2021

Geoprivacy, Convenience, and the Pursuit of Anonymity in Digital Cities

Jerome Dobson
University of Kansas

William A. Herbert
CUNY Hunter College

Chapter 32
Geoprivacy, Convenience, and the Pursuit of Anonymity in Digital Cities

Jerome E. Dobson and Willam A. Herbert

Abstract Cities demand spatial efficiencies that can be achieved only through sharing of information. Current technologies support collection, processing, and dissemination of unprecedented quantities of personal, public, and corporate information. Inherent in this milieu is an inevitable contest among societal efficiency, corporate profits, consumer convenience, personal privacy, and even freedom. The authors examine current trends in technology, data collection, legislation, and public acceptance. They find that without broad specific regulations limiting location data collection and use—including a universal protected right for individuals to pursue anonymity—governments, commercial enterprises, employers, and individuals increasingly will exploit tracking technologies at the expense of geoprivacy.

32.1 Introduction

Cities exist because of society's overriding need for spatial efficiency. Placing people close together, connected through systems that operate quickly and smoothly, can enhance productivity and leisure, resulting in the potential for relatively high standards of living for many, while also creating wide disparities in economic and social well-being. Information sharing is essential in commerce and marketing, which typically are concentrated in urban areas.

Here, we explain the range of urban information technologies and applications available now and likely to emerge soon. We discuss current policies, legislation, and court rulings governing geoprivacy—defined here as "individual rights to prevent [surveillance and] disclosure of the location of one's home, workplace, daily activities, or trips" (Kwan et al. 2004)—together with surveillance and control, including

J. E. Dobson (✉)
Department of Geography, University of Kansas, Lawrence, USA
e-mail: dobson@ku.edu

W. A. Herbert
Hunter College, City University of New York, New York, USA
e-mail: wh124@hunter.cuny.edu

W. Shi et al. (eds.), *Urban Informatics*, The Urban Book Series,
https://doi.org/10.1007/978-981-15-8983-6_32

the European Union's recent General Data Privacy Regulation (GDPR). We address the extent of government, corporate, and individual information gathering, and the risks involved in such data collection and use. We explore the processes and considerations by which corporations, groups, and individuals decide whether to accept or resist surveillance and control.

Delivering goods, managing traffic and mass transit, facilitating urban pleasures, and myriad other essential services such as crime prevention, depend on individuals merging their own activities with communal operations. Maximizing efficiency necessitates information sharing, which foments tension between societal demands and personal expectations of freedom and privacy. Tensions can rise to conflict when urban policymakers adopt "smart" technologies without studying and managing the impacts such technologies will have on privacy (Williams 2019).

How a society balances community needs with individual rights reflects collective values and priorities. The escalating growth of privatized urban spaces (Garrett 2015) impedes geoprivacy protections in the USA because, in general, private actors have more license to surveil and track than government agents who are subject to greater legal restrictions. More important, government regulations rarely reflect majoritarian views about geoprivacy, especially since Amazon, Apple, Facebook, Google, and Microsoft collectively spent $582 million over thirteen years to lobby the US Congress to promote their proprietary interests (Dellinger 2019).

In the USA, except for California, there is no comprehensive regulatory scheme (Swisher 2019). Instead, the burden of balancing convenience and privacy regarding data collection and accessibility is placed squarely on the individual. Hence, as Fowler (2018) warns, "Many of us will delete apps … disable as much tracking as we can on our phones … delete our Facebook accounts … delete our social media histories and old emails and text messages. But it won't be enough because most people will not care: The trade-off between privacy and convenience will be worth it to them, because the loss of their privacy will have little to no impact on their day-to-day lives. Most people will read (or perhaps ignore) the news stories about every new privacy scandal, and they will then go back to their phones." Even those who study and report on location privacy have a hard time retaining their location invisibility on the electronic surveillance grid (Swisher 2019).

Individuals routinely sacrifice some degree of privacy and personal choice for the common good or consumer convenience. These sacrifices are usually implicit tradeoffs without discernment or adequate information for informed consent. The extent of sacrifice is oftentimes mollified by extreme individual wealth, creating a non-egalitarian opt-out from shared sacrifice. In addition to economic inequality, a digital divide exists with respect to individual access to and sophistication with the use of technology (Slinn and Herbert 2011). Nevertheless, urban habits, design, customs, and laws frequently favor collective efficiency and commerce over individual self-determination with respect to privacy.

Traditionally, cities have provided individuals with a means of hiding in the crowd and maintaining relative anonymity. Many people crave the subjective perception of invisibility in crowded streets, parks, and trains. For centuries, they enjoyed an

overarching sense of obscurity based on time, space, impermanence, and inherent limitations on human memory (Hartzog and Selinger 2019).

Collectively, however, people cannot have all they may want simultaneously. The more one seeks fame the less likely he or she can have anonymity or obscurity and so it goes for whole population segments within cities. Individuals and groups may choose open lifestyles—such as those of political and civic leaders, entertainers, entrepreneurs, and social media influencers. Others are forced into the public spotlight against their will or live a life in the shadows out of choice, necessity, or circumstances beyond their control.

New information technologies increase benefits and risks and make today's societal and individual choices ever more difficult. Some applications improve government, commercial, familial, and individual efficiencies and conveniences at the cost of privacy, but they are rarely designed to protect privacy. At the same time, emerging technologies enhance surveillance or control by government, employers, loved ones, or caregivers. Through the collection of location data by commercial enterprises, the most basic democratic rights of dissent and protest in the streets can be easily tracked (Warzel and Thompson 2019).

These technologies also can create a new form of slavery—geoslavery—based on location control, "a practice in which one entity, the master, coercively or surreptitiously monitors and exerts control over the physical location of another individual, the slave. Inherent in this concept is the potential for a master to routinely control time, location, speed, and direction for each and every movement of the slave or, indeed, of many slaves simultaneously. Enhanced surveillance and control may be attained through complementary monitoring of functional indicators such as body temperature, heart rate, and perspiration" (Dobson and Fisher 2003, pp. 47–48; 2007; Herbert 2006). Geoslavery violates a central component of personal liberty, namely freedom of locomotion, which includes the ability of a person to move from place to place without external restraint unless pursuant to law (see the works of Blackstone in Lemmings 2018).

Generalized fear of government or corporate electronic surveillance is common, even though the public barely knows the collective scope and magnitude of the data collection, sale, and use of such information. Moreover, the collection, use, and distribution of personal data by individuals—family, friends, and strangers—is routinely accepted without protest.

Health records, in particular, are considered sacrosanct in the USA. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains a "Privacy Rule" so prominent that many people mistakenly dub the entire act the "Health Information Privacy Act." Its goals are to protect health insurance coverage when workers change or lose jobs and to protect health data confidentiality and availability. It guarantees a right of access to one's own health data on request (HIPAA Journal 2019). It was passed with the good intention of protecting individuals from any consequences that might result from divulging health information including workplace discrimination. Patients routinely are presented with a statement affirming their rights to privacy except for release to insurers, the one entity most likely to react detrimentally to a patient's interests if adverse health conditions are found. Concomitantly, HIPAA's

disclosure rules restrict the release of health and geographic information on individuals so completely that the act itself stymies high-precision geographic research on factors, causes, and effects linking local health to local environments, thus fettering the complementary fields of medical geography and epidemiology.

Many people have acquiesced to the commodification of personal location data for advertising and consumer targeting, becoming willing subjects to what Shoshana Zuboff has labeled "surveillance capitalism" (Zuboff 2019). Some recognize a risk vs. benefit ratio; others do not. We explore the integration of location technology with social media platforms and deregulatory ideology in the age of social media. We discuss social and cultural changes arising from accelerated use of location technology, implications for precarious work (Uberization), and unwritten tradeoffs of "convenience" for loss of privacy. Here, we discuss such matters in the context of three illustrative applications that feature tracking technology.

32.1.1 Application #1: The Role of Cities in Slavery Prior to the Civil War

To contextualize the impact of twenty-first-century information technologies on urban geoprivacy, human rights, and property rights, consider an example from the nineteenth century based on analog technology rather than digital. From the earliest days of the American republic, surveillance and restraint were core components of the American slavery system. Freedom of movement was substantially restricted for those enslaved. Federal laws enabled slaveholders to track down, recapture, and return runaway slaves, then defined as human chattel with high monetary value. Self-emancipated slaves constituted a major economic loss for slaveholders, who spent substantial sums for location information to aid in the legal and frequently extra-legal capture by slave catchers (Foner 2016).

Fugitive slaves in the nineteenth century flocked to cities in search of anonymity, personal redefinition, and employment. Cities with large populations of free African-Americans were particularly attractive for escaped slaves. There they had a greater chance to attain obscurity and even mingle in crowds at public events (Franklin and Schweninger 1999). Black and white abolitionists assisted self-emancipated slaves in traveling to safer areas, creating new identities, and finding work and lodging. To personalize, W.C. Pennington arrived in New York City in 1828 after escaping slavery and stayed, establishing himself as a minister and educator. Another escaped slave, Frederick Bailey, traveled to New York a decade later. During his short stay, Bailey changed his name, married with Pennington officiating, and went off to become the famous abolitionist writer and orator Frederick Douglass (Foner 2016).

Even slaves emancipated by their former masters faced difficulties in avoiding discovery that could result in re-enslavement. Urban vigilance committees were formed to protect escaped slaves, free African-Americans kidnapped off city streets, and challenge legal proceedings intended to compel their enslavement in another

state (Foner 2016). The importance of urban life to African-Americans explains, in part, the reluctance of many who received land grants from abolitionist and agrarian Gerrit Smith in the late 1840s to leave and start new lives in the remote Adirondack Mountains. Despite the continuing fear of slave catchers, the urban environment was more secure than attempting to create a safe community elsewhere (Stauffer 2002).

Imagine how modern tracking technologies, had they been available in antebellum times, would have maximized the efficiency of tracking down runaway slaves in cities and returning them to bondage. Indeed, such technologies might have negated the urban advantage in geoprivacy. The same principles apply to fugitive slaves in the nineteenth century or modern-day sex slaves seeking freedom and dignity or immigrants seeking refuge in the twenty-first century.

32.1.2 Application #2: Informed Delivery by the US Postal Service

How pervasive and vexing geoprivacy can be today. How integrally it is entangled with efficiency and convenience. In the first half of the twentieth century, it was generally assumed that a mailman could deliver a package by knocking on the door and handing it to a live person inside. Starting with World War II, however, changes in lifestyle rendered that premise untrue. More women were working, and fewer extended families lived together in the same house. Eventually, it became necessary to leave packages unattended at the door. That gave rise to "porch pirates"—scofflaws who steal unattended packages. Eventually, the problem became so rampant that critics objected to "porch pirate" as too frivolous a term for the damage done. An estimated 1.7 million packages are stolen every day across the USA (Hu and Haag 2019).

To counter theft, the US Postal Service (USPS) initiated a program called Informed Delivery. Any USPS customer could sign up for an electronic notice to inform him or her when a package would arrive so the customer could arrange to be home at or soon after its arrival. Unfortunately, USPS failed to install proper security procedures, and now it is fairly easy for crooks to sign up for someone else's account. Thus, some thieves receive convenient notices alerting them to deliveries at a time unknown to the resident. The problem could be solved by more stringent measures, such as holding the package for customer pickup at the Post Office, but that would incur unacceptable delays and additional travel on the part of the customer or mail carrier. It is a clear case of customers, bent on convenience, wanting a solution that turns out to be vulnerable itself.

Simultaneously, Amazon.com offered a program for customers to pre-approve delivery personnel to open the front door and place each package inside. Predictably, most customers recoiled at the thought. Next, Amazon offered to deliver inside the garage, but many urban dwellers do not have garages and acceptance among those who do is unclear.

Today, the most popular countermeasure to porch piracy is Amazon's Ring technology, which employs a video surveillance camera integrated into a doorbell (Wingfield 2018). Privacy concerns have been expressed because each installation surveils not only the owner's yard, but neighbors' yards, driveways, and streets as well, and formal agreements are being instituted for police departments (600 so far) to harvest and process data with the consent of owners but not the consent of neighbors, visitors, and other passersby (Harwell 2019a, Thorbecke 2019). Worse yet, hackers have frightened some residents (famously including an eight-year-old girl) by speaking to them through Ring security cameras inside the home (Chiu 2019).

32.1.3 Application #3: Geoslavery in the Middle East and China

In their initial article on geoslavery, Dobson and Fisher (2003) proposed "realistic scenarios of potential enslavement applications." Based on the real-life honor murder of Sevda Gok, "a teenage girl [in eastern Turkey] whose family held a council and voted to execute her in violation of their own country's laws," they envisioned the following hypothetical scenario, which would be anathema to Western societies, yet acceptable in some Middle Eastern countries: "Soon an enterprising businessman … may be able to purchase a central monitoring system … which can be locked onto the wrists of every member of the village (women, children, and men). Most likely, he will be able to offer a service to village parents at an affordable price that will cover his investment and a tidy profit."

At the time, some critics claimed the hypothetical scenario was futuristic and inflammatory. Yet in 2019, "U.S. Representative Jackie Speier and 13 colleagues wrote Apple CEO Tim Cook and Google CEO Sundar Pichai to call for the removal of a mobile app from the companies' app stores that allows Saudi men to track women and migrant workers…" The Congressional press release (Speier 2019) states, "The ingenuity of American technology companies should not be perverted to violate the human rights of Saudi women. Twenty-first century innovations should not perpetuate sixteenth century tyranny… Keeping this application in your [app] stores allows your companies and your American employees to be accomplices in the oppression of Saudi Arabian women and migrant workers… The app, Absher … allows a male "guardian" to take away permission for a woman or migrant laborer to exit the country and provides the man with notifications if there is an attempt to leave. Amnesty International has stated this app is another example of how the Saudi Arabian government has developed and employed tools to limit women's rights and freedoms."

When we first wrote about geoslavery (Dobson and Fisher 2003; Herbert 2006), the ultimate example we imagined was a nation tracking its entire population, and employers tracking their employees, surveilling with GPS, enhancing with government and corporate databases, and rewarding individuals for good behavior or punishing them for bad behavior.

In 2014, China announced plans to do exactly that. A year later, China's "omnipotent" Social Credit System was tested in pilot projects run by eight major companies for planned national implementation in 2020 (Hatton 2015). Today, the test involves more than twenty companies, where every individual is monitored through human tracking and surveillance to produce a social credit score used to rate each citizen's trustworthiness. The current concept is not a unified platform generating unique scores for 1.4 billion citizens. "Instead, the national program is envisioned as a web of individual systems run by cities, hospitals, businesses and agricultural-produce markets — all linked by data-sharing and using incentives and penalties to make people and businesses behave as the government wishes" (Mistreanu 2018). It is as if the US government were to explicitly appoint Google, Equifax, Sprint, and other corporations as guardians of every citizen's reputation, social success, job opportunities, and travel destinations.

The stated intention of China's original plan was to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step" (Mistreanu 2018). By the end of 2018, "Citizens placed on black lists for social credit offences were prevented from buying train tickets 5.5 million times … [and] in 2017 … 6.15 million citizens had been barred from taking flights" (Kuo 2019). Data variables, held in vast national and corporate databases, include government information such as tax payments and traffic violations and corporate data such as consumer debt.

The program qualifies as geoslavery even with Dobson's original stipulation that geoslavery must be either "coercive or surreptitious." It is conspicuously not surreptitious, but surely it is coercive because the masters (currently the Chinese government and 26 large corporations) completely control every life that is being evaluated, including the decision to be watched. It cannot be consensual because the Chinese government and its corporate partners hold the ultimate power relationship over everyone submitting to it.

A Washington Post article (Song 2018) claims that the Chinese system is not as bad as it sounds, because, for instance, many of the worst offences (such as denying all travel requests for people who had traffic violations) happened in overzealous pilot projects and were then rejected from the national plan. We do not understand how that makes it better since the very same private companies running the tests are slated to continue running the program in a somewhat autonomous status, and private companies typically have more license to abuse than government itself does. Regardless, when citizens eagerly accept daily, continuous evaluation of any kind, as Chinese citizens are said to have done, there will be no turning back. Any future bureaucracy can add another and another at its whim, and no one can object without being down-scored.

China's Social Credit System is the ultimate digital-age version of the long-feared Panopticon. More than two centuries ago Samuel Bentham, an architect, designed a building that was actually a surveillance machine; his brother Jeremy Bentham fervently promoted the invention. Its optics were such that a single "inspector" could observe every occupant simultaneously. They called it the "Panopticon" (all seeing). It was, Jeremy said, "A new mode of obtaining power of mind over mind, in a

quantity hitherto without example." Since its inception, surveillance technology has advanced in three major spurts, each of which triggered a new specter of surveillance and control. The first instance was the Benthams' building; the second was and is a tightly controlled closed-circuit television network (CCTV), and the third is today's electronic tracking services. Each had and has its own distinctive rationale: first the utopian perfection of society; second the enforcement of absolute tyranny; today safety, security, and convenience. Functionally, however, their root function is the same—total surveillance—and they are indeed three successive generations of Panopticons. Dobson and Fisher (2007) called them, respectively, Panopticon I, II, and III.

Clearly, China's Social Credit System qualifies as Panopticon III, a case of cultural acceptance that would not be acceptable in most western countries. But is western culture really that opposed? In 2019, the Trump Administration proposed a point-based plan to assign merit scores to immigrants applying for entry into the country (Shoichet 2019). US education officials are considering a new adversity score added to the SAT score that is so instrumental in determining social and financial opportunity (Jaschik 2019).

32.2 Tracking Technologies

New information technologies increase benefits and risks and make today's choices ever more crucial. Here, we explain the range of human tracking technologies and applications now available and how each is involved in tracking.

Human tracking technologies include Global Positioning System (GPS) receivers that are attachable or wearable with GPS chips embedded in cell phones, bracelets, or dedicated navigation devices, all of which may be connected to telecommunication networks that record coordinates and interact with geographic information systems (GIS) (Commonwealth v. Almonor 2019). A related form gets coordinates not from GPS but from less precise cell-site location information (CSLI) when a cell phone connects to a cell tower (Carpenter v. USA 2018).

Other ubiquitous sources of location data are the geosocial footprints extracted from social media activity and smartphones (Weidemann et al. 2018). A New York Times investigation described the extraordinary breadth of location information extracted from a million smartphones in New York City and stored in one database (Harris et al. 2018). Data from smartphones used in urban areas enables massive tracking of individuals regardless of their economic status, neighborhood, or worksite (Thompson and Warzel 2019).

The electronic exhibitionism inherent in social media is a major source of location data that are collected, analyzed, and sold. Until 2019, Facebook continuously collected location information on Android users even when the app was not in use (Gomez 2019). For close to a decade, Google has maintained a database called Sensorvault with detailed location information from millions of devices (Valentino-DeVries 2019).

Other tracking technologies include radio-frequency identification (RFID) and biometrics (Herbert and Tuminaro 2008). RFID chips can be imbedded in worn or carried objects such as urban transit cards and can be implanted in a person's body. Biometrics is an identification technology based on unique biological characteristics such as voice and facial recognition that is being utilized in immigration and even by landlords (Bellafante 2019). Wearable biometric devices are being used by professional sports teams to monitor the physical functions of athletes (Venook 2017). Location data from RFID are not spatially continuous and are limited to specific locations, but they are excellent for maintaining inventories of goods and people. Thus, a core use of RFID and biometrics is monitoring pedestrian traffic in buildings and transit systems. When integrated with surveillance cameras, these technologies can form the basis for a modern-day Panopticon II (Dobson and Fisher 2007).

Facial pattern recognition can be stationary, as when used to monitor crowds entering a stadium without necessarily following them home. However, frequent detection at ubiquitous geo-referenced sites or by mobile sensors creates a trail of geo-coordinates as effectively as GPS itself. Recently, Schuppe (2019) declared it a "routine policing tool in America." Yet, resistance is developing, and San Francisco has banned its use (Conger et al. 2019).

Increasingly, automobiles are equipped with surveillance devices capable of monitoring every aspect of engine performance but also direction, speed, and braking of the car itself, plus personal details such as eye movements to measure attentiveness.

Geoslavery is the most extreme application threatening privacy and personal freedom (Dobson and Fisher 2003; 2007; Fisher and Dobson 2003; Herbert 2006). The term was coined (Dobson 2002) soon after entrepreneurs started offering "kid-tracking" technology. Despite its kid name, then and now the devices can be used for tracking people of any age. Applications can be highly beneficial, and many are, but absolute control is a dangerous thing. The key to protecting the tracked is to establish applicable ethical standards, laws, and regulations.

Less extreme but still concerning is "nudging," a practice in which governments or corporations encourage mass behavior, and "big nudging," which uses big data to do it (Helbing et al. 2017; Dasgupta 2017). Insurance companies, for instance, reward customers for using location-based services (LBS) to enforce "safe" driving habits. State Farm Insurance offers a driving score that determines insurance rates, and they advertise it on TV making light of how it will dictate driving decisions such as workers being late for a meeting or a pregnant mother arriving late at the hospital for her baby's delivery (State Farm Insurance Company 2019).

Dasgupta views such nudging as "a modern form of paternalism. The new, caring government [or company] is … interested in what we do, but also … that we do [what] it considers to be right … To many this appears to be a sort of digital [prod] that allows one to govern the masses efficiently, without having to involve citizens in democratic processes." The technology used for nudging is ubiquitous computing and telecommunications systems, over which the individual consumer has little control. Laws and customs determine what is acceptable, but most collection and processing occurs in cloistered rooms. It is this separation of watcher and watched that frightens many people.

32.3 Informed Acceptance of Benefits and Adverse Acceptance of Risks

Society views geosurveillance—defined here as the practice, usually electronic, of monitoring and recording the geometries, topologies, and attributes of places and human and physical entities both stationary and moving—with two faces. When presented in the abstract, as CCTV was in George Orwell's 1984, geosurveillance is frightening in the extreme. When it is available commercially and used by many or even just a few, however, the specter subsides. This is particularly true when the technology is imbedded in smartphones, wearable devices, and apps. CCTV is now deployed routinely for surveillance in cities and sensitive rural sites, and the greatest fear for most people is merely a traffic fine. Likely, the key factor is individual perception of actual use. Prior to deployment, there is no such experience on which to judge. If then a device is widely deployed and seldom indicted for harm, the public is lulled into thinking the risk is small or nonexistent. We call this phenomenon an adverse acceptance.

The marketing of tracking technologies includes aggressive promotion of conveniences but reticence about dangers. Voluntary full disclosure of the scope, use, and sale of data collected would be self-defeating for proponents. The lack of understandable information renders it impossible for an urban dweller to make rational risk assessments connected to geoprivacy.

Excellent examples of this phenomenon are Hudson Yards—a new 28-acre "smart city" in Manhattan—and Waterfront Toronto, both owned by a subsidiary of Google's parent company Alphabet. In designing and promoting Hudson Yards, the developer emphasizes the conveniences of installed tracking technologies without disclosing what may be done with the data. As the developer's president proclaimed to a reporter: "The data is our data for the purposes of allowing us to make Hudson Yards function better" (Jeans 2019). Yet, privacy concerns ultimately forced Alphabet to scale back severely on certain onerous aspects of Waterfront Toronto (Bilefsky 2019).

Faced with such opaqueness, a resident, worker, visitor, or commercial customer at Hudson Yards has only three choices: accept the surveillance based on the developer's assurance of a positive or benign purpose; ignore the surveillance and accept an unknown risk concerning the use of the data by the developer or a third party; or refuse to enter the "smart city" to avoid surveillance and data collection. Buyers and renters must judge based on predominantly positive presentations. This situation is an example of what Attoh et al. (2019) have termed "idiocy in the smart city."

A similar dilemma is faced by Uber drivers and passengers because tracking technologies are imbedded in the labor relationship of the "gig" worker (Attoh et al. 2019). The driver can accept the cost of creating geodata for Uber as part of work or decline employment. Similarly, a potential customer can accept geosurveillance as a cost of the convenience of using the service or decline the ride (Smith and Leberstein 2015).

Consider the nature of this cost/risk versus benefit ratio at Hudson Yards, Uber, and anywhere else surveillance is installed. If the ratio is, say, 999 benefits to every

1 cost/risk, society may favor surveillance, but how can and should society protect itself from that one cost/risk? Consider this analogy: The benefits of white phosphorus matches are overwhelmingly positive, but we still have to devote some societal resources to match safety.

Some applications improve government and commercial efficiencies at the cost of privacy. Some yield control to government, loved ones, and caregivers. It is often said that the problem with privacy is not technology but rather misuse of technology. In turn, misuse is a function of societal norms and deviations from those norms. If a business offered a female tracking service in the USA similar to the one in Case Study #3, there would be wide public outrage including demands for government investigation, regulation, and prosecution. In Saudi Arabia, however, it fits within the norm of how women have been treated in the analog world. Still, some people in Saudi Arabia will object, and some Americans will try to do it anyway.

Already one tragedy complicated by geoslavery has been documented (Dobson 2007). When Stacy Peterson went missing in 2007, news reports claimed her husband Drew Peterson, a policeman in the Bolingbrook, Illinois Police Department, obsessively monitored her movements prior to her disappearance. She complained to family and friends that he was controlling her. She changed her cell phone number in a futile attempt to avoid his control. When confronted with the allegation that Drew was tracking Stacy's friends, his lawyer defended his actions in a frightening way. It was a common practice, the lawyer said, for local police officers to track their spouses, friends, and acquaintances. Stacy Peterson's body was never found. If she is dead, geoslavery is complicit in her murder. If she survived, geoslavery denied her the possibility of taking her children with her.

32.4 Legal and Regulatory Responses to Tracking Technologies

For decades, the European Union (EU) has been the international leader in regulating collection and use of personal electronic data, including location data (Herbert 2008). In May 2018, its General Data Privacy Regulation (GDPR) became effective, substantially broadening and improving protections for EU citizens. The regulation constitutes a significant step forward for protecting geoprivacy in European cities, particularly with its grant of the right to be forgotten.

The GDPR defines personal data to include location data as well as any other information related to a specific individual. The new regulations impose mandates that are relevant to geoprivacy, some particularly so: a requirement for informed and unambiguous individual consent; an insistence that data collection must be legitimate and necessary; a guarantee that individuals have rights to access and correct the information; and, most important, the provision of a right to be forgotten. The GDPR right to be forgotten, that is, to pursue anonymity, gives individuals a high degree of authority over their own location data. It is codified in GDPR, Article 17, which

states, "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay." Erasure is enforceable under certain circumstances including when the data are "no longer necessary in relation to the purposes for which they were collected or otherwise processed."

The USA is far behind in developing such a comprehensive response to the privacy implications of electronic data. While American courts have grappled with some privacy disputes resulting from tracking technology, primarily involving criminal prosecutions, legislatures generally have been slow to respond. The delay in the USA is due, in part, to the fact that the rise of electronic tracking and social media occurred during the ascendancy and domination of neoliberal deregulation ideology.

The US Supreme Court and some state courts have ruled that the Fourth Amendment to the United States Constitution mandates that law enforcement obtain a judicial warrant before tracking with GPS or CSLI technologies. These rulings are interpretative of constitutional limitations on the use of tracking technologies by government actors. They are premised on concepts of property rights and reasonable expectations of privacy, rather than universal principles of human rights.

It is unlikely that federal legislation will be passed to grant strong privacy protections similar to GDPR in light of "the relationships between some members of Congress and Silicon Valley companies" (Fowler 2018). Therefore, the impetus for policy innovation concerning geoprivacy will more likely come from state legislatures and local governments unless a new national social movement arises to compel Congress to act with strong federal protections.

California has followed the EU's lead by adopting a right to be forgotten through passage of the California Privacy Act of 2018. Under the new state law, businesses that collect and/or sell personal consumer information, including geolocation data and biometric information, must notify the consumer, upon request, of the types or information being collected, used, and/or sold. More important, the law requires the deletion of such data, upon a consumer's request, except in certain specified situations. The City of Los Angeles sued an "IBM-owned app maker accused of sharing user location data with affiliates of its parent company and other advertisers, but also hiding the practice in a 10,000-word-long privacy policy" (Cimpanu 2019).

Other states have passed laws that seek to limit location tracking in narrower ways. The following examples highlight the lack of uniformity in such legislative measures. Montana and Utah statutes require law enforcement to seek a warrant before obtaining location data from a device under certain circumstances. It is a crime in Iowa and Wisconsin for a person to attach a GPS device to another person's vehicle without consent. Mandated or coerced RFID chip implants are prohibited by laws in California, Maryland, Utah, and New Hampshire. Some states have prohibited or regulated the collection of biometric information, particularly with respect to students.

Many people fear government or corporate surveillance, while ignoring the collection, use, and distribution of personal data by individuals, including family members, friends, and strangers. Some recognize a risk versus benefit ratio; most do not. Government and corporate surveillance and data collection are indiscriminate,

applying to everyone for purposes of political control or corporate profit. In terms of everyday impact, however, the government might not care whether someone stops for a beer on the way home from work, while a spouse, parent, or caregiver may.

Surveys of public attitudes toward geosurveillance reveal a contradictory mixture of fear and acceptance. Rzeszewski and Luczys (2018) found, "The prevailing attitude that we identified [in Poznan, Poland and Edinburgh, UK] is neutral with a strong undertone of resignation—surrendering personal location is viewed as a form of digital currency. A smaller number of people had stronger, emotional views, either very positive or very negative, based on uncritical technological enthusiasm or fear of privacy violation. Such a wide spectrum of attitudes is not only produced by interaction with technology but can also be a result of different values associated with space and place itself."

Surveying public perception of privacy in the USA, Kar et al. (2013) found that respondents expect location data to be protected on the same level as health data and other personal information. However, respondents themselves are unaware of the legal implications of location privacy violations.

Indeed, public misunderstanding or outright ignorance of geoprivacy, geosurveillance, and geoslavery closely matches other manifestations of geographic ignorance and anti-intellectualism in the USA. The American purge of geography from all levels of education has left its mark on science and society (Kozak et al. 2015). In elementary school, geography has been misconstrued as "social studies," which deemphasize physical geography and spatial thinking. In high school, geography is required now by only 14 states. Geography is offered by most public universities but rarely by private universities. Only one geography department remains within the top twenty private US universities. To anyone who values education, it would seem remarkable if such neglect did not result in serious losses of public understanding. As one prominent example, a recent Pew Research Center (2018) report purporting to summarize "The State of Privacy in Post-Snowden America" missed its mark by failing to mention geoprivacy, spatial privacy, geosurveillance, geoslavery, or location (Pew Research Center 2018).

Citizens may fear government, but government agencies sometimes serve as their advocate and protector. The Federal Trade Commission (FTC 2014) has engaged in some limited efforts at challenging technology company misrepresentations concerning privacy. In 2014, the FTC issued a report entitled, "Data Brokers: A Call for Transparency and Accountability." In it, they named nine data brokers who amass and administer vast databases of personal information:

1. Acxiom: consumer data and analytics for marketing campaigns and fraud detection; information on about 700 million consumers worldwide.
2. CoreLogic: property, consumer, and financial information; more than 795 million historical property transactions, 93 million mortgage applications, and property-specific data covering over 99% of US residential properties; in total exceeding 147 million records.
3. Datalogix: businesses with marketing data on US households and more than a trillion dollars in consumer transactions; partnership with Facebook.

4. eBureau: predictive scoring and analytics services for marketers, financial services companies, online retailers; billions of consumer records.
5. ID Analytics: analytic services principally to verify identities or detect fraudulent transactions; 1.1 billion unique identity elements; 1.4 billion consumer transactions.
6. Intelius: background check and public record information; more than twenty billion records.
7. PeekYou: analyzes content from more than 60 social media sites, news sources, homepages, and blog platforms.
8. Rapleaf: data aggregator with at least one data point associated with more than 80% of all US consumer email addresses; supplements with the age, gender, marital status, and thirty other variables.
9. Recorded Future: historical data on consumers and companies; predicts future behavior.

Mirani and Nisen (2014) call them "The nine companies that know more about you than Google or Facebook." A representative list of what they know shows many variables that are spatial (address, address history, longitude and latitude); many reveal geographic identity (race, ethnicity, country of origin, religion, language); others relate to geographic habits (travel, vacation), not to mention dozens of variables that deeply probe finances, behavior, and lifestyle. The FTC report urged Congress to require the data broker industry to be more transparent and to give consumers greater control over their personal information.

32.5 Geoprivacy, the Inconscient Syndrome, and Control in the Academy

"We have entered a grand social experiment as momentous as any in our past and yet one so insidious that hardly anyone seems to have noticed" (Dobson 2009). For the first decade and more that we wrote about geoprivacy and geoslavery, there was precious little scholarly literature to cite. Today, there is a growing body based on empirical research, and we are especially thankful for those cited above. Still, technological and commercial advances are happening so fast that this chapter relies heavily on recent news media reports to augment the academic literature.

We encourage all applicable disciplines to join the quest for deeper understanding. Psychologists and sociologists, for instance, can study human motivations, responses, and behavioral issues. Technologists and legal scholars can develop alternative devices and regulations to thwart surveillance systems. Political scientists can explore better means for developing proactive and responsive public policies. Historians can search for antecedents to technologies, applications, and implications. Geographers and integrative teams of diverse disciplines can conduct interdisciplinary research.

Unfortunately, some academics have adopted tracking technologies with no more forethought than the general public. California physics professor Tom Bensky

designed "a new mobile application and website … that tracks students' attendance using their cell phones," which is now used by "a couple hundred other professors and officials" (Bauer-Wolf 2019). He faced predictable complaints and answered in a typically naïve way, "But I can't convince them that I'm not going to do anything with the data I'm getting. It's just the app, server, and a database, but it is hard to convince people." Therein lies the ever-present question: Why should anyone trust anyone who holds the keys to his or her private world? One must ask, what happens if a student can't afford a smartphone or refuses to sign up? Is an accommodation (e.g., free phones, manual check-in) made, or does the student have to drop the class? Will only the compliant be educated?

At the very least, such impositions on students should be raised to a higher level, addressed in university policies to be developed through shared governance, and challenged in state and federal courts. Professor Bensky's app could form the basis for one of the first legal challenges under the new California Privacy Act. If Bensky were conducting a research experiment in precisely the same manner, federal law would require him to file an application and face an Institutional Review Board to ensure informed consent by those being tracked. A decade ago, privacy advocates were outraged when a research team published results from tracking 100,000 people without informed consent (González et al. 2008; Dobson 2009).

Bensky's quote above is a prime example of what we term the inconscient syndrome. In the course of our research, we have observed an inordinate number of inconscient actors who show no malice but also no forethought. Most simply do not think through the matter of surveillance deeply enough to perceive risks, and the geographic dimension makes the perception even more difficult. Manifestations include entrepreneurs who create and market new software and systems without realizing their potential dangers, consumers who persistently perceive benefits but not risks, workers and their unions acquiescing to geosurveillance, targeted individuals who naïvely trust their watchers, and commentators who trivialize risks in favor of benefits. Most seem genuinely convinced that no risk exists, but that perception often is influenced by sophisticated advertising aligned with commercial interests. Indeed, universities have become leading advocates and practitioners of geosurveillance to the concern of some faculty and others worried about intrusions into privacy (Vance 2019; Harwell 2019b).

32.6 Conclusions

Urbanization and the rapid rise of integrated location data technologies raise profound questions concerning societal values and priorities about privacy and control. The deregulated free market economy over the past four decades has empowered technology companies to develop products, platforms, and applications that maximize profits and data collection and effectively deliver individual conveniences while simultaneously eroding geoprivacy. Europe has responded with strong measures to protect privacy, freedom, and the pursuit of anonymity. Conversely, China's response

is a perverse government assault on privacy. In the USA, use of tracking technologies against individuals is prohibited or regulated in certain areas, but true pro-active privacy regulation exists only in California.

The benefits of smartphones, GPS, social media, and other technologies are accepted for their conveniences with adverse acceptance of their risks and without a rigorous examination of potential means to balance benefits with risks. While such technologies help meet the need for urban spatial efficiencies, including infrastructure necessary for smart cities, they also feed massive corporate and government databases that can be used in urban areas to promote human control, manipulation, and even geoslavery. Developments in the Middle East and China, combined with memories of chattel slavery, demonstrate that the loss of geoprivacy is no longer a hypothetical proposition.

Regulation of geosurveillance to protect privacy is essential for cities to remain places where individuals can live and move about in relative obscurity. The EU's GDPR and the new California Privacy Act provide models for how societies can balance communal needs, consumer convenience, and individual autonomy. Central to such regulations are informed notice and consent; insistence on legitimacy and necessity in data collection; limitations of scope and duration of surveillance; rights of access and to correct the information; and a person's right to have the data destroyed. That last and crucial element would restore a vital aspect of urban living: the right to be forgotten—a guaranteed right to the pursuit of anonymity.

32.7 Epilogue

We submitted our final draft shortly before COVID-19 struck in earnest. The pandemic then hampered publication while dramatically changing the circumstances of our topic. Suddenly, geosurveillance was seen in a positive light as information technologies became essential for controlling the contagion country by country, enforcing social distancing, and tracing individuals exposed to the virus. When Apple and Google joined forces to support contract tracing, their offer was welcomed with fanfare. Simultaneously, the pandemic justified tracking workers, university students, and beachgoers. Some Americans envied China's apparent success without realizing how completely the country embraced geoslavery before the crisis. Conversely, some Americans resisted overhead drone surveillance while others objected even to preventive measures such as face masks.

We ourselves wrote an op-ed for the St. Louis Post Dispatch (May 6, 2020) condensing this whole chapter into a few points relevant to the pandemic. "For reopening," we said, "the goal must be to minimize deaths and illnesses while restoring essential goods and services, protecting fundamental rights, and maintaining acceptable life styles."

References

Attoh K, Wells K, Cullen D (2019) We're building their data: Labor, alienation, and idiocy in the smart city. Environ Plann D: Soc Space. https://doi.org/10.1177/0263775819856626

Bauer-Wolf J (2019) GPS to track student attendance. Inside Higher Ed, http://insidehighered.com/news/2019/06/20/professor-develops-new-app-gps-tracking-student-attendance. Accessed 25 June 2019

Bellafante G (2019) The landlord wants facial recognition in its rent-stabilized buildings. Why? New York Times, 28 Mar 2019, https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html?action=click&module=News&pgtype=Homepage. Accessed 25 June 2019

Bilefsky D (2019) Toronto's City of Tomorrow is scaled back amid privacy concerns. New York Times, October 31, 2019. https://www.nytimes.com/2019/10/31/world/canada/toronto-google-sidewalk.html. Accessed 6 Jan 2020

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

Chiu A (2019) She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter. Washington Post, December 12, 2019. https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/?arc404=true. Accessed 6 Jan 2020

Cimpanu C (2019) City of LA sues Weather Channel app for sharing location data with advertisers. https://www.zdnet.com/article/city-of-la-sues-weather-channel-app-for-sharing-location-data-with-advertisers/. Accessed 5 Aug 2019

Commonwealth v. Almonor (2019) 120 N.E. 3d. 35 (Mass.)

Conger K, Fausset R, Kovaleski SF (2019) San Francisco bans facial recognition technology, New York Times, May 14, 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Accessed 25 June 2019

Dasgupta A (2017) How geospatial justice can restrain misuse of data against humanity. Geospatial World, 10/16/2017. https://www.geospatialworld.net/blogs/need-to-develop-geospatial-justice/. Accessed 25 June 2019

Dellinger EJ (2019) How the biggest tech companies spent half a billion dollars lobbing Congress. Forbes, 30 Apr 2019. https://www.forbes.com/sites/ajdellinger/2019/04/30/how-the-biggest-tech-companies-spent-half-a-billion-dollars-lobbying-congress/#26329d3c57c9. Accessed 25 June 2019

Dobson JE (2002) Geoslavery. Paper presented at Annual Meeting of the American Association of Geographers, 19–22 Mar 2002, Los Angeles, CA

Dobson JE (2007) Under an electronic eye, 24/7. Ft. Worth Star-Telegram, December 27, 2007, also published as Geoslavery in the Stacy Peterson case, The Cleburne News, 3 Jan 2008

Dobson JE (2009) Big brother has evolved. Nature 458:968. https://doi.org/10.1038/458968a

Dobson JE, Fisher PF (2003) Geoslavery. IEEE Technol Soc Mag 22(1):47–52. https://doi.org/10.1109/mtas.2003.1188276

Dobson JE, Fisher PF (2007) The Panopticon's changing geography. Geogr Rev 97(3):307–323. https://doi.org/10.1111/j.1931-0846.2007.tb00508.x

Federal Trade Commission (2014) Data brokers: A call for transparency and accountability. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014. Accessed 25 June 2019

Fisher PF, Dobson JE (2003) Who knows where you are, and who should, in the era of mobile geography? Geography 88(4):331–337

Foner E (2016) Gateway to freedom: the hidden history of the underground railroad. Norton & Company, New York. ISBN-1978-0393352191

Fowler S (2018) The 3 biggest challenges for tech in 2019. New York Times, 29 Dec 29 2018. https://www.nytimes.com/2018/12/29/opinion/tech-2018-trends-2019-predictions.html. Accessed 25 June 2019

Franklin JH, Schweninger L (1999) Runaway slaves: Rebels on the plantation. Oxford University Press, Oxford. ISBN-10: 0195084519, ISBN-13: 978-0195084511

Garrett BL (2015) The privatization of cities' public spaces is escalating. It is time to take a stand. The Guardian, 4 Aug 4 2015. https://www.theguardian.com/cities/2015/aug/04/pops-privately-owned-public-space-cities-direct-action. Accessed 25 June 2019

Gomez V (2019) Facebook adds new background location privacy controls to its Android app. RR-Magazine, 20 Feb 2019. https://rr-magazine.com/2019/02/20/facebook-adds-new-background-location-privacy-controls-to-its-android-app/. Accessed 25 June 2019

González MC, Hidalgo CA, Barabási AL (2008) Understanding individual human mobility patterns. Nature 453:779–782. https://doi.org/10.1038/nature07850

Harris R, Keller MH, Valentino-DeVries J (2018) 8 Places where smartphones tracked people's movements. New York Times, 15 Dec 2018. https://www.nytimes.com/2018/12/15/business/location-tracking-phones.html. Accessed 25 June 2019

Hartzog W, Selinger E (2019) Why you can no longer get lost in the crowd. New York Times, 17 Apr 2019. https://www.nytimes.com/2019/04/17/opinion/data-privacy.html. Accessed 25 June 2019

Harwell D (2019a) Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator. Washington Post, 19 Nov 2019. https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/. Accessed 6 Jan 2020

Harwell D (2019b) Colleges are turning students' phones into surveillance machines, tracking the locations of hundreds of thousands. Washington Post, 24 Dec 2019. https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/. Accessed 6 Jan 2020

Hatton C (2015) China "social credit": Beijing sets up huge system. BBC 26 Oct 2015. https://www.bbc.com/news/world-asia-china-34592186. Accessed 25 June 2019

Helbing D, Frey BS, Gigerenzer G, Hafen E, Hagner M, Hofstetter Y, van den Hoven J, Zicari RV, Zwitter A (2017) Will democracy survive big data and artificial intelligence? Scientific American, 25 Feb 2017. https://doi.org/10.1007/978-3-319-90869-4_7

Herbert WA (2006) No direction home: will the law keep pace with human tracking technology to protect individual privacy and stop geoslavery? I/S: A J Law Policy Inf Soc 2(3):409–473. https://kb.osu.edu/bitstream/handle/1811/72738/1/ISJLP_V2N2_409.pdf. Accessed 26 June 2019

Herbert WA (2008) Workplace electronic privacy protections abroad: the whole wide world is watching. Univ Florida J Law Public Policy 19 J.L. & PUB POL'Y 379–420. https://works.bepress.com/william_herbert/12/. Accessed 26 June 2019

Herbert WA, Tuminaro AK (2008) The impact of emerging technologies in the workplace: who's watching the man (Who's watching me)? Hofstra Labor Employ J 25(2):355–393. https://scholarlycommons.law.hofstra.edu/cgi/viewcontent.cgi?article=1431&context=hlelj. Accessed 25 June 2019

HIPAA Journal (2019) What is the purpose of HIPAA? https://www.hipaajournal.com/purpose-of-hipaa/. Accessed 5 Aug 2019

Hu W, Haag M (2019) 90,000 packages disappear daily in N. Y. C. Is help on the way? New York Times, 3 Dec 2019. https://www.nytimes.com/2019/12/02/nyregion/online-shopping-package-theft.html. Accessed 5 Jan 2020

Jaschik S (2019) New SAT score: adversity. Inside Higher Ed. https://www.insidehighered.com/admissions/article/2019/05/20/college-board-will-add-adversity-score-everyone-taking-sat. Accessed 5 Aug 2019

Jeans D (2019) Related's Hudson Yards; Smart city or surveillance city. The Real Deal: New York Real Estate News, 15 Mar 2019. https://therealdeal.com/2019/03/15/hudson-yards-smart-city-or-surveillance-city/. Accessed 25 June 2019

Kar B, Crowsey RC, Zale JJ (2013) The myth of location privacy in the United States: surveyed attitude versus current practices. Prof Geogr 65(1):47–64. https://aquila.usm.edu/fac_pubs/7559. Accessed 25 June 2019

Kozak SL, Dobson JE, Wood JS (2015) Geography's American constituency: results from the AGS geographic knowledge and values survey. Int Res Geogr Environ Educ 24(3):1–22. https://doi.org/10.1080/10382046.2015.1034457

Kuo L (2019) China bans 23 m from buying travel tickets as part of 'social credit' system. The Guardian, Mar 2019. https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system?CMP=share_btn_fb. Accessed 26 June 2019

Kwan M-P, Casas I, Schmitz BC (2004) Protection of geoprivacy and accuracy of spatial information: how effective are geographical masks? Cartographica 39(2):15–28. https://doi.org/10.3138/x204-4223-57mk-8273

Lemmings D (ed) (2018) The Oxford Edition of Blackstone's commentaries on the laws of England: book I: of the rights of persons. Oxford University Press, Oxford. ISBN: 9780199600991

Mirani L, Nisen M (2014) The nine companies that know more about you than Google or Facebook. Quartz. https://qz.com/213900/the-nine-companies-that-know-more-about-you-than-google-or-facebook/. Accessed 25 June 2019

Mistreanu S (2018) Life inside China's social credit laboratory; The party's massive experiment in ranking and monitoring Chinese citizens has already started. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/. Accessed 6 Aug 2019

Pew Research Center (2018) The state of privacy in post-Snowden America. https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/. Accessed 25 June 2019

Rzeszewski M, Luczys P (2018) Care, indifference and anxiety—attitudes toward location data in everyday life. Int J Geo-Inf 7:383. https://doi.org/10.3390/ijgi7100383. Accessed 25 June 2019

Schuppe J (2019) How facial recognition became a routine policing tool in America. NBC News Online, 11 May 11 2019. https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251. Accessed 25 June 2019

Shoichet CE (2019) What 'merit-based' immigration means, and why Trump keeps saying he wants it. https://www.cnn.com/2019/05/16/politics/merit-based-immigration-explainer/index.html. Accessed 5 Aug 2019

Slinn S, Herbert WA (2011) Some think of the future: Internet, electronic and telephonic labor representation elections. 56 St. Louis U. L.J. 171:190–192 (Fall 2011). https://digitalcommons.osgoode.yorku.ca/scholarly_works/461/. Accessed 26 June 2019

Smith R, Leberstein S (2015) Rights on demand: ensuring workplace standards and worker security in the in-demand economy. Natl Employ Law Project (Sept 2015) https://s27147.pcdn.co/wp-content/uploads/Rights-On-Demand-Report.pdf. Accessed 25 June 2019

Song B (2018) The West may be wrong about China's social credit system. https://www.washingtonpost.com/news/theworldpost/wp/2018/11/29/social-credit/?noredirect&utm_term=.2c7afc38be63. Accessed 25 June 2019

Speier J (2019) Rep Speier calls on Apple and Google to remove a Saudi Government app tracking women. Press Release, 22 Feb 2019. https://speier.house.gov/media-center/press-releases/rep-speier-calls-apple-and-google-remove-saudi-government-app-tracking. Accessed 26 June 2019

State Farm Insurance Company (2019) Kim's discount (drive safe & save). State Farm® commercial. https://www.youtube.com/watch?v=yMsmubcvY_k. Accessed 5 Aug 2019

Stauffer J (2002) The black hearts of men: radical abolitionists and the transformation of race. Harvard University Press, Cambridge. ISBN-10: 0674013670, ISBN-13: 978-0674013674

Swisher K (2019) Be paranoid about privacy. New York Times, 24 Dec 2019. https://www.nytimes.com/2019/12/24/opinion/location-privacy.html Accessed 6 Jan 2020

Thompson SA, Warzel C (2019) Twelve million phones, one dataset, zero privacy. New York Times, 19 Dec 2019 https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Accessed 6 Jan 2020

Thorbecke C (2019) Long Island police partner with Amazon's Ring to crack down on porch pirates. ABC News, 4 Dec 2019. https://abcnews.go.com/Technology/long-island-police-crack-porch-pirates-amazon-ring/story?id=67489715. Accessed 6 Jan 2020

Valentino-DeVries J (2019) Tracking phones, Google is a dragnet for the police. New York Times, 13 Apr 2019. https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html. Accessed 25 June 2019

Vance A (2019) Protecting student privacy. Opinion Letter. New York Times, 19 Dec 2019. https://www.nytimes.com/2018/12/19/opinion/letters/student-privacy-laws.html. Accessed 6 Jan 2020

Venook J (2017) The upcoming privacy battle over wearables in the NBA. The Atlantic, 10 Apr 2017. https://www.theatlantic.com/business/archive/2017/04/biometric-tracking-sports/522222/. Accessed 25 June 2019

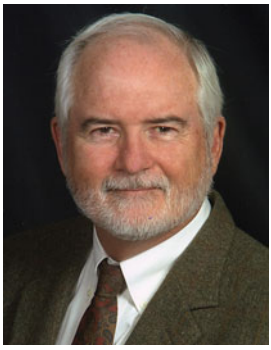
Warzel C, Thompson SA (2019) How your phone betrays democracy. New York Times, 21 Dec 2019 https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html. Accessed 6 Jan 2020

Weidemann C, Swift J, Kemp K (2018) Geosocial footprints and geoprivacy concerns. In: Thatcher J, Ekert J, Shears A (eds) Thinking big data in geography: New regimes, new research. University of Nebraska, Lincoln (doi:9781496205377)

Williams T (2019) In high-tech cities, no more potholes, but what about privacy? New York Times, 1 Jan 2019. https://www.nytimes.com/2019/01/01/us/kansas-city-smart-technology.html. Accessed 25 June 2019

Wingfield N (2018) Amazon buys Ring, maker of smart home products. New York Times, 27 Feb 2018. https://www.nytimes.com/2018/02/27/business/dealbook/amazon-buys-ring.html. Accessed 6 Jan 2020

Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Hachette Book Group, New York. ISBN-978-1-61039-659, ISBN-968-1-61039-570-0



Jerome E. Dobson is Emeritus Professor of Geography, University of Kansas; President Emeritus, American Geographical Society; and a Trustee of Reinhardt University. He is a Jefferson Science Fellow with the National Academies and the U.S Department of State.

William A. Herbert is a Distinguished Lecturer at Hunter College, City University of New York, and a Faculty Associate at the Roosevelt House Institute for Public Policy. He is also Executive Director of the National Center for the Study of Collective Bargaining in Higher Education and the Professions.