# Human Tagging

**Jeffrey Voas,** IEEE Fellow
**Nir Kshetri,** University of North Carolina at Greensboro

*Several technologies—some new, some familiar—are being used to identify, authenticate, and track people on the go. Human tagging offers many novel benefits but also raises serious privacy concerns, and the laws, regulations, and policy guidelines regarding its practice are inconsistent and unevenly applied.*

Should we be able to drive to and from different destinations, go shopping, and talk to or get together with others without the government or companies knowing about it? What information about our daily activities—the routes we travel, the things we buy, the people we communicate with, and so on—can be lawfully collected by other entities, and who should have access to that data? Such questions are increasingly important as devices add more functionality, sensor networks proliferate, analytics improves, and data storage becomes cheaper.

The limits of privacy in the information age, especially since 9/11 and the spread of terrorism across the world, is a subject of ongoing and heated debate. Technologically advanced authoritarian regimes practice nearly limitless surveillance, and many European and Asian democracies seem to be moving in the same direction. The US hasn't gone as far yet due to a combination of factors including the Fourth Amendment's prohibition of warrantless searches, public outrage over revelations of government snooping, and litigation by privacy advocates. However, the USA Patriot Act of 2001 authorized more intrusive investigative techniques, and recent advances have made it easier than ever for both government agencies and private companies to monitor what we do, where we go, and who we interact with.

## HUMAN TAGGING

Cutting-edge technology has always been used to identify, authenticate, and track humans. For example, law-enforcement agencies began taking mug shots of arrestees in the 1840s soon after the invention of photography (en.wikipedia.org/wiki/Mug_shot). Today, various biometrics including fingerprints, palm geometry, retina and face characteristics, gait, voice, DNA, and keystroke patterns—are used in a wide variety of security applications.

Information and communications technology and the Internet have made it possible for companies and governments to gather, aggregate, analyze, and share all kinds of


0018-9162/17/$33.00 © 2017 IEEE

EDITOR **JEFFREY VOAS**
NIST; j.voas@ieee.org

sensitive or personally identifiable information including full names, background and genetic data (birthplace, birth date, gender, race/ethnicity), Social Security/national ID numbers; relatives and contacts; driver's license, license plate, and vehicle registration numbers; passport numbers and travel histories; addresses and phone numbers; financial account numbers and transaction histories; tax records; IP addresses, login names, email addresses, device MAC numbers, and web browsing histories; criminal and court records; social media use, including forum postings and uploaded documents, photos, and videos; and consumption habits.

Table 1 list several technologies being used to identify, authenticate, and track users on the move either in public or within a space such as a home, office, care facility, or store. Some of these technologies are relatively new, while others have been around for a while but are being repurposed—in some cases without our knowledge or permission—for what we call human tagging.

### Benefits

Human tagging offers three main benefits to users and/or corporate or government entities.

First, human tagging reduces the reliance on traditional means of identification like driver's licenses, passports, and organization IDs. This not only increases convenience but can be critical in certain scenarios—for example, to identify a dead victim, an unconscious patient, or an uncooperative criminal suspect. Tagging can also provide more secure authentication and identity-based access control, such as admittance to a facility or access to credit or services.

Second, human tagging can be used to track users' whereabouts in real time—for example, to deliver location-based services or ascertain where certain individuals are or whether people in an area are authorized to be there. User behavior and mobility patterns can also be inferred from aggregated location data.

Third, human tagging can facilitate activities such as opening a locked door, operating a restricted device, and purchasing or checking out items because tags can be scanned or tracked quickly and easily—in some cases, automatically.

> Human tagging places a premium on security and efficiency at the expense of privacy.

### Concerns

On the flip side, human tagging places a premium on security and efficiency at the expense of privacy. When people use their smart credit card, arrange an Uber lift, talk to Alexa, and walk through a store with cameras, are they aware of how much data about them is being collected and what is being shared with others? When should such technology be restricted or outlawed?

Furthermore, like any technology, human tagging can have unintended negative consequences. For example, microchip implants could lead to a new underground business in removing or swapping chips using minor surgery; location data from smartphones can be used for spying and stalking; and employers could use data from company-issued fitness and activity trackers to surreptitiously monitor and even discriminate against their workers.

## MICROCHIP IMPLANTS

Digital microchip implants have long been used to identify the ownership of pets and livestock. The success of this technology naturally led to exploring its use in people, especially for medical purposes.

In 2004, the US Food and Drug Administration (FDA) approved use of VeriChip, a glass-coated, rice grain–size RFID chip injected in the arm under the skin that, when exposed to a barcode scanner, links to a secure database containing information about the user. The chip was designed to save lives and reduce medical errors. For example, when linked to a health record database, it can provide crucial information to caregivers about a patient who can't speak, such as the existence of other implantable devices like a pacemaker or a chronic disease like diabetes. It can also help identify dementia patients who might wander off from a care facility.[1]

In 2010, after some early pilot projects, the Florida-based developer of VeriChip partnered with Innovations Avocare, which builds physician portals to health record databases, to incorporate the chip—renamed PositiveID—in the state's healthcare system.[2] However, concerns about patient privacy and possible health risks inhibited adoption, inducing the company to stop marketing the technology.[3] However, other companies, such as Microchips Biotech (microchipsbiotech.com), are continuing to develop chip implants for medical applications, such as storing and delivering drugs in lieu of using needles.

Chip implants are also used to authenticate user identities. In July 2004, Mexico's then attorney general, Rafael Macedo de la Concha, stated that he and 160 staff members had

**TABLE 1.** Human tagging technologies.

| Technology | Examples | Applications/benefits | Risks/concerns |
|---|---|---|---|
| Microchip implants | • VeriChip/PositiveID<br>• Microchips Biotech<br>• Epicenter (Stockholm, Sweden)<br>• Three Square Market (Wisconsin, USA)<br>• Baja Beach Club (Barcelona, Spain) | • Identification/authentication<br>• Access control<br>• Medical records access<br>• Medical applications (for example, glucose monitoring and drug delivery)<br>• Electronic payments<br>• Cadaver identification/tracking | • Possible health complications (for example, infection, chip migration, and cancer)<br>• Device cloning/identity theft<br>• Surreptitious employee tracking<br>• Human trafficking |
| Wearable RFID tags | • Alzheimer's Real Time Location System<br>• QR-coded stickers (Iruma, Japan) | • Identification<br>• Low-cost tracking<br>• Identifying lost dementia/Alzheimer's patients<br>• Improved elder care management | • Easily removed<br>• Vulnerable to wear and tear/weather |
| Fitness and activity trackers | • Fitbit, Jawbone UP, and Nike+ Fuelband bracelets<br>• Smart watches | • Increased workplace health, wellness, and productivity<br>• Lower company health insurance costs | • Invasive employee monitoring, including outside the workplace<br>• Discrimination against employees due to poor health or low productivity |
| Smart cards | • Visa payWave, Mastercard PayPass, and GeldKarte (Germany)<br>• US Department of Defense Common Access Card<br>• Smart Card Driving License (India)<br>• Federal Emergency Management Agency (FEMA) emergency responder ID card<br>• ID-Kaart (Estonia), Resident Identity Card (China) | • Electronic payments<br>• Two-factor/multifactor identification/authentication<br>• Access control<br>• Computer security (for example, single sign-on, encryption, and secure web browsing)<br>• Multipurpose functionality | • Lesser-known vulnerabilities—false sense of security<br>• Inadequate security standards<br>• Identity theft due to more personal data<br>• Targeted and mass surveillance |
| Mobile devices | • GPS<br>• Wi-Fi<br>• Motion sensors | • Location-based services<br>• Wireless connectivity<br>• Big data/crowdsourcing analytics | • Location-based advertising<br>• Targeted surveillance<br>• Electronic eavesdropping<br>• Cyberstalking |
| Intelligent "things" | • Intelligent virtual assistants<br>• Smart home systems<br>• Healthcare IoT devices<br>• Vehicle/driver data collection systems<br>• Face-recognition software for retail store cameras<br>• License-plate reader data analytics/sharing services | • Wireless/hands-free operation<br>• Increased safety and efficiency<br>• Remote monitoring<br>• Big data/crowdsourcing analytics | • Electronic eavesdropping<br>• New hacking/cyberattack vectors<br>• Voice/image capture<br>• Presence data<br>• Inferred user characteristics, behaviors, and mobility patterns |

VeriChips implanted to control access to restricted rooms and sensitive documents related to the country's drug cartels.[4] The same year, a Barcelona country club offered VeriChip implants to members to access VIP lounges.[5] After the Hurricane Katrina disaster in August 2005, VeriChips were implanted in human cadavers to help identify and track victims.[6]

Another application of microchip implants is user convenience—that is, to serve as a substitute for keys and credit cards. In January 2015, Epicenter, a corporate innovation hub in Stockholm, Sweden, began implanting volunteer employees with a chip that enables them "to open doors, operate printers, or buy smoothies with a wave of the hand."[7] In August 2017, a Wisconsin tech company became

the first US company to offer similar hand-implanted chips.[8]

Criminals have discovered a more nefarious application for chip implants: human trafficking. In October 2015, an ER doctor at a major US hospital reported that one of his patients, a young woman forced into prostitution, had a GPS tracking device implanted in her side.[9]

## WEARABLE RFID TAGS

Wearable RFID tags in conjunction with installed or portable barcode scanners can be used to track people much like retailers use barcodes and RFID tags to track inventory in stores and warehouses.

In 2013, researchers at Universiti Putra Malaysia developed a prototype real-time location system using wearable RFID tags to track patients at an Alzheimer's care facility. The tags not only identify where residents are but reveal which areas they frequent and the routes they follow, information that can be used to better understand patient needs and enhance care management.[10]

In December 2016, the Japanese city of Iruma, near Tokyo, introduced a free service to track elderly people with dementia using tiny, water-resistant QR-coded stickers that attach to fingers and toes. If a wearer becomes lost, police can scan the QR code to obtain the person's identity and contact information.[11]

Unlike chip implants, wearable RFID tags don't require a surgical procedure with its attendant health risks. On the other hand, they're easily removed and exposed to the elements and thus less durable.

## FITNESS AND ACTIVITY TRACKERS

In recent years, employers have begun launching "wellness" programs and various health and productivity initiatives that encourage, reward, and even require employees to regularly wear devices like Fitbit and Jawbone UP wristbands. By monitoring employees' activity levels, weight, stress and sleep patterns, and other data, corporations seek to make their workforce healthier, reduce accidents, and keep insurance costs in check. Data analytics firm Tractica expects enterprise purchases of wearable devices to grow 108 percent annually from 2013 through 2020.[12]

Although such programs do benefit employees, they also raise significant privacy concerns including increasingly intrusive monitoring by employers, including outside the workplace, and potential discrimination (promotion opportunities, for example) against those deemed less fit or productive.[13]

## SMART CARDS

Chip-enabled smart cards are used around the world for numerous purposes including electronic payments (for example, credit and debit cards, fuel cards, public transit and toll-road cards, and phone payment cards), identification (for example, national ID cards, organization ID cards, healthcare ID cards, drivers' licenses, student ID cards, and e-passports), authorization (for example, to access pay TV or certain websites), and security (for example, government or military access control, disk encryption, computer login, and secure web browsing). The chip's memory can contain a wide variety of user information depending on the card's purpose.

Smart cards provide more powerful features and antifraud protections than traditional magnetic swipe cards, yet the potentially large quantity of data they contain puts users' privacy at greater risk should the card become compromised—for example, through a man-in-the-middle attack.[14] In addition, the concentration of more and more functions in popular multipurpose cards makes it easier for companies or governments to keep tabs on user behavior.

A case in point is China's all-encompassing surveillance system, the Golden Shield Project, which was first implemented in 2007 in the southern city of Shenzhen. In conjunction with Internet censorship (the "Great Firewall"), email and cell phone monitoring, and the extensive deployment of police cameras with face-recognition software in public areas, all citizens will be required to carry residency cards with government-issued chips.[15]

> *Data on the chip will include not just the citizen's name and address but also work history, educational background, religion, ethnicity, police record, medical insurance status and landlord's phone number. Even personal reproductive history will be included, for enforcement of China's controversial "one child" policy. Plans are being studied to add credit histories, subway travel payments and small purchases charged to the card.*[16]

By 2020, China also hopes to roll out its Social Credit System, which assigns a numerical rating to every adult based on factors such as financial standing, criminal record, and social media behavior.[17] One expert has described it as "Amazon's consumer tracking with an Orwellian political twist."[18]

## MOBILE DEVICES

Cell phones, laptops, car navigation systems, and other mobile technologies use GPS geolocation for various consumer applications such as driving directions, traffic and weather reports, ridesharing, dating, and nearby restaurant recommendations. However, location data can also be exploited without the user's knowledge to serve up ads for location-based services and for other questionable and possibly illegal purposes such as surveillance and cyberstalking. Aggregated over time, such data can reveal movements we might regard as private—for example, travel to a medical clinic or political demonstration.

Numerous companies have engaged in sketchy data collection and sharing practices. For example, in 2011, *The Wall Street Journal* reported

that iPhones and Android phones secretly sent user location information to Apple and Google, respectively, as part of the companies' efforts to tap the multibillion-dollar location-based services market.[19] The same year, a security blogger revealed that Nissan transmitted the location, speed, and destination of its Leaf brand cars to websites that other users could access through a built-in RSS reader.[20] A recent Carnegie Mellon University study found that user location data was shared with social networking sites like Facebook and e-commerce sites like Groupon thousands of times a week.[21]

## INTELLIGENT "THINGS"

The devices we interact with in the emerging Internet of Things (IoT) are becoming increasingly intelligent, just as the places we frequent are adding more powerful cameras and other sensors. All of these "things" record the user's location, listen to conversations, and look at texts and photos.[26]

Mobile device users' location can also be inferred less precisely, but still with a high degree of accuracy, through means other than GPS—namely, Wi-Fi signals[27] and smartphone motion sensors.[28]

> Current laws fail to adequately address the privacy challenges associated with human tagging technologies.

Controversy has swirled over the warrantless use of International Mobile Subscriber Identity (IMSI) catchers, colloquially known as stingrays, by federal, state, and local law enforcement agencies to help identify, track, and apprehend criminal suspects.[22] These devices are essentially cell-tower simulators that trick target phones into connecting to them, making it possible to track the users' location and even eavesdrop on their conversations. Commercial IMSI catchers are largely sold to government agencies, but researchers have created low-cost versions, demonstrating that the technology is within reach of tech-savvy hobbyists or criminals.[23]

GPS data can also be used by so-called "stalker apps."[24] Some of these apps—like the now-defunct Girls Around Me—combine such data with publicly available information from social media sites like Facebook and Twitter to lets users snoop on and send messages to strangers.[25] Other apps, like FlexiSPY, can be surreptitiously installed—by a parent or partner, for example—on a phone to track our presence, creating a data footprint, and might include software specifically designed to identify us, recognize us, or track our whereabouts.

Last month's Cybertrust column highlighted the ability of one such IoT technology—intelligent virtual assistants such as Amazon's Alexa and Google Assistant—to capture human voice commands and conversations.[29] Other intelligent devices record potentially sensitive information including what we put in our fridge, medicines we take, whether someone is at home, what we watch on TV, our electricity usage patterns, our driving habits, and so on. All of this data can be exploited for commercial purposes by device manufacturers and app developers; it's also less secure than consumers realize due to vulnerabilities in many IoT devices.

Both public and private spaces have a growing array of devices including motion sensors, microphones, and high-resolution cameras that record human activity. These devices are becoming ever-more powerful—for example, some high-end store surveillance systems employ the same face-recognition technology used by airports, banks, and casinos to alert store personnel to the presence of VIP customers and potential shoplifters.[30] In addition, data from multiple devices—for example, automated license-plate readers—can be fused to create a detailed picture of a person's movements over time and across different locations.[31]

## PRIVACY LAWS AND HUMAN TAGGING

In most countries, laws that govern the collection, storage, analysis, processing, reuse, and sharing of data were enacted decades ago and thus fail to adequately address the privacy challenges associated with human tagging technologies. Here we look at some recent legislative, regulatory, and judicial responses to these challenges in the EU, the US, and China.

### European Union

In June 2015, the British High Court ruled that authorities had to remove an electronic ankle tag attached to an imam suspected of recruiting for al-Shabaab—a Somalia-based jihadi fundamentalist group designated as a terrorist organization by numerous countries including the UK, the US, Canada, and Australia—because it breached Article 3 of the European Convention on Human Rights, which prohibits "inhuman or degrading treatment or punishment."[32]

In November of the same year, the Dutch Data Protection Authority (DPA) published a report alleging that Nike's Nike+ Running app violated the country's privacy laws in two ways. First, the app, which can be synchronized with sensors in running shoes or other wearable devices to track distance traveled, speed, time, and calories burned, illegally collected user health data. Second, Nike failed to sufficiently inform users in its privacy notices about the types of personal data the app collected and processed; thus, users didn't give explicit consent.[33]

In March 2016, the DPA ruled that companies can't use fitness and activity trackers to monitor employees' wellness and productivity even with consent on the grounds that employees, due to their financial dependence on their employer, can't freely give consent. Moreover, it asserted that the data collected by such devices, such as movement and sleep patterns, is sensitive and personal and thus subject to the country's stringent data-protection legislation.[34] Other EU countries will likely follow the Netherlands's lead and enact similar measures.

In April 2016, the European Parliament approved the General Data Protection Regulation (GDPR; www.eugdpr.org), which goes into force in May 2018. Superseding the 1995 Data Protection Directive, GDPR aims to "protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established."

GDPR significantly strengthens consent requirements:

> *Companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.*

In addition, GDPR gives individuals the right to know "whether or not personal data concerning them is being processed, where and for what purpose." The "right to be forgotten" has been more precisely reworded as the "right to data erasure." Perhaps most importantly, GDPR legally mandates *privacy by design*: data-protection mechanisms must be incorporated into the design of systems rather than added later, and systems by default must collect only the minimum amount of personal data needed for a task and limit access to such data.

### United States

Unlike the EU, data-protection legislation in the US is piecemeal, with no overarching framework—separate federal and state laws applies to different, narrowly defined types of personal data.[35] The US Health Insurance Portability and Accountability Act of 1996 does broadly restrict access to and the dissemination of personal health records, but such data is limited to that collected by healthcare providers such as doctors, hospitals, and nursing homes and to health insurers; HIPAA doesn't apply to health information collected by wearables.[36]

Some efforts are underway that might leading to stronger regulatory protections of personal and sensitive data. In January 2017, the Federal Trade Commission released a report on cross-device tracking, in which companies associate data collected on the same consumer from multiple Internet-based devices including wearables.[37] The report outlines best practices and recommends that companies "(1) be transparent about their data collection and use practices; (2) provide choice mechanisms that give consumers control over their data; (3) provide heightened protections for sensitive information, including health, financial, and children's information; and (4) maintain reasonable security of collected data."

In the wake of the FDA's approval of microchip implants, four states alarmed by the future prospect of mandatory use of such technology—Wisconsin, North Dakota, California, and Oklahoma—passed laws prohibiting companies and government entities from forcing a person to have RFID chips implanted under the skin; similar legislation is pending in Nevada.[38]

Many states have enacted laws protecting user location data privacy rights.[39] Although no federal statutes currently exist, several bills have been proposed to address the issue including the Location Privacy Protection Act, the Online Communications and Geolocation Protection Act, the Geolocation Privacy and Surveillance Act, and the Transportation Appropriations Act, which has a provision regarding vehicle GPS data (www.gps.gov/policy/legislation/gps-act).

### China

Given China's emphasis on infrastructure security and cybercontrol to maintain social stability and political unity, the country provides a relatively lower level of privacy protection for user data compared to the EU and US.[40] In June 2017, a new Cybersecurity Law went into effect that standardizes the collection and usage of personal data by network operators, including a requirement to inform and obtain consent from users, and criminalizes the unauthorized disclosure of data. However, the law is vague as to what constitutes personal data or what a network operator is, and has ambiguous mandates such as network operators must "obey social norms and commercial ethics." In addition, data on Chinese citizens must be stored on domestic servers, making government surveillance easier.[41,42]

Human tagging offers many tangible social benefits including greater convenience and security protection, new types of location-based applications in a variety of sectors, and a source of big data that can yield novel insights into human behavior. Governments, corporations, and individuals all have something to gain. However, these technologies also pose considerable privacy risks, and their ultimate value will depend on the sophistication and awareness of users; the goals, resourcefulness, and ethics of the organizations that deploy them; and the laws, regulations, and policy guidelines that govern their use.[43,44] Human tagging can be used for noble

or ignoble purposes, and whether it will become a new means of "staying connected," a tool of mass surveillance, or both remains an open question.[45]

## REFERENCES


1. L. Sullivan, "FDA Approves RFID Tags for Humans," *InformationWeek*, 14 Oct. 2004; www.informationweek.com/fda-approves-rfid-tags-for-humans/d/d-id/1027823?.
2. J. Edwards, "PositiveID Deal Advances Use of Microchip Implants in Florida Health System," CBS News, 3 Dec. 2009; www.cbsnews.com/news/positiveid-deal-advances-use-of-microchip-implants-in-florida-health-system.
3. J. Edwards, "Down with the Chip: PositiveID Axes Its Scary Medical Records Implant," CBS News, 17 Sept. 2010; www.cbsnews.com/news/down-with-the-chip-positiveid-axes-its-scary-medical-records-implant.
4. W. Weissert, "Microchips Implanted in Mexican Officials," NBC News, 14 July 2004; www.nbcnews.com/id/5439055/ns/technology_and_science-tech_and_gadgets/t/microchips-implanted-mexican-officials.
5. S. Morton, "Barcelona Clubbers Get Chipped," BBC News, 29 Sept. 2004; news.bbc.co.uk/1/hi/technology/3697940.stm.
6. M. Kanellos, "RFID Chips Used to Track Dead after Katrina," CNET News, 16 Sept. 2005; www.cnet.com/news/rfid-chips-used-to-track-dead-after-katrina.
7. J. Brooks, "A Swedish Company Has Started Implanting Microchips under its Employees' Skin," *Business Insider*, 5 Apr. 2017; www.businessinsider.com/startup-workers-wearing-microchips-2017-4.
8. M. Astor, "Microchip Implants for Employees? One Company Says Yes," *The New York Times*, 25 July 2017; www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html.
9. D. Gorenstein, "Health Care Takes on the Fight against Trafficking," *Marketplace*, 2 Mar. 2016; www.marketplace.org/2016/03/02/health-care/health-care-takes-fight-against-trafficking.
10. M.F. Abuhan et al., "Tracking Elderly Alzheimer's Patient Using Real Time Location System," 2013; www.spp-j.com/spp/1-1/spp.2013.11A0002.
11. "Japan Tracks Dementia Patients with QR Codes Attached to Fingernails," BBC News, 8 Dec. 2016; www.bbc.com/news/world-asia-38247437.
12. P. Olson, "More Bosses Expected to Track Their Staff through Wearables in the Next 5 Years," *Forbes*, 1 June 2015; www.forbes.com/sites/parmyolson/2015/06/01/wearables-employee-tracking/#32b0831e4ece.
13. I. Manohka, "Why the Rise of Wearable Tech to Monitor Employees Is Worrying," *The Independent*, 4 Jan. 2017; www.independent.co.uk/life-style/gadgets-and-tech/why-the-rise-of-wearable-tech-to-monitor-employees-is-worrying-a7508656.html.
14. A. Greenberg, "X-ray Scans Expose an Ingenious Chip-and-Pin Card Hack," *Wired*, 10 Oct. 2015; www.wired.com/2015/10/x-ray-scans-expose-an-ingenious-chip-and-pin-card-hack.
15. F. McCreery, "But at What Cost? Shenzhen, China and the Social Implications of Urban 'Success'," *Anthrojournal*, 14 Jan. 2012; anthrojournal.com/issue/may/article/but-at-what-cost-shenzhen-china-and-the-social-implications-of-urban-success1.
16. K. Bradsher, "China Enacting a High-Tech Plan to Track People," *The New York Times*, 12 Aug. 2007; www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?pagewanted=print.
17. M. FlorCruz, "China to Use Big Data to Rate Citizens in New 'Social Credit System,'" *Int'l Business Times*, 28 Apr. 2015; www.ibtimes.com/china-use-big-data-rate-citizens-new-social-credit-system-1898711.
18. F. Obbema, M. Vlaskamp, and M. Persson, "China Rates Its Own Citizens—Including Online Behaviour," *de Volksrant*, 25 Apr. 2015; www.volksk-rant.nl/buitenland/china-rates-its-own-citizens-including-online-behaviour~a3979668.
19. J. Angwin and J. Valentino-DeVries, "Apple, Google, Collect User Data," *The Wall Street J.*," 22 Apr. 2011; www.wsj.com/articles/SB10001424052748703983704576277101723453610.
20. D. Storm, "Nissan Leaf Secretly Leaks Driver Location, Speed to Websites," *Computerworld*, 14 June 2011; www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to-websites.html.
21. B. Spice, "Carnegie Mellon Study Shows People Act to Protect Privacy When Told How Often Phone Apps Share Personal Information," CMU School of Computer Science News, 23 Mar. 2015; www.cs.cmu.edu/news/carnegie-mellon-study-shows-people-act-protect-privacy-when-told-how-often-phone-apps-share-personal-information.
22. R. Gallagher, "Meat the Machines That Steal Your Phone's Data," *Ars Technica*, 25 Sept. 2013; arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data.
23. B. Schneier, "The Further Democratization of Stingray," blog, 27 Apr. 2015; www.schneier.com/blog/archives/2015/04/the_further_dem_1.html.
24. A. Cohen, "Will 'Stalking Apps' Be Stopped?," *Time*, 4 Feb. 2013; ideas.time.com/2013/02/04/will-stalking-apps-be-stopped.
25. I. Paul, "Girls Around Me App Voluntarily Pulled after Privacy Backlash," *PCWorld*, 2 Apr. 2015; www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html.
26. P. Cain, "Is a Stalker Spying on You through Your Phone? Here's What to Look for," Global News, 28 Sept. 2016; globalnews.ca/news/2966238/is-a-stalker-spying-on-you-through-your-phone-heres-what-to-look-for.

27. P. Sapiezynski et al., "Tracking Human Mobility Using Wi-Fi Signals," *PLoS ONE*, vol. 10, no. 7, 2015, e0130824; doi.org/10.1371/journal.pone.0130824.
28. J. Hua, Z. Shen, and S. Zhong, "We Can Track You if You Take the Metro: Tracking Metro Riders Using Accelerometers on Smartphones," *IEEE Trans. Information Forensics and Security*, vol. 12, no. 2, 2017, pp. 286–297.
29. H. Chung et al., "'Alexa, Can I Trust You?,'" *Computer*, vol. 50, no. 9, 2017, pp. 100–104.
30. C. Frey, "Revealed: How Facial Recognition Has Invaded Shops—and Your Privacy," *The Guardian*, 3 Mar. 2016; www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.
31. American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, July 2013; www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.
32. P. Dominiczak and E. Gosden, "Terror Suspect's Tag 'Violates His Human Rights,'" *The Telegraph*, 19 June 2015; www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11687979/Terror-suspects-tag-violates-his-human-rights.html.
33. Proskauer Rose LLP, "Dutch Privacy Watchdog to Nike—You Can't Just Do It," 29 Feb. 2016; www.lexology.com/library/detail.aspx?g=cad25150-7d5c-47a6-976d-986234750f51.
34. R. Chirgwin, "Don't Snoop on Staff via Wearables, Says Dutch Privacy Agency," *The Register*, 9 Mar. 2016; www.theregister.co.uk/2016/03/09/dont_snoop_on_staff_via_wearables.
35. "Should the U.S. Adopt European-Style Data-Privacy Protections?," *The Wall Street J.*, 10 Mar. 2013; www.wsj.com/articles/SB10001424127887324338604578328393797127094.
36. G. Gross, "Privacy Protections for Wearable Devices Are Weak, Study Says," CSO, 15 Dec. 2016; www.csoonline.com/article/3151006/security/privacy-protections-for-wearable-devices-are-weak-study-says.html.
37. Federal Trade Commission, *Cross-Device Tracking*, staff report, Jan. 2017; www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf.
38. L. Hohmann, "Lawmaker Wants to Ban Forced Microchip Implants, Markings," *WND*, 19 Feb. 2017; mobile.wnd.com/2017/02/lawmaker-wants-to-ban-forced-microchip-implants-markings.
39. P. Cihon, "Status of Location Privacy Legislation in the States: 2015," blog, 26 Aug. 2015; www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015.
40. N. Kshetri, "China's Data Privacy Regulations: A Tricky Trade-Off between ICT's Productive Utilization and Cyber-Control," *IEEE Security & Privacy*, vol. 12, no. 4, 2014, pp. 38-45.
41. S. Yan, "China's New Cybersecurity Law Takes Effect Today, and Many Are Confused," CNBC News, 21 May 2017; www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html.
42. J. Wagner, "China's Cybersecurity Law: What You Need to Know," *The Diplomat*, 1 June 2017; thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know.
43. A.A. Allen, "Privacy Law: Positive Theory and Normative Practice, *Harvard Law Rev.*, vol. 56, no. 3, 2013, pp. 241–251.
44. D. Bollier, *The Promise and Peril of Big Data*, The Aspen Inst., 2010; www.emc.com/collateral/analyst-reports/10334-ar-promise-peril-of-big-data.pdf.
45. G. Branstetter, "How the Fall of RFID Chips Explains Our Current Surveillance state," *The Daily Dot*, 14 May 2016; www.dailydot.com/via/rfid-tagging-smartphones-privacy.





**JEFFREY VOAS**, Cybertrust column editor, is an IEEE Fellow. Contact him at j.voas@ieee.org.

**NIR KSHETRI** is a professor of management at the Bryan School of Business and Economics, University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu