones, Internet of Things (IoT) sensors, software, and digital platforms—are both intensifying and transforming these practices (Ferguson, 2017; Murakami Wood & Monahan, 2019). Our analysis shows how these new devices and capabilities benefit the interests of both the user and the state; they allow more expansive and invasive surveillance capabilities as technology evolves; they allow governments to evade privacy-protective legal constraints; and, while they have the potential to further marginalize vulnerable groups, they can potentially be used to turn the lens back on the state itself.

Although this article focuses on surveillance deputization, we hope the framework and empirical hypotheses detailed below spurs sociolegal work on questions of how the law deals with technological change, how ordinary people make sense of and contribute to the workings of the legal system, and continuities and changes in the practice of policing and in legal institutions. We begin with a brief social history of surveillance deputization, then explain our analytic and theoretical approach, including the literatures we draw from and the empirical examples we provide. We then move to a discussion of our four hypotheses, laying the groundwork for testable propositions in future empirical work. We

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

close by encouraging scholars to continue to examine whether and how the acceleration of surveillance deputization augments the scope of state surveillance, intensifies the effects of surveillance on marginalized populations, and opens opportunities for collective resistance.

A BRIEF HISTORY OF SURVEILLANCE DEPUTIZATION

Despite the recent emergence of Amazon Ring and other technologies, surveillance deputization is not a new phenomenon. For as long as states have watched their populations, they have relied on everyday people to help them do so. Historically, governments have enlisted their residents to aid in law enforcement, peacekeeping, and the imposition of state-sanctioned behaviors. The mechanisms have varied over time. Individuals are sometimes granted official authority to act *as* state actors—for instance, governments can grant citizens arrest powers, allowing for the conscription of citizens into a *posse comitatus*, or use statutory means like California's Private Attorney General Act to formally deputize civilians (Meshel, 2021). In other contexts, states may legally endow citizens with private rights of action to address certain wrongs, which can serve not only to "crowdsource" rule enforcement, but also provide state enforcers with otherwise inaccessible information about rule-breaking (Megiddo, 2023; Michaels & Noll, 2021; Scholz, 2022). In still other cases, residents are incentivized to work *alongside* state agents, serving as eyes and ears for the state.

Governments have long sought to solicit informants who can provide pivotal information about fellow community members in the course of investigations (Bergemann, 2021; Bloom, 2002; Donnelly, 1951; Hall, 2009; Klehr & Haynes, 2022; Rutledge, 2002). In the Middle Ages, the English frankpledge system required civilians to report one another for crime or owe collective financial penalty (Reeves, 2017). During the fourteenth century, English communities employed "watch and ward" patrols, composed of groups of day wardens and night watchmen deployed to monitor goings-on and to "raise a hue" if the law was broken (Reeves, 2017). Watch and ward patrols developed into "town watches" in the seventeenth and eighteenth centuries; a town's male adults were conscripted into the watch, and until the nineteenth century it was rare that they were paid for their surveillance duties (Reeves, 2017). In seventeenth-century New Amsterdam (later New York City), civilians operating "rattle watches" would take turns overseeing their communities at night and would raise a hue by shaking rattles if a crime was committed (Reeves, 2017).

Early efforts at crowdsourcing surveillance were deeply entwined with racist policies and the maintenance of white social and racial order. As surveillance scholar Simone Browne details, in the eighteenth century, Northern U.S. cities passed "lantern laws" requiring Black residents to carry lit lanterns after dark, to enable them to be readily identified by white residents. White people were authorized to stop and question Black residents traveling without lanterns and to take them to jail (Browne, 2015). Meanwhile, America's first system of organized, civilian-based law enforcement (Ayers, 1984), the Indian Constables, were tasked with monitoring interactions between American Indians and white settlers in colonial New England.

In the antebellum South, all-white citizen patrols armed with whips and guns policed the areas surrounding plantations and were charged with management and insurrection suppression of people who were enslaved. As historians Elizabeth Hinton and DeAnza Cook (2021) describe: "Any person of African descent in the slave states who appeared to be outside of the control of a white master and failed to otherwise prove their free status could be seized, imprisoned, and corporeally punished by 'nearly any capable white civilian'" (p. 266; see also Hadden, 2003). The passage of the federal Fugitive Slave Act of 1850 codified the legal requirement that all escaped people who were enslaved were to be returned to the person enslaving them upon capture, incentivized bounty hunters to locate and capture them, and punished anyone who refused to assist (Blackett, 2018; Hadden, 2003).

Media and technology play key roles in deputization dynamics. As media scholar Joshua Reeves explains, the power of the state intensified when hue and cry declarations began to take advantage of print media. The distribution of print media expanded the jurisdiction of the community as deputies

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

not only in local affairs, but in more temporally and spatially distant affairs, "abstract[ing] [crime] from personal or communal experience and reconstitut[ing] [it] as an act not against specific citizens, but against the sovereign" (Reeves, 2017, p. 33). Over time, the genre of posted hue and cry declarations grew to include a variety of media, including "Wanted" posters, the public display of police mugshots in rogues' galleries, and pictures of missing children printed on milk cartons (LaFrance, 2017).

Today, networked information technologies, embedded into everyday life, enable these age-old practices to manifest in new ways. The milk-carton photos of the 20th century have morphed into the digital dissemination of AMBER Alerts, galvanizing community members to assist in the search for missing children; mugshots have proliferated online as digital criminal records, driving traffic and advertising revenue to the operators of private-sector criminal record websites (Lageson, 2020; Reeves, 2017). These examples raise questions about whether and how the digital turn has expanded surveillance deputization, potentially ushering in a new set of incentives for the state, the private market, and the individual.

Modern surveillance deputization may also extend the reach of the state into new realms by bootstrapping interpersonal concerns into the state surveillance apparatus. For instance, one of Donald Trump's early presidential actions was to launch a hotline called "Victims of Immigrant Crime Engagement" (VOICE) encouraging people to report crime by "individuals with a nexus to immigration" to the Immigration and Customs Enforcement authority (ICE) (O'Connor & Rivero, 2017). The calls fielded by the hotline ranged from individuals reporting against ex-wives, aggrieved friends, and business competitors, including a caller reporting a woman allegedly trying to lure customers away from her ballroom dance studio (O'Connor & Rivero, 2017). Surveillance deputization co-opts everyday aggravations in the service of state control and is thus an undertheorized modality through which state surveillance is entrenched in quotidian social life.

SURVEILLANCE DEPUTIZATION: FOUR HYPOTHESES

We offer four hypotheses describing the functioning and implications of surveillance deputization: (1) the *interest convergence hypothesis*, suggesting that surveillance deputization regimes are most likely to emerge when the interests of the state and the civilian, however distinct, are aligned toward mutual benefit; (2) the *legal institutionalization hypothesis*, suggesting that surveillance deputization is more entrenched when institutionalized by law but may also flourish when law is ambiguous; (3) the *technological mediation hypothesis*, suggesting that contemporary networked technologies spread and intensify surveillance deputization by virtue of the profit motives underlying private sector innovation and patterns of consumption; and (4) the *social stratification hypothesis*, suggesting that surveillance deputization often reinforces patterns of social stratification and structures of inequality.

To develop these hypotheses, we draw on social scientific, legal, and historical literature, legal cases, policy debates, and news articles that describe historical practices, contemporary applications, and the technologies that fit our definition of surveillance deputization: ordinary (i.e., nonstate) actors engaging in surveillance activities on behalf of the state. Like Lauren Edelman and Suchman (1999) and Galanter (1974), we aim to highlight "general features" of the sociolegal phenomenon of surveillance deputization, organize them into emergent themes, and develop testable hypotheses. We posit our theory and four hypotheses as starting points for understanding surveillance deputization as a widespread sociolegal phenomenon, describing its potential impacts in broad terms. For each of our hypotheses, as Edelman and Suchman do, we "muster a substantial body of evidence and argumentation; however, we leave conclusive testing of these hypotheses to the future efforts of researchers throughout the law and society community" (Edelman & Suchman, 1999, p. 944).

Again following Edelman and Suchman (1999), our evidence and argumentation is based on a synthesis of research literatures often treated as distinct: (1) theoretical and empirical work on surveillance activities by state actors like police and intelligence agencies; (2) social scientific work on "lateral" (Andrejevic, 2006) or "peer-to-peer" interpersonal surveillance by ordinary people in the

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

course of their daily activities; (3) sociolegal and sociotechnical theory on responsibilization and the consumerization of risk; and (4) work on the social impacts of private-sector technological innovations. These literatures fit together into a broader law and society tradition that seeks to clarify how sociolegal phenomena and understandings of law operate in rapidly changing and often ambiguous environments (e.g., Perry-Hazan & Birnhack, 2016; Thacher, 2005).

We draw on secondary analysis of extant literature with empirical instantiations from a variety of sources, including media coverage, policy briefs, materials from technology companies, and case law and litigation. Having collected examples of surveillance deputization across several years, in our hypothesis generation, we drew only upon cases that fit our specific definition of surveillance deputization (nonstate actors conducting surveillance activities that contribute to state interests), excluding those only tangentially related (e.g., the installation of a sophisticated closed circuit home security system for personal viewing). Though not systematically sampled and in no way exhaustive of all forms of surveillance deputization, our use of secondary literature and contemporary cases constitutes a historically grounded, theoretically motivated body of evidence that underpins the following four hypotheses.

HYPOTHESIS 1: INTEREST CONVERGENCE

States deputize civilians as surveillors for a variety of reasons—to help the state access otherwise-concealed information, to preserve state resources, and to foster collective identity, to name a few. In addition, civilians have a variety of reasons for serving as deputies, ranging from financial reward to ideological alignment to motivations borne of interpersonal conflict. The interest convergence hypothesis posits that surveillance deputization regimes are more likely to emerge when the interests of the state and the civilian—even if distinct—are aligned, such that deputization offers mutual benefit. Deputization regimes can rely on both proactive and reactive civilian participation, and have varying degrees of formality. In some of the cases we describe, the civilian "takes the lead" in volunteering information to state actors, while in other cases, state actors actively promote and incentivize opportunities for civilians to report. We examine this dynamic from two angles, drawing on theory and empirical examples that shed light on two questions: why do states deputize, and why do deputies surveil?

Why do states deputize?

Surveillance deputies typically work for free or cheap, and they are often recruited because they are privy to information the state would not otherwise be able to access or which would be costly or impossible to obtain in any other way. The state might benefit from surveillance deputization in multiple ways, which are discussed below.

Access to information

States often benefit when control is distributed to the margins. In line with Foucault's theory of capillary power, modern state power operates at the "lowest extremities of the social body in everyday social practices" (Fraser, 1981). Perhaps the most dominant rationale for deputization is that private individuals have access to information that the state, operating on its own, cannot reach. In some contexts, this is a function of scale; using the public for reporting increases the number of "eyes on the street" (Jacobs, 1961), effectively crowdsourcing surveillance.

AMBER alerts are emblematic. First issued in the mid-1990s, following the abduction and murder of nine-year-old Amber Hagerman in Arlington, Texas (Reeves, 2017), AMBER alerts were initially driven by community actors independent of law enforcement. Today, they have become tightly

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

incorporated into state public safety efforts, greatly extending their reach. Through publicizing descriptions of abductors, abductees, and vehicles to the public at large, the state effectively creates thousands of searching eyes on public highways and in communities, leveraging people's everyday observations in the service of locating missing people. Over time, AMBER alerts have come to rely on new technologies, like chyrons at the bottom of local television broadcasts and electric highway signs describing suspect vehicles to social media notifications in affected localities.

AMBER alerts rely on mass broadcast of information to potential deputies, any one of whom might happen to see an individual or vehicle of interest and relay this information back to the state. In other cases, deputies' access to information is more particularized, premised on personal and professional relationships. By virtue of their social position, individuals may have special access to others' secret information, and states may target such individuals to serve as deputies vis-a-vis one another (see Chiarello, 2015; Hall, 2009).

The early days of the COVID-19 pandemic introduced new opportunities for surveillance deputization. Globally, people were induced to report violations of social distancing guidelines. For example, in April 2020, New York City Mayor Bill de Blasio announced a new text-to-report service and advised residents that "when you see a crowd, when you see a line that's not distanced, when you see a supermarket that's too crowded, anything, you can report it right away so we can get help there to fix the problem, and now it's as simple as taking a photo. All you got to do is take the photo and put the location with it and bang, send a photo like this and we will make sure enforcement comes right away" (Figure 1; CBS New York, 2020). Crowdsourced enforcement aided the city in efficiently directing law enforcement to sites of rule violation, extending the government's gaze into restaurants, stores, and other spaces across the city.

Labor and resources

States may turn to deputization when they face resource limitations that impede desired surveillance goals. Sociolegal scholar David Garland (1996) notes community policing and neighborhood watch programs often accompany budget cuts to municipal police departments, as surveillance deputies are typically inexpensive or free sources of labor and can often be motivated through non-pecuniary means. Surveillance deputies thus constitute a renewable, motivated supply of cheap surveillance labor.

Early systems for income tax enforcement during the Civil War relied on such mechanisms. To facilitate new financial inflows needed for wartime expenses without creating a costly administrative system for enforcing honest reporting, tax returns were made publicly available under the theory that civilians would report on one another and tip off the government if their neighbors seemed to be underreporting (Smith & Kestenbaum, 2020). Such practices reinforce the Foucauldian (1977) notion of efficiency, wherein state enforcement resources are distributed across increasingly docile subjects. Even when surveillance deputies are compensated for their contributions, their labor is often a form of piecework, in which they are paid for actionable tidbits of information only (e.g., credible leads in an investigation). In contrast, paying for salaried centralized personnel involves significant overhead.

Alternatively, states may view deputization as providing a check on internal corruption or inefficacy of state employees. In this version, it serves an ombuds function through which the public may not only report on *private* individuals, but also can shed light on whether *public* officials are adequately executing their duties. Jeremy Bentham's "Panopticon Letters," a key text in surveillance theory, draws out the idea: the Panopticon inspector's visiting family may not only assist in surveilling prisoners, but also in snitching on the inspector *himself*: "What the inspector's or keeper's family are with respect to *him*, that, and more, will these spontaneous visitors be to the superintendent—*assistants*, *deputies, in so far as he is faithful, witnesses and judges should he ever be unfaithful*, to his trust" (Letter VI, Bentham, 1995 [1787], p. 47; emphasis added). The state, then, need not seek managerial public agents; instead, deputies can provide supervision that increases governmental workers' efficiency, efficacy, and accountability.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

FIGURE 1 Bill de Blasio invites New Yorkers to inform on individuals and businesses who are not participating in social distancing. *Source*: https://twitter.com/nycmayor/status/1251496378372632577.

Fostering collective identity

Finally, surveillance deputization may have prosocial effects by fostering collective identity. Like other forms of participatory governance, surveillance deputization may promote a feeling of common cause, accompanied by loyalty to the state and docility of the subject through a Durkheimian sense of collective consciousness. The community may be understood as benefitting from the public policing of norms (Durkheim, 1996; Erikson, 1966).

Sir Robert Peel, founder of the Metropolitan Police Service in the United Kingdom, alluded to this sense of community in his Peelian principles, commonly credited with establishing the model of "policing by consent" (Jackson et al., 2012). Among these principles, Peel charges police with "maintain[ing] at all times a relationship with the public that gives reality to the historic tradition that *the police are the public and that the public are the police*" (quoted in Williams, 2003, p. 100). Peel emphasized that "the police [are] the only members of the public who are paid to give full time attention to duties which are incumbent on every citizen in the interests of community welfare and existence" (quoted in Williams, 2003, p. 100). Surveillance deputization may promote this sense of allyship between civilian and state—a principle well-illustrated by the Port Authority of New York and New Jersey's "Look Out for Safety" poster, below (Figure 2). Here, an everyday civilian ("Jason") is meant to view himself as a police officer of sorts, equally equipped (with eyes, ears, and cell phone) to ensure public safety.

Why do deputies surveil?

People who serve as deputies have their own independent motivations for doing so, which often align with the interests of the state. We articulate some possibilities below.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

FIGURE 2 Image from the Port Authority of New York and New Jersey "Look Out for Safety" program. *Photo Credit:* Lauren Kilgour; *Source*: http://www.lookoutforsafety.com/.

Securing favorable treatment

Surveillance deputies may serve to secure favorable treatment for themselves or their families from the state. This is common under authoritarian regimes (Hall, 2009), though it manifests across political contexts and domains. In real-life variants of the "prisoner's dilemma" thought experiment, defendants are often known to "flip" on their co-conspirators, and police seek out people with lower-level criminal charges to leverage them against higher-value targets (Natapoff, 2009). Such "snitching" situations are enabled in part by the "substantial assistance" provisions of the U.S. Sentencing Guidelines and are regularly employed in criminal law (Knizhnik, 2015). Practically, this means that criminal defendants who provide valuable information to prosecutors may be "compensated" with a sentence below that calculated by the Guidelines' sentencing range or below any mandatory minimum sentencing. As legal scholar Shana Knizhnik articulates, this has created a system in which "defendants are incentivized to incriminate themselves and as many others as possible, all without any guarantee that their cooperation will actually result in a lesser sentence" (Knizhnik, 2015, p. 1722). Asymmetries in information, power, and discretion thus may lead defendants to "over-cooperate" toward uncertain gain (Knizhnik, 2015).

The motivation for favorable state treatment also implies the threat of *unfavorable* treatment—that is, punishment. Defendants may be threatened with charge stacking or gang sentencing enhancements unless they snitch. Individuals in statuses of legal precarity, such as those on parole or

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

probation, are thus at particular risk of coercion into deputization—a situation that reinscribes entrenched inequalities (see Hypothesis 4).

Financial and competitive interests

The state may directly remunerate deputies for useful information, such as through a "finder's fee" (i.e., a proportion of the money collected because of the deputy's report). For example, New York City's Citizens Air Complaint Program encourages civilians to submit video of trucks idling and compensates them with 25% of any fine collected (CBS New York, 2015). At least one "citizen reporter," disguised as a tourist to avoid confrontation with truck drivers, earned $64,000 reporting idlers in 2021 (Wilson, 2022).

Alternatively, the state may financially penalize deputies for *failure* to report. Historically, states imposed financial penalties on entire communities if they failed to apprehend someone who broke the law (e.g., they failed to perform the collective duty required by the frankpledge system). Collectivizing these interests may encourage individuals to report on wrongdoers and to report on *each other* for failure to serve as deputies.

Professional identity

States may harness the commitments of certain professional groups to encourage or compel them to act as deputies, both formally and informally. In sociologist Elizabeth Chiarello's (2015) research on pharmacists' role in curbing prescription drug abuse, she details how retail pharmacists are professionally conscripted as frontline criminal justice workers. Under The Controlled Substances Act, they must simultaneously "do medicine" and "do law"—attending to patients' health care needs while also becoming legally responsible for not dispensing prescription drugs that they believe, in good faith, are being abused or diverted (in this they are aided by prescription drug monitoring programs [PDMPs], a surveillance technology initially designed for law enforcement use). In the face of what Chiarello terms "discrepant institutional logics," pharmacists sometimes experience great ambivalence and frustration in fulfilling these roles.

Another case is Truckers Against Trafficking (TAT), a nonprofit coalition of truckers trained to intervene in human trafficking for forced labor or commercial sex. Because trafficking often occurs at truck stops, truckers are considered well-placed as "the eyes and ears of our nation's highways … in a unique position to make a difference" (Truckers Against Trafficking, n.d.). To aid efforts to intervene and rescue victims of human trafficking, TAT provides a variety of training programs that seek to "raise up a mobile army of transportation professionals to assist law enforcement in the recognition and reporting of human trafficking, in order to aid in the recovery of victims and the arrest of their perpetrators" (Truckers Against Trafficking, n.d.).

To date, over 800,000 truckers have registered as "Truckers Against Trafficking." States invoke several methods to turn truckers into surveillance deputies: they create training materials (such as a comic book called "Highway Justice" in which hero Jake Brakefield learns to spot and deliver traffickers to the FBI); they give truckers who report sex work the right to "cut the line" at inspection stations; and they attach TAT training requirements to the provision of commercial drivers' licenses (Goble, 2018). The program further incentivizes truckers with a way to rehabilitate their rather unpopular public image through service as surveillors (Levy, 2022). The result is a significant increase in reports of sex work; at the same time, it raises questions about who is targeted for reporting (particularly, there are concerns about consensual sex workers and LGBTQ people) and what motivates truckers to report (e.g., as a means of coercion or retaliation against vulnerable individuals) (Balay, 2018).

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

Interpersonal and ideological motivations

Deputies may be motivated to report as a form of revenge or interpersonal leverage. Family members, friends, and romantic partners are frequently privy to one another's private—and perhaps incriminating—data (Barocas & Levy, 2020; Levy & Schneier, 2020). As sociologist Spencer Headworth (2021) outlines, welfare fraud investigators frequently exploit clients' social networks to extract information, relying on both elective cooperation and coercion. Headworth finds envy is a major driver of voluntary fraud reporting—friends, family members, and neighbors may call welfare fraud hotlines and report on acquaintances who informants feel are receiving unfairly high benefits.

Similarly, in Freed et al.'s (2017) study of intimate partner abuse, individuals threatened the possibility of reporting their partner or family's immigration status to maintain control. The VOICE hotline, noted above, ostensibly intended "to assist victims of crimes committed by criminal aliens" (U.S. Department of Homeland Security, 2017), saw reports of a wide variety of family, neighborhood, business, and interpersonal disputes. One caller reported a family member who would not let her see her granddaughter. Another reported his wife, who he said was falsely accusing him of domestic violence to obtain legal residency. Still others targeted spouses who had committed adultery or abused their children (O'Connor & Rivero, 2017).

In another striking example, in February 2022, the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) advertised a Valentine's Day campaign encouraging people to report ex-partners for illegal firearm possession. Its exhortation that "Valentine's Day can still be fun even if you broke up" explicitly invokes a would-be deputy's desire for interpersonal revenge (Figure 3).

Further, ideological alignment with, or sense of duty to, the state—whether through a general perception of the state's legitimacy or agreement with its specific surveillance goals—may motivate participation. Deputies may view reporting on their peers as a "civic duty," akin to paying taxes, serving on a jury, or completing military service, connecting the duty to report to the protection of their community. These motivations package surveillant behaviors with emotional commitments and logics of care, and they may emphasize the negative consequences to victims of crime (Levy, 2014; Stark & Levy, 2018). Appeals to deputization commonly appeal to these themes, as seen in the Department of Homeland Security's "If You See Something, Say Something" messaging, deployed after September 11, 2001, which implore civilians to perform surveillance in the name of preventing terrorism (Figure 4).

The widespread availability of digital records has created new opportunities for community "digilantes" to collect and post information about local crime, often rooted in the sense that a grassroots approach is superior to traditional modes of public safety and mainstream media (Lageson, 2020). Using blogs, social media sites, and Nextdoor threads (Kurwa, 2019), digilantes post mugshots, doorbell camera footage, and links to public police and court records in an effort to leverage government transparency in the pursuit of self and community protection.

Finally, not to be minimized, the desire for entertainment may drive deputies' activity. Bentham again foresaw the power of interest and curiosity to motivate reporting by visitors to the inspection station:

> …I must not overlook that system of inspection, which, however little heeded, will not be the less useful and efficacious: I mean, the part which [visiting] individuals may be disposed to take in the business, without intending, perhaps, or even without thinking of, any other effects of their visits, than *the gratification of their own particular curiosity*.
>
> (Bentham, Letter VI, 1995 [1787]; emphasis added)

Bentham predicted that "as a matter of course… the doors of [panoptic] establishments will be… thrown wide open to the body of the curious at large—the great *open committee* of the tribunal of

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

FIGURE 3 Image from ATF Instagram. *Source*: https://www.instagram.com/p/CZ9WjChMQCt/.

FIGURE 4 Image from the Department of Homeland Security's "If You See Something, Say Something" website. *Source*: https://www.dhs.gov/see-something-say-something.

the world." In other words, nosy civilian busybodies as well as state representatives would operate as effective inspectors.

More recently, pharmacists in Chiarello's study, tasked with reporting suspected drug abusers through state prescription monitoring programs, described a sense of exhilaration: "Sometimes it's fun. …Getting the people who try to pass fake scripts… I love to catch them," said one. They continued, "We coordinated with the police. We had it all set up so that, you know, we filled the prescription. We gave it to them and as they're walking out the door, the cops are sitting out there waiting… It's fun… we were part of solving a little bit of a problem" (Chiarello, 2015, p. 101). Similar dynamics underlie some individuals' desire to donate their own

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

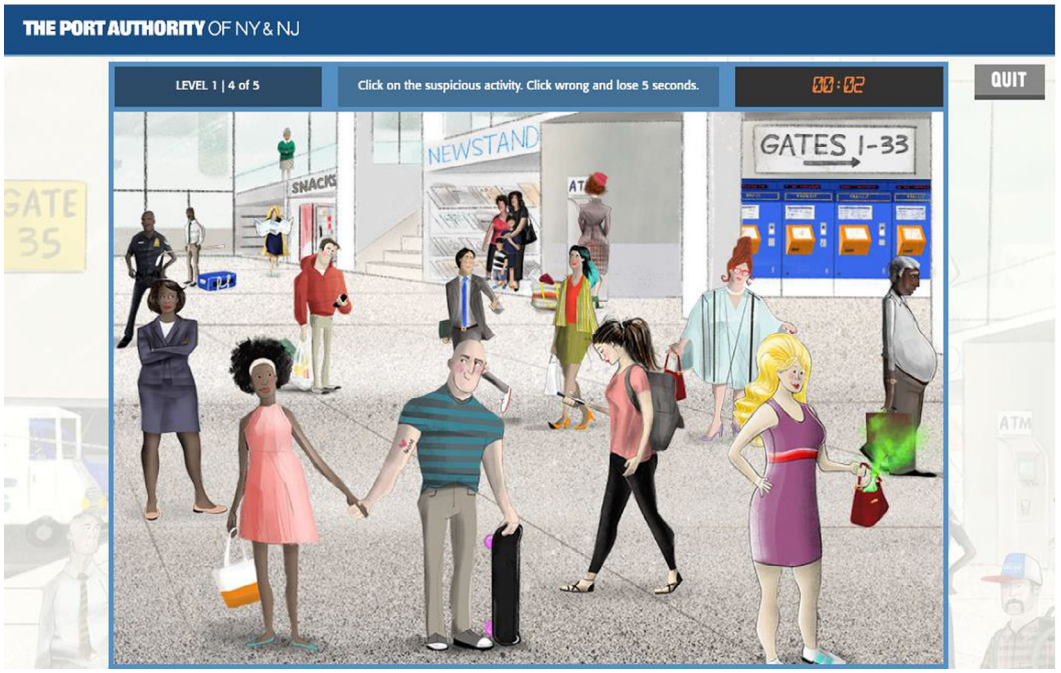

FIGURE 5 Image of "Safety Hero" From Port Authority of NY and NJ. *Source*: http://www.lookoutforsafety.com/game.html.

DNA to assist in solving cold cases (Lageson, 2019). These internal motivations give the state another chance to capitalize.

Elements of gamification in some reporting systems amplify this motivation for some deputies. As Fourcade and Johns (2020) explain, platforms employ psycho-social strategies and campaigns to draw people in and form habits by drumming up reciprocity and participation through notifications and rewards. For example, the Port Authority of New York and New Jersey's "Look Out for Safety" program deputizes commuters in the name of public safety.

The program's website offers training tips so that civilians know what to look for (that is, what information will be useful to police), bracketed into the categories "Suspicious activity," "Not quite right," and "Look out for yourself and others." Each includes specific examples like cars with weighted trunks parked far away from entrances to transit hubs, people who seem to be waiting in the same place at the same time every day, chemical odors, and unattended objects. The site also tries to harness citizens' "gut response," telling people to trust their instincts that "a strange shape is strange" and that "weird is weird." Civilians are invited to play Safety Hero, a web-based video game that purports to put their instincts to the test by playing through scenarios featuring potentially suspicious activity (Figure 5; Safety Hero Website).

Reflecting back on our opening example, Ring doorbells offer a single case in which many potential interests of the state and the civilian converge—a feature that may partially explain the device's popularity. The state benefits when users voluntarily share footage with local police in the name of community safety, thereby decreasing governmental labor and resources while offering an attractive collective identity-building experience. Ring users, in turn, may secure favorable treatment (increased protection or faster police response time) by offering to aid in local police investigations. Ring users might also share footage to social media or to the state through ideological or interpersonal motivations, such as publicly shaming delivery drivers (Nguyen & Zelickson, 2022). More broadly, interest convergence provides another foundation for understanding the conditions that encourage surveillance deputization.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

While we stop short of hypothesizing a consistent causal direction underlying this phenomenon (e.g., that states' activities foment the interests of civilians in acting as deputies, or conversely that civilians' inherent interest in surveillance causes state to respond by institutionalizing such programs), questions about causality and directionality of interest convergence are ripe for empirical investigation. As surveillance scholar Gary Marx (2016) reminds us, surveillance must always be understood in the social context (interpersonal, structural, sociolegal, and sociotechnical) in which it takes place. When the state enlists an army of human surveillance deputies in its cause—including nosy neighbors, spurned lovers, thrill-seeking vigilantes, and people motivated by personal safety and the welfare of their communities—we are left in a murky sociolegal middle ground.

HYPOTHESIS 2: LEGAL INSTITUTIONALIZATION

Formal law augments and encourages surveillance deputization in at least three ways. First, formal legal requirements for the constitutionality of state-initiated searches of people and their effects can be circumvented by legal doctrines that allow private citizens to surveil one another, and then voluntarily provide that information to the state (Heydari, 2022). As legal scholar Tamar Megiddo describes, crowdsourcing information collection allows government "to wash clean the stain of encroaching on the democratic checks that prevent them from directly collecting the information themselves" (Megiddo, 2023, p. 69). When private citizens voluntarily take on the task of surveillance, the state no longer requires a search warrant nor carries the burden of probable cause. Such partnerships distort the Fourth Amendment because private companies and persons are not subject to the same constitutional constraints or public records laws as governmental agencies (Joh, 2017). Second, legislation can codify and encourage surveillance deputization through private enforcement, or what Jon Michaels and David Noll (2021) refer to as "vigilante federalism." Third, rapid advances in technology outpace legal responses, so even when existing law is used by the state to deputize, ambiguous or nonexistent law can encourage new, varied, and potentially intensified peer-to-peer surveillance.

Fourth Amendment exceptions

States may use deputies to evade legal requirements that pose barriers to unfettered surveillance. By offloading surveillance work onto non-state actors, the state can circumvent legal constraints because ordinary civilians are not subject to legal constraints on state intrusion into private life, such as the Fourth Amendment in the U.S., which limits the state's ability to access civilians' private information without probable cause.

Deputies dramatically expand the types of information the state can access without a warrant through consent and voluntary disclosure. While soliciting old-fashioned tips from community members is nothing new (and comports with the Fourth Amendment), devices like Ring allow police to access much closer-to-home surveillance footage. In 2019, Amazon wrote in a response letter to U.S. Senator Edward Markey "[t]he law does not require an evidentiary standard for local police to ask residents if they would like to voluntarily assist in an investigation" (Amazon, 2019). Of course, police can, and do, encourage this voluntary sharing. Promotional materials sent by Ring to local police departments explicitly suggest "particular phraseologies police should use in their footage requests from homeowners," to "bypass warrant processes" (Morris, 2021, p. 247). Amazon has also developed law enforcement tools embedded into its Neighbors app that allow police investigating a crime to simply "drag and create a box on a map—a 'geofence'—and the portal will then push a request for relevant footage to every Ring user within that box" (Morris, 2021, p. 248). The electronic request allows Ring users to automatically and voluntarily share their footage with police, with or without reviewing it first; therefore, the consent exception is met, and no warrant is required.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

By leveraging consent to access vastly more surveillance content, surveillance deputies are akin to an ever-present private civilian rendering of a "tiny constable" achieved through the "fantastic advances" (Lopez v. United States, 1963) in ubiquitous monitoring technology. Cell site location data, GPS trackers, sensor technology, and the like have animated much Fourth Amendment jurisprudence over the past decade (Carpenter v. U.S., 2018; Riley v. California, 2014; U.S. v. Jones, 2012). As Justice Alito noted in *U.S. v. Jones*, prior to digital tracking technologies, such ubiquitous state surveillance would have required "a very tiny constable… with incredible fortitude and patience" (U.S. v. Jones, 132S. Ct. 945, 958 (2012), Alito, J., concurring). Alito makes this facetious observation to suggest its impossibility—and to establish that expectations of privacy are contingent on what has, historically, been structurally, economically, and pragmatically realistic for the state to observe (Bankston & Soltani, 2013; Hartzog, 2014; Surden, 2007). Now these constraints are all but obviated by consensual and voluntary disclosures from surveillance deputies presiding over low-cost, always-on tracking technologies.

Put differently, the widespread use of surveillance deputies demonstrates that the binary the *Jones* court wrestled with is too simplistic: there *is* a longstanding, low-cost mechanism through which states have effectively deployed civilian constables in private spaces for many years, and in ways that obviate many of the economic and structural barriers to information collection that have historically limited state actors. The combination of this phenomenon with the proliferation of digital data collection infrastructure stands poised to drastically expand the dynamic of surveillance deputization and its effects on social life.

Community-state partnerships have, accordingly, expanded and taken on new forms centered on the procurement of digitally collected data and appeals to community members' sense of civic citizenship and moral community duty (Fong, 2021; Heydari, 2022). For example, it is now possible to register one's private home or business security camera with a local police department so that it can monitor and respond to the footage. The local police in Little Elm, Texas urge community members to enroll:

> Registering your system could help solve crimes, and keep our community safe, but the police are not always aware which residents may have this potentially critical information. The Little Elm Police Department is asking residents and businesses to register their privately owned surveillance camera systems. As we respond to criminal incidents, we may be able to use the information in this registry to gather footage from your security cameras to assist in the apprehension and prosecution of the criminals involved.
>
> (Town of Little Elm, n.d.)

Private enforcement

Surveillance deputization has also been expanded through "vigilante federalism," or the enactment of state laws that pass enforcement to private parties. Here, "state legislatures deputize private actors to wage and win the culture wars by targeting the likes of abortion providers, trans kids, and teachers who adopt inclusive curricula" (Michaels & Noll, 2021, p. 4). These new laws "have deputized private partisans to surveil neighbors, doctors, and teachers" (Michaels & Noll, 2021, p. 1) and further legitimize surveillance deputization.

For example, Texas' S.B. 8, originally designed to circumvent *Roe v. Wade*, allows private citizens to file private civil actions ("citizen suits") against anyone facilitating an abortion (Megiddo, 2023). This deputizes ordinary people to punish those seeking abortions via lawsuits against anyone who helps them access an abortion—doctors, nurses, partners, friends, and even Uber drivers who drive them to the clinic. Similar laws include Florida's Stop WOKE and Don't Say Gay Acts, which provide school employees, students, and teachers a private right of action if classroom content involves

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

themes of critical race theory or sexual orientation. In these scenarios, the power of the state in institutionalizing spying and reporting both incentivizes and legitimizes surveillance deputies.

Legal ambiguity

The recent wave of statutorily sanctioned private enforcement also comes as a response to a lack of federal oversight and regulation, argue Michaels and Noll (2021). This raises a third point regarding legal institutionalization: while state-sanctioned vigilantism almost surely encourages surveillance deputization, ambiguous and/or rapidly changing law may also create opportunity for intensified private surveillance.

Law and society literature has long asked how social actors interpret, construct, and invoke ambiguous law in a nascent area (Silbey, 2005) and how organizations respond to and apply ambiguous and emerging law (Edelman, 2004; Edelman et al., 1999; Edelman & Suchman, 1997). These kinds of questions take on new meaning for the relationship between law and surveillance deputization, particularly amidst technological capabilities that outpace Fourth Amendment law (Ferguson, 2017) or in rapidly changing legal environments, as in our current moment of "vigilante federalism." While individuals might develop their own legal consciousness to justify expanded opportunities to surveil (e.g., Lageson, 2017), organizations might also exploit vague or nonexistent law to encourage deputies to share information.

As it stands, this is a speculative theoretical question well suited for empirical study. For instance, under what legal conditions does surveillance deputization emerge? How do people who engage in personal surveillance or in the sharing of surveillance content with the state conceptualize the law and legal rights? How might surveillance deputization illuminate the relationship between the legal and the personal?

There is profit to be made at the nexus between civilians and the state. This involves not only the privatization of public functions, but also the mediation of the state/civilian relationship through profit-seeking technology, to which we now turn.

HYPOTHESIS 3: TECHNOLOGICAL MEDIATION

Surveillance deputization relies on voluntary participation of civilians. Digital tools have facilitated this phenomenon and have created new sets of incentives. Here, we describe two means by which private-sector technology companies generate profit from surveillance deputization: (1) by developing devices and tools used to cultivate and capitalize on consumer fears; and (2) by generating state partnerships that expand private surveillance.

Surveillance consumerism

In terms of technological development facilitating surveillance deputization, *consumption* has emerged as a key mode of managing risk, fear, and insecurity. Science and technology studies scholar Torin Monahan describes the construction of the "insecurity subject": an "ideal citizen who can respond to the uncertainties of modern life without relying on the state. This insecurity subject anticipates risks and minimizes them through consumption" (Monahan, 2010, p. 2). By creating insecurity subjects, corporations construct risks, then offer surveillance products to ameliorate those risks (Draper, 2019); consumers then attempt to create and ensure their own safety through the purchase of products, apps, and services (Monahan, 2010). In other words, marketers of consumer technology aggravate and capitalize on cultures of fear and risk, positioning their devices and services as essential tools for protection

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

against danger (Haggerty, 2003; O'Malley, 2010; Stark & Levy, 2018). A new suite of products that emphasize analytics, security, and "big data" have followed suit (Talesh & Cunningham, 2021).

In 2003, surveillance scholar Kevin Haggerty tallied a list of products marketed in the name of personal crime prevention: "personal alarms, access controls, steering wheel locks, pepper spray, gated communities, guard dogs, bullet proof vests and cars, cellular phones, instruction in martial arts, car alarms, surveillance cameras, handguns, motion-sensitive lighting, vehicle geographic positions systems [GPS], home alarms (infrared, ultrasonic, photoelectric, and audio sensor), personal electronic monitors, motion detectors, missing child kits, private security services, light timers, window bars, fencing, safes, and tasers" (Haggerty, 2003, p. 194). The scope, scale, and capabilities of such technologies have continued to proliferate in the ensuing 20 years. Luke Stark and Karen Levy (2018) describe the subject position of the "surveillant consumer" who purchases devices and services to collect data about those around them to manage uncertainty and risk. Consumer-driven responses to risk do not require state action; rather, individual consumers can use market tools and products (like nannycams, "luxury surveillance" products (Gilliard & Golumbia, 2021), wearable health trackers, and other devices) to organize their responses to individual and collective fears (Levy, Kilgour, & Berridge, 2019).

The ability to create relatively inexpensive surveillance networks also encourages responsibilized citizens to engage in "controlwork" (Koskela, 2011) through consumption practices that produce surveillance data. Controlwork is increasingly "platformed" or "crowdsourced" (Megiddo, 2023) on applications like Nextdoor. Further, many consumer products to alleviate insecurity are networked digital technologies, including "smart" home security sensors, doorbell cameras that integrate facial recognition capabilities, crime watch and notification apps that rely on user-generated content, platforms and hotlines that crowdsource intelligence, and the like.

In 2016, the startup sp0n launched an app called Vigilante in New York City (Lin & Baker, 2020). The app's goal was to aggregate and broadcast 911 call alerts to users in the geographic vicinity of the 911 call and to allow users to report incidents to others in real-time. Users close to the location of the report were encouraged to capture live video from the scenes of crimes in progress, uploading them using the app. Later re-branded as "Citizen," the product became the top-ranked news app in 2020 with more than 7 million users (Kim, 2021). Soon, the NYPD announced a similar app of its own, StepForward (Moore & O'Neill, 2023).

The merger of the structural and cultural forces that brought about a focus on risk, control, and responsibilization, along with the consumerization of surveillance capability and concomitant emotional insecurity marketed by technology companies, has created fertile ground for the expansion of state power into social relations by facilitating governmental access into previously private spaces. Crucially, the commodification of risk and the responsibilization of the consumer do not merely substitute state power, nor do they fully displace the function of the state. Rather, they *supplement* state power by providing an additional set of human and digital resources that support state control. Civilians are not simply internalizing state surveillance goals, but rather are voluntarily extending the capabilities of the state into new, private spaces, including their cell phone GPS data, live video footage taken from their front doors, and even their DNA.

Public-private surveillance partnerships

The state itself is an indirect consumer of surveillance technologies: these "private security" tools facilitate individual consumers' surveillance of one another, feeding data captured or contributed by civilians back to the state via data sharing agreements and arrangements (for instance, in Detroit's Green Light program, businesses provide surveillance footage to police in exchange for access to cameras). In surveillance deputization, the state retains its central surveillant role, but is aided greatly by the purchasing power and participation of civilians. Both the state and the private sector benefit

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

through fostering security consumption, generating profit for technology companies (Zuboff, 2019), and markedly expanding state surveillance abilities.

Automated license plate readers (ALPRs), for instance, automate and expand the range of data capture possibilities in driving contexts. ALPRs use cameras and computer software to scan the license plates of all cars in a given vicinity. ALPRs may be stationary (e.g., installed on poles) or mobile (e.g., mounted on a police cruiser or a handheld device), and they are able to link additional information to a car, logging the date, time, and GPS coordinates of the image and sometimes including photos of the car and its passengers (Diaz & Levinson-Waldman, 2020). ALPR technology is proliferating—according to the Department of Justice's Bureau of Justice Statistics, 93 percent of police departments in cities with populations over one million use ALPRs, and according to a recent national survey of law enforcement agencies, two thirds of police agencies with 100 or more officers use ALPRs (Oliver & Kugler, 2021; see also Roberts & Casanova, 2012, Slobogin & Brayne, 2023). As with Ring doorbells, a growing number of memorandums of understanding (MOUs) formalize the transfer of data from homeowner-association-provided ALPRs to local police departments (Kelley & Guariglia, 2020). Both privately designed and vended tools serve and extend police surveillance, exemplifying the growing role of the private sector in public policing.

In this context, consumer technology provides crucial infrastructure that reduces the friction involved in acting as a deputy. Surveillance data are passively captured and increasingly available, allowing deputization to occur cheaply and at scale. While earlier iterations of public-private partnerships centered on outside actors providing technological solutions for government policies (Feeley, 2002), today's penal entrepreneurialism is marked by an opportunistic model of private sector innovation that is developed independently from the state and then marketed and sold to public agencies and surveillant consumers (Corda & Lageson, 2020). The supply of new devices meant to aid public safety projects outpaces state requests for such tools (e.g., Brayne, 2021). In this reversal, technology companies elevate surveillance products, which are legitimized (and then encouraged) by the state. In this sense, the state becomes another tech consumer, but still often relies on permissive civilian users to supply data. For example, when conducting research on police use of surveillance technology, sociologist Sarah Brayne writes:

> Prior to the first of these [surveillance technology] conferences, I assumed that law enforcement representatives would ask surveillance company representatives how their platforms could help police achieve their goals. …[But] instead of filling analytic gaps or technical voids identified by law enforcement, software representatives helped create new kinds of institutional demand to sell lucrative platform licensing agreements.
>
> (Brayne, 2021, p. 26)

As Garland (2001) argues, "this embrace of the private sector is liable to have fateful consequences, as it begins to transform the character of the crime control field, setting up new interests and incentives, creating new inequalities of access and provision, and facilitating a process of penal and security expansion that might otherwise have been more constrained" (p. 117).

In sum, the proliferation of surveillant consumer technology influences who performs surveillance and how these functions are accomplished. In so doing, public-private relationships are reconfigured through the individualization of social problems. Private corporations have identified as a new profit opportunity in those areas of life, information, and data that are beyond the scope of what the state can easily access without the cooperation of civilians. The appetite to capitalize on these profit opportunities results in the expansion of the surveillance tech market, which often emphasizes personal safety and individual protection. These examples demonstrate that surveillance

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

deputization, though deeply rooted in history, may be accelerated by the digital turn and the creation of new profit incentives.

HYPOTHESIS 4: SOCIAL STRATIFICATION

There is a voluminous sociolegal literature on how the legal system both reflects and reproduces social inequalities, both in terms of selection (i.e., differential exposure to the criminal legal system across axes of social differentiation) and treatment effects (i.e., the impact of criminal legal system involvement). There is not yet a substantial—let alone systematic—body of evidence regarding surveillance deputization and its association with social inequality and stratification.

On one hand, deputization may exacerbate pre-existing inequalities by intensifying surveillance of structurally disadvantaged groups, coercing system-involved people into serving as deputies, limiting avenues for recourse, and encouraging vigilantism against weaker opponents. On the other hand, surveillance deputization may in some cases reduce or disrupt entrenched inequalities by providing new opportunities for collective resistance and democratizing surveillance. It is an open empirical question whether and under what conditions surveillance deputization disrupts or ossifies existing structures of inequality. We explore each of these possibilities below.

Increase inequality

Through surveillance deputization, interpersonal relations—from petty everyday grievances to efforts at community care—are wielded as instruments of state power. These are underappreciated but real and important avenues through which the state can exert power on individuals. In the digital age, the ubiquitous use of data-intensive technology and personal surveillance technologies represent both the privatization and expansion of control in governmental and institutional contexts. The common refrain of requesting civilian "eyes and ears" to support state efforts at upholding community safety takes on new depth in a time when that frequently means providing access to extensive, digitally mediated information that significantly extends state surveillance capacity.

Surveillance deputization may reinforce existing structural inequalities by intensifying effects on marginalized populations. As Monahan (2010, p. 10) reminds us, "the profusion of surveillance technologies throughout societies in no way indicates the democratization of surveillance" (see also Stuart 2020). Rather, surveillance is a form of "social sorting" (Lyon, 2002): a means of creating and reinforcing social differences, assessing risks, and assigning worth. While surveillance is continually expanding, its penetration is unevenly distributed (Ericson & Haggerty, 1997; Fiske, 1998). As such, surveillance deputization may extend the reach of the state's power and intensify effects on the marginalized in at least three ways.

First, well-documented implicit and explicit biases motivate reporting behaviors on social platforms like Nextdoor (Reynald, 2019)–where Black people are more likely to be reported as suspicious than White people, regardless of behavior (Eberhardt, 2020)–and San Francisco's BART Watch, a security app that allows riders to send alerts to BART police, with racially biased results (BondGraham, 2015). Platformed opportunities for racial gatekeeping reinforce the association people have between Blackness and crime (Eberhardt, 2020; Quillian & Pager, 2001), which have real consequences in the criminal legal system from policing to sentencing decisions.

Here, unfettered surveillance deputization capitalizes on fears of the "other" (Cheney-Lippold, 2017; Hempel, 2017) and directs surveillance toward racially minoritized and economically marginalized people (Benjamin, 2019; Browne, 2015; Eubanks, 2018; Hinton & Cook, 2021; Noble, 2018). As critics have noted, these platforms "more often than not descend into a security politics of neighborhood watch activities, without any regard to the actual presence of crime or

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

observed criminality" (Bloch, 2021; see also Calacci et al., 2022). Amplifying paranoia around crime is not a colorblind practice and the burden of these fears is not borne equally.

Surveillance deputization and its associated legal frameworks can also systematically disadvantage vulnerable groups, such as victims of spousal abuse. For example, under the aforementioned Texas S.B. 8, a man who had a history of abusing his wife sued her best friends for helping her obtain an abortion (the friends later counter-sued). Surveillance deputization can also lead to misidentification, such as the misidentification of an arson suspect by the Citizen app, perhaps spurred by a $30,000 bounty for information (Morrison, 2021). Crowdsourced enforcement also enables ideologically motivated individuals with extremist political views to play vigilante and use reporting as a tool of harassment against vulnerable groups, while harassment on digital platforms allows people to reinforce ideological membership while silencing dissenting views (Marwick, 2021).

Second, recalling Hypothesis 1, those in vulnerable legal positions may be at higher risk of becoming coerced into serving as deputies. For example, individuals on parole or probation or those in the early stages of criminal legal involvement may be threatened with apprehension, charge stacking, or gang sentencing enhancements unless they provide information about others to the police. Since involvement in the criminal legal system is highly stratified by race and class, the incentives around and practices of surveillance deputization may be similarly disproportionately distributed, exacerbating preexisting inequalities. However, this is an empirical question. An alternate hypothesis is that individuals and groups who do not trust the police or formal institutions more generally (Brayne, 2014)—which include individuals with prior criminal legal contact, racially minoritized individuals, and economically marginalized populations—are less likely to report crimes (Sampson & Bartusch, 1998) and may be less likely to act as surveillance deputies.

Third, surveillance deputization circumvents individuals' already limited capacity to seek recourse for biased enforcement. State actors commonly conduct surveillance and enforce laws in ways that propagate racial subjugation with few avenues for recourse (Browne, 2015)—but those avenues are all but erased when it comes to deputized members of the public. Private technology companies that provide the tools for surveillance deputization are outside the bounds of the Fourth Amendment, and the diffuse (sometimes anonymous) nature of reporting can preclude civil rights claims brought against state actors.

Finally, recent laws enabling surveillance deputization makes it possible for classes of people who are legally protected by the state to be targeted and harmed by private actors through legal workarounds, in ways that both reflect and reproduce political inequalities. As Michaels and Noll write, these new laws have "stripped historically subordinated groups and their allies of the ability to engage in constitutionally protected conduct; they've empowered private actors to enforce traditional understandings of caste and status in the public sphere; and they've further legitimated political violence as an acceptable component of civic discourse" (Michaels & Noll, 2021, p. 4).

Whether and under what conditions expanded surveillance capabilities entrench state power and exacerbate the harms to already marginalized communities are open empirical questions, yet a substantial literature implies it is likely.

Reduce inequality

Technologically mediated platforms increase the ease with which community members might choose to inform on one another. However, the use of such digital platforms and portals *also* offers ripe ground for community members to turn the camera, instead, on state actors who engage in racist or otherwise discriminatory behaviors. In other words, surveillance deputization may open opportunities for collective resistance.

For instance, when Trump's anti-immigration VOICE hotline opened for reporting crimes committed by (in the Department of Homeland Security's terms) "criminal aliens," the hotline was reportedly trolled by people claiming UFO sightings and describing the plots of *X-Files* episodes

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

(BBC, 2017). Much the same happened in response to Texas's S.B. 8 when a whistleblower website created by an anti-abortion group was flooded with fake tips. One person even made a bot that submitted a false report every ten seconds and an iOS shortcut that allowed thousands of people to submit false reports (Pruitt Young, 2021). In another example, Ohio, facing a wave of unemployment claims, attempted to reduce the backlog by creating a fraud reporting website through which employers can report workers who have the opportunity to work but refuse to, making them ineligible for unemployment insurance (Marr, 2020). The portal drew critique from labor rights advocates who emphasized the inhumanity of employers snitching on employees refusing to work in unsafe conditions. In May 2020, an anonymous hacker released a script that enabled people to flood the site with "junk data" as a means of obfuscatory protest (Brunton & Nissenbaum, 2015), making it more difficult for the state to process real submissions and deny workers their benefits (Rose, 2020a). State officials soon strengthened their authentication protocols, but the hacker who wrote the original code worked to update the script, saying "What I'm hoping is that, whether people use this exact code or not, they see it's possible for people to take direct action against these sort of snitch programs, and that making and spreading small tools like this amongst ourselves can help" (Rose, 2020a). Shortly thereafter, Ohio removed the form and stopped denying claims based on a refusal to return to work (Rose, 2020b).

Here we see that state reliance on surveillance deputies can backfire, and that technological mediation (e.g., a centralized web-based reporting mechanism) can open state vulnerabilities. As Marx shows in his classic work *Undercover: Police Surveillance in America* (Marx, 1989), surveillance is context-specific and entails both intended and unintended consequences. Although Marx argues covert policing is ambivalent, he suggests ways it might uncover crimes typically neglected by "street-level" policing—such as white-collar crimes—thus remedying some of the class bias in policing. Relatedly, Newell's (2021) work on police bystander videos provide an example of the mobilization of digital technologies by concerned civilians to surveil police who violate constitutional rights.

By providing means for individuals to marshal the apparatus of the state for personal reasons, surveillance deputization provides a way for individuals to "bargain in the shadow of" disclosure to the state as a means of managing their interpersonal dealings (Mnookin & Kornhauser, 1979). The most egregious instance of this dynamic is blackmail, in which a reporter lords exposure of compromising information over a target for purposes of exploitation. But the specter of disclosure may also serve to prosocially rebalance asymmetric power relations between individuals (Headworth, 2021), as in government whistleblowing (Johnson, 2003) or in the #MeToo movement (Lageson & Kaplun, 2021).

Because almost anyone—regardless of structural position—may serve as a surveillance deputy, certain instantiations may represent, to some degree, a leveling of surveillance within certain contexts. That said, we caution against the interpretation that platformed surveillance deputization is *inherently* democratizing. As Fourcade and Johns note in their work on machine learning platforms, "The kinds of ruptures and reorderings engineered through machine learning do not, however, create equal opportunities for value creation and accumulation, any more than they are inherently liberating or democratizing" (Fourcade & Johns, 2020).

In sum, it is possible that empirical instantiations of surveillance deputization may represent deepenings or disruptions in existing lines of social stratification and structures of inequality. Our tentative argument is that surveillance deputization, on net, tends to reinforce existing inequalities, but many open empirical questions remain about whether and under what conditions it reduces or reinforces pre-existing power relations. As such, this sociolegal phenomenon requires future empirical study. If our hypotheses find support through empirical study, they imply significant changes in the contours of the surveillance landscape and attendant modern legal order.

CONCLUSIONS AND FUTURE RESEARCH

In 1969, Lawrence Friedman wrote in the *Law & Society Review* that "legal institutions are responsive to social change; moreover, they have a definite role, rather poorly understood, as instruments

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

that set off, monitor, or otherwise regulate the fact or pace of social change" (Friedman, 1969, p. 29). Today, social change is often facilitated by technological innovation, which in turn shifts how people conceive of their legal rights, how legal and non-legal institutions respond to new opportunities afforded by new technologies, and how formal law should, does, or fails to respond. Our aim in this article is to present a specific case—surveillance deputization—that is emblematic of a rapidly changing legal and technological environment and ripe for law and society inquiry.

The hypotheses we pose focus on a specific concept but have broader implications for the study of law and society. For instance, law and society scholarship has long studied how "ordinary people" make sense of law (Ewick & Silbey, 1998). We extend this inquiry by asking how ordinary people make sense of new technologies that directly interact with the state and legal regimes, as explored by our first hypothesis: that surveillance deputization is likely sustained when state and personal interests converge. Here, surveillance deputization becomes a mechanism for people to interact with state and legal institutions while also serving their own interests, potentially creating new forms of legal consciousness. We further interrogate the role of law in this relationship through our second hypothesis on legal institutionalization. Here, we illustrate how people may engage in a form of legal mobilization (McCann, 1994) by engaging in surveillance deputization: ordinary people may assist the state in securing evidence and access previously barred by law, ordinary people may engage in state-sanctioned private enforcement through filing lawsuits, and ordinary people can manipulate and leverage new tools to conduct peer-to-peer surveillance in a manner that quickly outpaces legal responses.

The adoption of everyday surveillance technology thus holds important consequences for relationships between the private sector and the state. Data are increasingly collected by civilians using digital tools designed by private companies and uploaded to private servers, making it possible for private vendors to hide behind trade secrecy and nondisclosure agreements to circumvent typical public-sector transparency requirements, ultimately reducing state accountability (Brauneis & Goodman, 2018). In other cases, they are generated and shared voluntarily, becoming both a consequence and an extension of legal ambiguities and Fourth Amendment workarounds.

Our last two hypotheses engage with law and society scholarship on neoliberalism, privatization, and social control. First, the dominance of the private sector in surveillance opportunities creates new avenues for both private companies and private people to take over what we might view as traditional state functions, such as crime control. For instance, recent law and society scholarship has described increasing shifts toward private policing (Bayley & Shearing, 1996; Button, 2017). Our final hypothesis—that unequal groups can use surveillance to gain power or leverage resistance—calls to mind recent debates in the field regarding surveillance as a "new visibility" (Thompson, 2005), where advances in communication technology leave people both simultaneously more powerful and more fragile, as well as the notion of "police's new visibility" as cameras are turned on officers by civilians (Goldsmith, 2010). As the examples we describe demonstrate, surveillance is not simply a top-down control mechanism performed by the state, but rather is a *participatory* practice that enrolls interested parties. The crux of surveillance deputies' impact is tied to instances when the motivations to surveil coalesce for both civilians and the state, as well as when the state actively encourages civilians to contribute their surveillant attention and attendant data collection to state objectives, creating a "voluntary panopticon" (Humphreys, 2011).

Thus, surveillance deputization might be viewed as something indicative of larger trends. For instance, Garland (2001) writes of the emergence of a new network of public-private partnerships aimed at crime prevention through the commercialization of public functions, and the rise of the private security industry that shifts responsibility for crime control from the state to the public. As sociologist Katherine Beckett (2001) describes, "the novelty of these preventative programs lies in their devolution of responsibility for crime control to private actors and their attempt to forge links between these actors and traditional criminal justice agencies, blurring the lines between public and private, state and non-state" (pp. 911–2; see also Shamir 2008). In the vein of public safety, Garland's (2001) view is of "interlocking and mutually conditioning patterns of action: the formal controls

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

exercised by the state's criminal justice agencies and *the informal social controls that are embedded in the everyday activities and interactions of civil society*" (p. 5; emphasis added). Surveillance deputization brings these informal social practices into clear view and clarifies how the state relies upon them for the expansion of its own power.

In describing the broader implications of this phenomenon, we aim to provide historical nuance. Surveillance deputization is a longstanding social process that has expanded with the proliferation of networked technologies. It is overdue for scrutiny from sociolegal scholars. Both the practices and stakes of surveillance deputization continue to grow in the digital age, as new technologies facilitate private data collection and firms find ways to profit from it. By turning our attention to this dynamic, we can better appreciate the entwinement of lateral surveillance with state and corporate power, the points of tension and ambiguity in existing legal doctrine, the uneven consequences of deputization for marginalized groups, and the prospect of new avenues for collective action.

Our theoretically driven hypotheses about the operation and implications of surveillance deputization vis-a-vis state power, technological mediation, and the law are supported by a sampling of suggestive illustrations of the phenomenon and its dynamics. Yet, we have not undertaken to empirically test these hypotheses, which remain speculative but, we hope, generative for further empirical investigation. Most critically, research is needed to establish the extent of surveillance deputization and to identify and measure the conditions under which it arises. Comparative research that identifies the interests of both states and civilians, the degree of their convergence, and the mechanisms through which deputization is induced and supported by state policies and by the affordances of technological systems, may be particularly fruitful. Scholars pursuing comparisons of deputization dynamics across political regimes may want to examine the ways that authoritarian regimes, such as those in Iran, China, and Russia, leverage surveillance deputization to entrench their power—and the ways citizens have undertaken countermeasures.

Moreover, future studies may seek to develop longitudinal data on how surveillance deputization has—and has not—changed over time, and with what effects. As surveillance is always context-specific (Marx, 2016), future empirical work should investigate the contexts in which surveillance deputization grows, contracts, and manifests in different ways, as well as the contexts in which surveillance deputization reflects, reduces, and/or reproduces social inequalities. It is also an open empirical question whether and how more traditional state surveillance functions, including policing strategies, change in light of digital technologies making more information available to them. For example, do police rely more or less on undercover work as other modalities of information gathering become more prevalent?

We are mindful that our hypotheses engage a rapidly changing environment and will likely evolve over time; this only reinforces the need for systematic, longitudinal data on the types and scope of surveillance deputization so that we might capture differences across contexts and settings. To borrow, one final time, from Edelman and Suchman, the concept "probably has not proceeded at an equal pace in all social settings, but to put this variation to good empirical use, we will need far more fine-grained observations than the current literature provides" (Edelman & Suchman, 1997, p. 984). Surveillance deputization has entered a new phase in the digital world, and we are just beginning to understand its effects. Research on the topic is poised to make strong contributions to law and society scholarship.

ACKNOWLEDGMENTS

We gratefully acknowledge Lauren Kilgour, Brad Silberzahn, and Letta Page for their valuable suggestions and contributions to this work. We thank Wendy Espeland, Ron Lee, and participants at the 2020 Privacy Law Scholars Conference, the 2022 American Sociological Association Annual Meeting, and the Cornell Artificial Intelligence, Policy, and Practice (AIPP) Working Group for helpful feedback on earlier versions of this manuscript. The authors are grateful for support from the John D. and Catherine T. MacArthur Foundation, the American Bar Foundation, and grant P2CHD042849, awarded to the Population Research Center at The University of Texas at Austin.

ORCID

Sarah Lageson https://orcid.org/0000-0002-4108-4365

REFERENCES

Amazon. 2019. Response Letter to Senator Markey November 1, 2019 https://www.markey.senate.gov/imo/media/doc/Response%20Letter_Ring_Senator%20Markey%2011.01.2019.pdf

Andrejevic, Mark. 2006. "The Discipline of Watching: Detection, Risk, and Lateral Surveillance." *Critical Studies in Media Communication* 23(5): 391–407.

Ayers, Edward L. 1984. *Vengeance and Justice: Crime and Punishment in the 19th Century American South*. New York: Oxford University Press.

Balay, Anne. 2018. *Semi Queer: Inside the World of Gay, Trans, and Black Truck Drivers*. Chapel Hill: University of North Carolina Press.

Bankston, Kevin S., and Ashkan Soltani. 2013. "Tiny Constables and the Cost of Surveillance: Making Cents out of United States v. Jones." *The Yale Law Journal* 123: 335–357.

Barocas, Solon, and Karen Levy. 2020. "Privacy Dependencies." *Washington Law Review* 95(2): 555–616.

Bayley, David H., and Clifford D. Shearing. 1996. "The Future of Policing." *Law and Society Review* 30(3): 585–606.

BBC. 2017. Trump's Immigrant Crime Hotline Trolled with Calls about Aliens and UFOs April 27, 2017 https://www.bbc.com/news/world-us-canada-39731085

Beckett, Katherine. 2001. "Crime and Control in the Culture of Late Modernity." *Law & Society Review* 35(4): 899–930.

Benjamin, Ruha. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Bentham, Jeremy. 1995 [1787]. In *The Panopticon Writings*, edited by Miran Božovič. London: Verso Books.

Bergemann, Patrick. 2021. *Judge Thy Neighbor: Denunciations in the Spanish Inquisition, Romanov Russia, and Nazi Germany*. New York: Columbia University Press.

Blackett, Richard J. M. 2018. *The Captive's Quest for Freedom: Fugitive Slaves, the 1850 Fugitive Slave Law, and the Politics of Slavery*. Cambridge: Cambridge University Press.

Bloch, Stefano. 2021. How Surveillance Technologies and Neighborhood Watch Apps Are Capturing and Reflecting Communities' Prejudices. *United States Politics and Policy* September 10, 2021 https://blogs.lse.ac.uk/usappblog/2021/09/10/how-surveillance-technologies-and-neighborhood-watch-apps-are-capturing-and-reflecting-communities-prejudices/

Bloom, Robert M. 2002. *Ratting: The Use and Abuse of Informants in the American Justice System*. Westport: Greenwood Publishing Group.

BondGraham, Darwin. 2015. BART Riders Racially Profile Via Smartphone App. *East Bay Express* August 5, 2015 https://eastbayexpress.com/bart-riders-racially-profile-via-smartphone-app-2-1/

Brauneis, Robert, and Ellen P. Goodman. 2018. "Algorithmic Transparency for the Smart City." *Yale Journal of Law & Technology* 20: 103–176.

Brayne, Sarah. 2014. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." *American Sociological Review* 79(3): 367–391.

Brayne, Sarah. 2021. *Predict and Surveil: Data, Discretion, and the Future of Policing*. New York: Oxford University Press.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press.

Button, Mark. 2017. *Private Policing*. Oxfordshire: Routledge.

Calacci, Dan, Jeffrey J. Shen, and Alex Pentland. 2022. "The Cop in Your Neighbor's Doorbell: Amazon Ring and the Spread of Participatory Mass Surveillance." *Proceedings of the ACM on Human-Computer Interaction Art.* 400: 1–47.

Carpenter v. United States. 2018. 138 S. Ct. 2206.

CBS New York. 2015. Council Member Wants to Train Citizens to Spot, Turn-In Illegal Idlers. *CBS News* March 10, 2015 https://www.cbsnews.com/newyork/news/council-member-wants-to-train-citizens-to-spot-turn-in-illegal-idlers/

CBS New York. 2020. Coronavirus Crackdown: New Yorkers Asked to Report Social Distancing Violations. *CBS News* April 19, 2020 https://www.cbsnews.com/newyork/news/new-york-city-report-social-distancing-violations/

Cheney-Lippold, John. 2017. *We Are Data*. New York, NY: New York University Press.

Chiarello, Elizabeth. 2015. "The War on Drugs Comes to the Pharmacy Counter: Frontline Work in the Shadow of Discrepant Institutional Logics." *Law & Social Inquiry* 40(1): 86–122.

Corda, Alessandro, and Sarah E. Lageson. 2020. "Disordered Punishment: Workaround Technologies of Criminal Records Disclosure and the Rise of a New Penal Entrepreneurialism." *The British Journal of Criminology* 60(2): 245–264.

Diaz, Angel, and Rachel Levinson-Waldman. 2020. Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use. *Brennan Center for Justice* September 10, 2020 https://www.brennancenter.org/our-work/research-reports/automatic-license-plate-readers-legal-status-and-policy-recommendations

Donnelly, Richard C. 1951. "Judicial Control of Informants, Spies, Stool Pigeons, and Agent Provocateurs." *The Yale Law Journal* 60(7): 1091–1131.

Draper, Nora. 2019. "Reputation Anxiety: Consumer Background Checks and the Cultivation of Risk." *Communication, Culture, and Critique* 12(1): 36–52.

Durkheim, Émile [1893]. 1996. *The Division of Labor in Society*. New York: The Free Press.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

Eberhardt, Jennifer. 2020. *Biased: Uncovering the Hidden Prejudice that Shapes What We See, Think, and Do*. New York: Penguin Books.
Edelman, Lauren B. 2004. "Rivers of Law and Contested Terrain: A Law and Society Approach to Economic Rationality." *Law and Society Review* 38: 181–198.
Edelman, Lauren B., and Mark C. Suchman. 1997. "The Legal Environments of Organizations." *Annual Review of Sociology* 23: 479–515.
Edelman, Lauren B., and Mark C. Suchman. 1999. "When the "Haves" Hold Court: Speculations on the Organizational Internalization of Law." *Law and Society Review* 33(4): 941–991.
Edelman, Lauren B., Christopher Uggen, and Howard S. Erlanger. 1999. "The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth." *American Journal of Sociology* 105: 406–454.
Ericson, Richard V., and Kevin D. Haggerty. 1997. *Policing the Risk Society*. Toronto: University of Toronto Press.
Erikson, Kai. 1966. *Wayward Puritans: A Study in the Sociology of Deviance*. London: John Wiley & Sons, Inc.
Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.
Ewick, Patricia, and Susan S. Silbey. 1998. *The Common Place of Law: Stories from Everyday Life*. Chicago: University of Chicago Press.
Feeley, Malcolm M. 2002. "Entrepreneurs of Punishment: The Legacy of Privatization." *Punishment & Society* 4(3): 321–344.
Ferguson, Andrew. 2017. "The 'Smart' Fourth Amendment." *Cornell Law Review* 102: 547–632.
Fiske, John. 1998. "Surveilling the City: Whiteness, the Black Man and Democratic Totalitarianism." *Theory, Culture and Society* 15(2): 67–88.
Fong, Kelley. 2021. "Getting Eyes in the Home: Child Protective Services Investigations and State Surveillance of Family Life." *American Sociological Review* 85(4): 610–638.
Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Random House.
Fourcade, Marion, and Fleur Johns. 2020. "Loops, Ladders and Links: The Recursivity of Social and Machine Learning." *Theory and Society* 49(5–6): 803–832.
Fraser, Nancy. 1981. "Foucault on Modern Power: Empirical Insights and Normative Confusions." *Praxis International* 1(3): 272–287.
Freed, Diana, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders." *Proceedings of the ACM on Human-Computer Interaction* 1(CSCW): 1–22.
Friedman, Lawrence M. 1969. "Legal culture and social development." *Law and Society Review* 4(1): 29–44.
Galanter, Marc. 1974. "Why the Haves Come out Ahead: Speculations on the Limits of Legal Change." *Law and Society Review* 9: 95.
Garland, David. 1996. "The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society." *The British Journal of Criminology* 36(4): 445–471.
Garland, David. 2001. *The Culture of Control: Crime and Social Order in Contemporary Society*. New York: Oxford University Press.
Gilliard, Chris. 2021. A Black Woman Invented Home Security. Why Did it Go So Wrong? *WIRED* November 14, 2021 https://www.wired.com/story/black-inventor-home-security-system-surveillance/
Gilliard, Chris, and David Golumbia. 2021. Luxury Surveillance: People Pay a Premium for Tracking Technologies that Get Imposed Unwillingly on Others. *Real Life* July 6, 2021 https://reallifemag.com/luxury-surveillance/
Goble, Keith. 2018. States Pursue CDL Tie-in to Combat Human Trafficking. *Land Line Media* February 5, 2018 https://landline.media/states-cdl-combat-human-trafficking/
Goldsmith, Andrew John. 2010. "Policing's New Visibility." *The British journal of criminology* 50(5): 914–934.
Hadden, Sally E. 2003. *Slave Patrols: Law and Violence in Virginia and the Carolinas*. Cambridge: Harvard University Press.
Haggerty, Kevin D. 2003. "The Rationalities of Personal Crime Prevention." In *Risk and Morality*, edited by Richard V. Ericson and Aaron Doyle, 193–214. Toronto: University of Toronto Press.
Hall, Claire M. 2009. "An Army of Spies? The Gestapo Spy Network 1933—45." *Journal of Contemporary History* 44(2): 247–265.
Hartzog, Woodrow. 2014. "The Value of Modest Privacy Protections in a Hyper Social World." *Colorado Technology Law Journal* 12(2): 333–352.
Haskins, Caroline. 2021. Ring Now Has 350 Fire Departments in Its Neighborhood Surveillance Program. *Buzzfeed* June 9, 2021 https://www.buzzfeednews.com/article/carolinehaskins1/amazon-ring-partnered-with-350-fire-departments
Headworth, Spencer. 2021. *Policing Welfare*. Chicago: University of Chicago Press.
Hempel, Jessi. 2017. For Nextdoor, Eliminating Racism Is No Quick Fix. *WIRED* February 16, 2017 https://www.wired.com/2017/02/for-nextdoor-eliminating-racism-is-no-quick-fix/
Heydari, Farhang. 2022. "The Private Role in Public Safety." *George Washington Law Review* 90: 696–760.
Hinton, Elizabeth, and De Anza Cook. 2021. "The Mass Criminalization of Black Americans: A Historical Overview." *Annual Review of Criminology* 4(1): 261–286.
Humphreys, Lee. 2011. "Who's Watching Whom? A Study of Interactive Technology and Surveillance." *The Journal of Communication* 61(4): 575–595.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

Huseman, Hayato. 2021. Ring Neighbors Hits 10 Million Users, Gaining End-to-End Encryption Soon. Android Central https://www.androidcentral.com/ring-neighbors-hits-10-million-users-gaining-end-end-encryption-soon

Jackson, Bradford, Mike Hough, and Katherine Murray. 2012. "Compliance with the Law and Policing by Consent: Notes on Police and Legal Legitimacy." In *Legitimacy and Compliance in Criminal Justice* 29–49. London, UK: Routledge.

Jacobs, Jane. 1961. *The Death and Life of Great American Cities*. New York: Random House.

Joh, Elizabeth. 2017. "The Undue Influence of Surveillance Technology Companies in Policing." *New York University Law Review Online* 92: 19–47.

Johnson, Roberta Ann. 2003. *Whistleblowing: When it Works–and Why*. Boulder, Colorado: Lynne Rienner Publishers.

Kelley, Jason, and Matthew Guariglia. 2020. Things to Know Before Your Neighborhood Installs an Automated License. *Electronic Frontier Foundation* September 14, 2020 https://www.eff.org/deeplinks/2020/09/flock-license-plate-reader-homeowners-association-safe-problems

Kim, Granate. 2021. False Arrest, Racial Profiling: Why the Citizen App Is a Threat to Vulnerable Communities. Fast Company https://www.fastcompany.com/90657035/false-arrest-racial-profiling-why-the-citizen-app-is-a-threat-to-vulnerable-communities

Klehr, Harvey, and John Earl Haynes. 2022. "Informants by the Hundreds: FBI Penetration of the CPUSA." *American Communist History* 21(1–2): 1–24.

Knizhnik, Shana. 2015. "Failed Snitches and Sentencing Stitches: Substantial Assistance and the Cooperator's Dilemma." *NYU Law Review* 90(5): 1722–60.

Koskela, Hille. 2011. "Hijackers and Humble Servants: Individuals as Camwitnesses in Contemporary Controlwork." *Theoretical Criminology* 15(3): 269–282.

Kurwa, Rahim. 2019. "Building the Digitally Gated Community: The Case of Nextdoor." *Surveillance and Society* 17(1/2): 111–17.

LaFrance, Adrienne. 2017. When Bad News Was Printed on Milk Cartons. *The Atlantic* February 14, 2017 https://www.theatlantic.com/technology/archive/2017/02/when-bad-news-was-printed-on-milk-cartons/516675/

Lageson, Sarah Esther. 2017. "Crime Data, the Internet, and Free Speech: An Evolving Legal Consciousness." *Law and Society Review* 51(1): 8–41.

Lageson, Sarah Esther. 2019. Privacy Concerns Don't Stop People from Putting Their DNA on the Internet to Help Solve Crimes. *The Conversation* June 7, 2019 http://theconversation.com/privacy-concerns-dont-stop-people-from-putting-their-dna-on-the-internet-to-help-solve-crimes-118091

Lageson, Sarah Esther. 2020. *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. New York: Oxford University Press.

Lageson, Sarah, and Kateryna Kaplun. 2021. "Public Accusation on the Internet." In *Media and Law: Between Free Speech and Censorship*, Vol 26, edited by Mathieu Deflem and Derek M. D. Silva, 99–114. Bingley, West Yorkshire: Emerald Publishing Limited.

Levy, Karen. 2014. "Intimate Surveillance." *Idaho Law Review* 51(3): 679–693.

Levy, Karen. 2022. *Data Driven: Truckers, Technology, and the New Workplace Surveillance*. Princeton: Princeton University Press.

Levy, Karen, Lauren Kilgour, and Clara Berridge. 2019. "Regulating Privacy in Public/Private Space: The Case of Nursing Home Monitoring Laws." *Elder Law Journal* 26(2): 323–365.

Levy, Karen, and Bruce Schneier. 2020. "Privacy Threats in Intimate Relationships." *Journal of Cybersecurity* 6(1): 1–13.

Lin, Belle, and Camille Baker. 2020. Citizen App Again Lets Users Report Crimes — And Experts See Big Risks. *The Intercept* March 2, 2020 https://theintercept.com/2020/03/02/citizen-app/

Lopez v. United States. 1963. 373 U.S. 427.

Lyon, David. 2002. *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*. New York: Routledge.

Lyons, Kim. 2021. Amazon's Ring Now Reportedly Partners with More than 2,000 US Police and Fire Departments. *The Verge* January 31, 2021 https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras

Marr, Chris. 2020. States Urge Employers: Report Workers Not Returning to Jobs. *Bloomberg Law* May 6, 2020 https://news.bloomberglaw.com/daily-labor-report/states-urge-employers-to-report-workers-who-wont-return-to-jobs

Marwick, Alice. 2021. "Morally Motivated Networked Harassment as Normative Reinforcement." *Social Media + Society* 7(2): 1378.

Marx, Gary. 1989. *Undercover: Police Surveillance in America*. Berkeley: University of California Press.

Marx, Gary. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

McCann, Michael W. 1994. *Rights at Work: Pay Equity Reform and the Politics of Legal Mobilization*. Chicago: University of Chicago Press.

Megiddo, Tamar. 2023. "Crowdwashing Surveillance; Crowdsourcing Domination." *Law and Ethics of Human Rights* 17: 67–94.

Meshel, Tamar. 2021. "The PAGA Saga." *Pepperdine Law Review*. 48(2021): 36–71.

Michaels, Jon D., and David Noll. 2021. "Vigilante Federalism." *Cornell Law Review* 108: 1187–1264. https://doi.org/10.2139/ssrn.3915944.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

Mnookin, Robert H., and Lewis Kornhauser. 1979. "Bargaining in the Shadow of the Law: The Case of Divorce." *The Yale Law Journal* 88(5): 950.
Molla, Rani. 2020. How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells. *VOX Media* January 28, 2020 https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks
Monahan, Torin. 2010. *Surveillance in the Time of Insecurity*. New Brunswick: Rutgers University Press.
Moore, Tina, and Natalie O'Neill. 2023. NYPD Unveils New Citizen-Like App with Crime-Reporting Button. *New York Post* January 25, 2023 https://nypost.com/2023/01/25/nypd-unveils-new-citizen-like-app-with-crime-reporting-button/
Morris, Justine. 2021. *Surveillance by Amazon: The Warrant Requirement*. Tech Exceptionalism, & Ring.
Morrison, Sara. 2021. How Citizen Sparked a $30,000 Manhunt for the Wrong Guy. *Vox* May 18, 2021 https://www.vox.com/recode/2021/5/18/22442024/citizen-app-manhunt-california-fires-arson
Murakami Wood, David, and Torin Monahan. 2019. "Platform Surveillance." *Surveillance and Society* 17(1/2): 1–6.
Natapoff, Alexandra. 2009. *Snitching: Criminal Informants and the Erosion of American Justice*. New York: New York University Press.
Newell, Bryce. 2021. *Police Visibility: Privacy, Surveillance, and the False Promise of Body-Worn Cameras*. Berkeley: University of California Press.
Nguyen, Aiha, and Eve Zelickson. 2022. "At the Digital Doorstep: How Customers Use Doorbell Camaras to Manage Delivery Workers." *Data and Society* 1–40. https://datasociety.net/wp-content/uploads/2022/10/AttheDigitalDoorstepFINAL.pdf.
Noble, Safiya Umoja. 2018. *Algorithms of Oppression*. New York: New York University Press.
O'Connor, Brendan, and Daniel Rivero. 2017. This Is What It Looks Like When the President Asks People to Snitch on Their Neighbors. *Splinter* October 3, 2017 https://splinternews.com/this-is-what-it-looks-like-when-the-president-asks-peop-1819077393
Oliver, Mariana, and Matthew B. Kugler. 2021. "Surveying Surveillance: A National Study of Police Department Surveillance Technologies." *Arizona State Law Journal* 54: 103–143.
O'Malley, Pat. 2010. *Crime and Risk*. Thousand Oaks: SAGE Publishing.
Perry-Hazan, L., and M. Birnhack. 2016. "Privacy, CCTV, and School Surveillance in the Shadow of Imagined Law." *Law and Society Review* 50(2): 415–449.
Pruitt Young, Sharon. 2021. TikTok Activists Are Flooding A Texas Abortion Reporting Site With Spam. *NPR* https://www.npr.org/2021/09/03/1034008380/tiktok-texas-abortion-ban-spam-website-activists
Quillian, Lincoln, and Devah Pager. 2001. "Black Neighbors, Higher Crime? The Role of Racial Stereotypes in Evaluations of Neighborhood Crime." *American Journal of Sociology* 107(3): 717–767.
Reeves, Joshua. 2017. *Citizen Spies: The Long Rise of America's Surveillance Society*. New York: New York University Press.
Reynald, Danielle M. 2019. "Guardianship in the Digital Age." *Criminal Justice Review* 44(1): 11–24.
Riley v. California. 2014. 573 U.S. 373.
Roberts, David J., and Meghann Casanova. 2012. *Automated License Plate Recognition (ALPR) Use by Law Enforcement: Policy and Operational Guide*. Alexandria, Virginia: International Association of Chiefs of Police.
Rose, Janus. 2020a. This Script Sends Junk Data to Ohio's Website for Snitching on Workers. *VICE* May 8, 2020 https://www.vice.com/en/article/wxqemy/this-script-sends-junk-data-to-ohios-website-for-snitching-on-workers
Rose, Janus. 2020b. Ohio Has Stopped Kicking Workers off Unemployment After A Hacker Targeted Its Website. *VICE* May 13, 2020 https://www.vice.com/en/article/n7wwdw/ohio-has-stopped-kicking-workers-off-unemployment-after-a-hacker-targeted-its-website
Rutledge, Steven H. 2002. *Imperial Inquisitions: Prosecutors and Informants from Tiberius to Domitian*. London: Routledge.
Sampson, Robert J., and Dawn J. Bartusch. 1998. "Legal Cynicism and (Subcultural?) Tolerance of Deviance: The Neighborhood Context of Racial Differences." *Law and Society Review* 32: 777–804.
Scholz, Lauren Henry. 2022. "Private Rights of Action in Privacy Law." *William & Mary Law Review* 63(5): 1639–93.
Shamir, Ronen. 2008. "The Age of Responsibilization: On Market-Embedded Morality." *Economy and Society* 37: 1–19.
Silbey, Susan S. 2005. "After Legal Consciousness." *Annual Review of Law and Social Science* 1: 323–368.
Slobogin, Christopher, and Sarah Brayne. 2023. "Surveillance Technologies and Constitutional Law." *Annual Review of Criminology*. 6: 219–240.
Smith, Robert, and David Kestenbaum. 2020. SUMMER SCHOOL 6: Taxes & Donald Duck. *NPR* August 12, 2020 https://www.npr.org/2020/08/12/901837703/summer-school-6-taxes-donald-duck
Stark, Luke, and Karen Levy. 2018. "The Surveillant Consumer." *Media, Culture and Society* 40(8): 1202–20.
Stuart, Forrest. 2020. *Ballad of the Bullet: Gangs, Drill Music, and the Power of Online Infamy*. Princeton: Princeton University Press.
Surden, Harry. 2007. "Structural Rights in Privacy." *SMU Law Review* 60(4): 1605–29.
Talesh, Shauhin A., and Bryan Cunningham. 2021. "The Technologization of Insurance: An Empirical Analysis of Big Data an Artificial Intelligence's Impact on Cybersecurity and Privacy." *Utah Law Review* 2021(5): 967–1027.
Thacher, David. 2005. "The Local Role in Homeland Security." *Law and Society Review* 39(3): 635–676.
Thompson, John B. 2005. "The New Visibility." *Theory, Culture and Society* 22(6): 31–51.
Town of Little Elm. n.d. Video Crime Watch Program July 6, 2022 https://www.littleelm.org/FormCenter/Police-4/Video-Crime-Watch-Program-37
Truckers Against Trafficking. n.d. July 6, 2022. https://truckersagainsttrafficking.org/.

https://doi.org/10.1111/lasr.12681 Published online by Cambridge University Press

U.S. Department of Homeland Security. 2017. DHS Announces Launch of New Office for Victims of Illegal Immigrant Crimes October 3, 2022 https://www.dhs.gov/news/2017/04/26/dhs-announces-launch-new-office-victims-illegal-immigrant-crime

U.S. v. Jones. 2012. 132 S. Ct. 945.

West, Emily. 2019. "Amazon: Surveillance as a Service." *Surveillance and Society* 17(1/2): 27–33.

Williams, Keith L. 2003. "Peel's Principles and their Acceptance by American Police: Ending 175 Years of Reinvention." *Police Journal* 76: 97–120.

Wilson, Michael. 2022. $87.50 for 3 Minutes: Inside the Hot Market for Videos of Idling Trucks. *The New York Times* March 19, 2022 https://www.nytimes.com/2022/03/19/nyregion/clean-air-idle-car.html

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

How to cite this article: Brayne, Sarah, Sarah Lageson, and Karen Levy. 2023. "Surveillance Deputies: When Ordinary People Surveil for the State." *Law & Society Review* 57(4): 462–488. https://doi.org/10.1111/lasr.12681