BULLETIN OF THE ATOMIC SCIENTISTS
2019, VOL. 75, NO. 3, 109–115
https://doi.org/10.1080/00963402.2019.1604886

Facial recognition and the future of privacy: I always feel like … somebody's watching me

Brenda Leong

ABSTRACT

In the 21st century, we live in a world packed with closed-circuit video cameras, facial recognition systems, radio frequency identification chips, electronic toll collectors, smartphones with location tracking, and widespread monitoring of our electronic communications. As deeply as the industrial revolution upended 20th century social norms and political structures, so too has modern information technology been a revolution, giving governments and large private corporations vast power to keep track of, manipulate, and potentially repress entire populations. China offers some examples in this area, but even democratically elected governments have shown a tendency to want to digitally profile and analyze their citizens without sufficient respect for individual privacy. And just as rampant industrialization had to be reined in to protect human rights and individual dignity, information technology and digital systems must be controlled to prevent abuse and exploitation. This "boundary setting" can come none too soon, as rapid advances in artificial intelligence allow an even greater ability to process and categorize the vast amounts of data generated by all our electronic devices.

KEYWORDS

Artifical intelligence; AI; privacy; tracking; facial recognition; surveillance

There is no more Orwellian thought than "Big Brother is Watching." Even without specifying exactly how people are being watched – whether from tracking cell phones or profiling online browsing behavior – it's a sobering thought to imagine constant surveillance. When the concept becomes literal, and people believe that cameras are, in fact, watching them everywhere they go, possibly even in their homes, certainly in their cars, the result is a chilling effect on individuals who may no longer feel free to live their lives the way they'd like. There's also the opportunity for extreme abuse, by governments, corporations, bad actors, international officials – and even by fellow citizens.

So what does that mean for people dealing with the facial recognition systems that are popping up all over? Individuals can use facial recognition to open their phones, access bank accounts, authorize payments and other on-line activity, or organize their photos. Organizations use these systems for managing facility access, crowd control, and hospitality functions, and governments use them for terrorist tracking, border security, and criminal investigations (Cullum 2018). New uses are being imagined and developed all the time (Bogle 2015). Is this good? Is it terrifying? Should we stop using it all together?

While there are certain leading thinkers who have publicly advocated for halting all use of facial recognition systems until standards and rules can be put in place, that seems unlikely to happen. Woodrow Hartzog, a Northeastern University professor of law and computer science and Evan Selinger, a professor of philosophy, do make a strong case for a complete ban on such systems, and it is certainly possible that individual states or localities may pilot such restrictions (Hartzog and Selinger 2018). But I believe a general, national ban is unlikely – and if a ban does occur, then the same concerns that are outlined here will continue to exist and continue to need to be addressed, but perhaps with more time available to do so. What's more likely is that society will continue to debate these applications "on the fly" as use cases abound.

"Say Cheese!"

When is your face just a photo and when is it a "biometric identifier?" Understanding how the tech systems work is a critical foundation for effectively understanding and evaluating the risks of facial recognition. (While this discussion is focused on facial recognition, there are many options for biometric systems that essentially all work following the same process. Facial recognition, finger/palm scans, and iris/retinal scans all have different pros and cons, so for one to be "better" would very much depend upon the use to which it was being put.)

CONTACT Brenda Leong bleong@FPF.org

A photo of a face is an image – possibly physically printed ink on paper, or perhaps displayed digitally. It is the actual two-dimensional picture of the person, which another human would look at and say: "That's my friend, Parva!"

In contrast, a facial recognition system does not create photos. It creates templates. This means that when the face is scanned, the system isn't taking your picture, it is creating a web design based on your facial structure that is generated by proprietary software. (That is, every company's system will do it differently, and they will not be interchangeable.) That web overlay is a template that is then turned into a series of 0's and 1's – which can then also be encrypted, if desired. To "enroll" someone in a database for facial recognition purposes, a scan is made of the real person's live face, for which the created template is then stored, along with a tag or code to connect to the full record of any other personal information collected or retained. If an actual picture of the person is part of the record, it is normally taken separately, and should be stored completely separately from the template.

When the person returns to be identified (or an image is selected from a video or photo for identification to be attempted), then the system scans the person or image, creates a new template, runs that template through the algorithmic math, and then compares the binary number against the enrolled file or files for a match. When a matching template is found, the person is identified. This process likely takes less than a second, and for any reputable system, no image is ever stored with the template, and no face can be recreated from the template. (By "reputable system," I mean that the National Institute of Standards and Technology evaluates, grades, and publicly lists the results for most systems. It is to the industry's competitive advantage to be extremely accurate across the broadest demographic variations possible. Systems are getting better at an accelerated pace in recent years, and leading providers are achieving extremely high accuracy levels.)

But not all cameras running some kind of facial software are "recognition" systems. There are, in fact, at least four levels of facial image software, each with different use cases, benefits, risks, and privacy implications. These levels are, in ascending orders of complexity: facial detection; characterization; verification; and identification. They are described in more detail in Figure 1.

The most basic is **facial detection**, such as what you might see through your camera – the small square overlay that moves around to frame the faces of the people in your field of vision. This technology finds what is a human face versus what is not-a-face, and marks it to allow for the camera to focus, or perhaps to count people passing a certain spot, or other completely non-personalized applications that simply have a need to know when a person is present.

The next level is called **facial characterization**. In this case, the camera is still not creating a template or other personal, individualized record, but is collecting and observing more detailed information than under facial detection. Examples include an interactive billboard at a bus stop, or a screen mounted above a product display that might be used to collect information such as gender, approximate age, and potential emotional indicators ("smiling," "sad"); this material can then be combined with other data such as how long the person looked at the screen, or where else they went within the store. Such data can give advertisers useful information about shoppers' reactions, based on type: young women responded favorably; older men glanced away quickly. Similar technology can also benefit visually disabled individuals by describing on-screen images to them: "A man and a woman seated on a towel on the beach, laughing and sharing a drink."

Neither detection nor characterization systems create or collect personally identifiable information and consequently have very low privacy risks.

The next two levels refer to how the term "facial recognition" is often used by a lay audience: verification and identification.

Verification is a one-to-one matching system, like what happens when you access your phone: The screen scans your face and tries to match you to the template saved on your phone. Either it matches, or it does not. Verification can be summed up as, "Is this person who they are claiming to be?"

In another example of verification, a building may hold a database with all the templates of the building employees created and stored ("enrolled") in it. When an employee then attempts to enter the building, the camera scans their face, and a reader checks their ID card. The ID card tells them who the person is claiming to be, and the scan is matched against that template, and that template only. If it matches, the person is allowed into the building. If it does not, they are rerouted to a receptionist or other alternate system for evaluation. This is also the type of system being tested at airports now for international boarding processes – it compares the traveler's presented identity (their face, along with a government-issued ID) against the enrolled template tied to photos of passengers on the flight manifest. In verification, the system does not

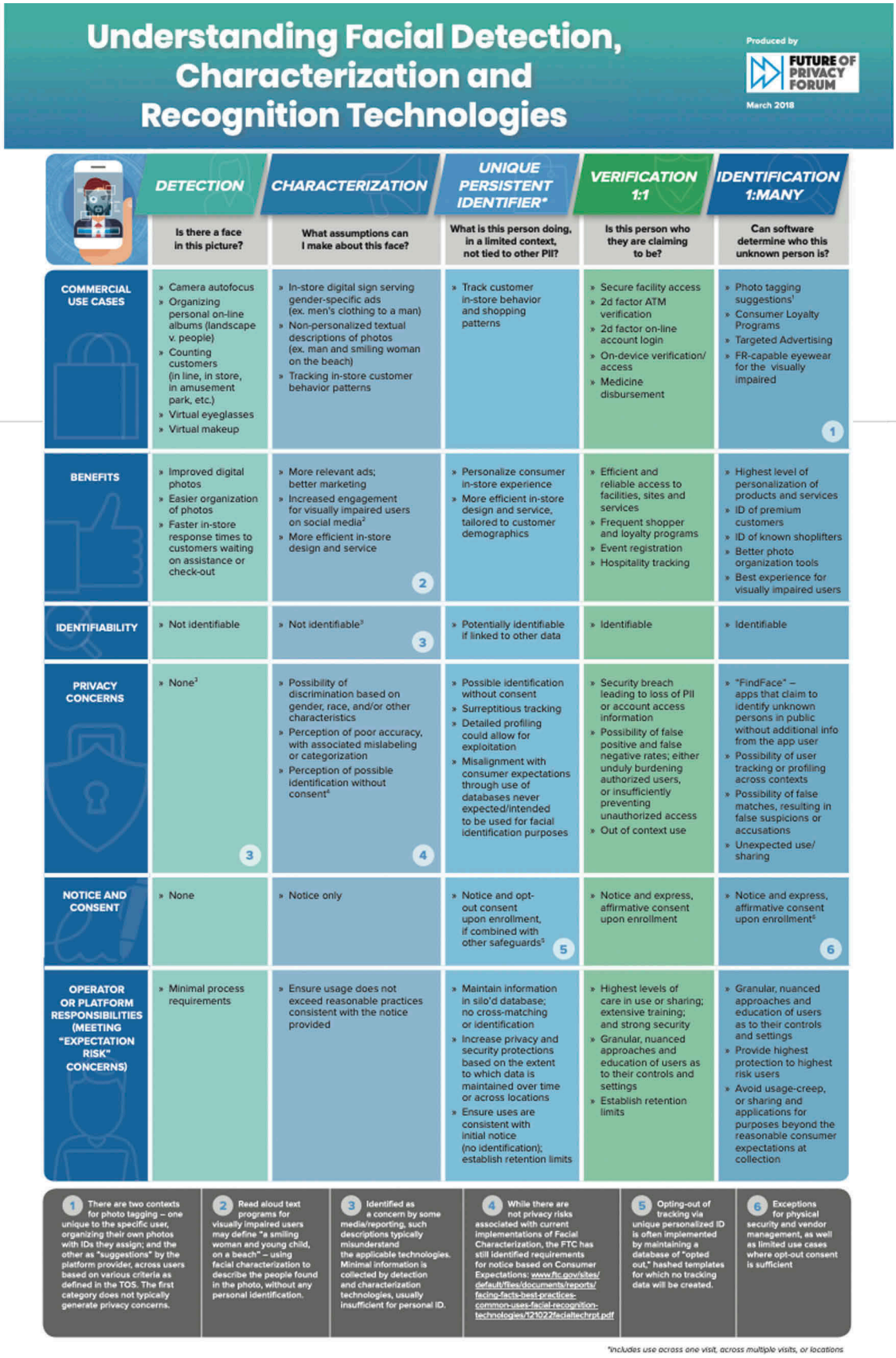

Figure 1. Understanding facial detection, characterization, and recognition technologies. Image courtesy FPF.

look at any other templates or attempt to identify the person as anyone else. The output is a simple "yes" or "no" to validate a claimed identity.

The final category of facial recognition is **identification**, also known as a one-to-many matching process. This case can be summed up as: "Can software determine who this unknown person is?" This type of system is what law enforcement uses, running a collected image against a database filled with enrolled criminals, or driver's license holders, or other pre-selected data sets. The system scans the image – possibly from a videotape at a public venue, or an image from a camera on-scene – and attempts to match the template within whatever dataset is available to it. In this case, the system is most likely to come back with multiple possible matches. It can be set to varying levels of sensitivity (based on presets that default for false positives or false negatives), and ultimately a human will review any suggested matches for a final decision on whether this person has been successfully identified.

Identification is most commonly used in the context of security – such as identifying someone shoplifting against a data set of known shoplifters or individuals present in a restricted area at a sports arena against a database of season ticket-holders. And of course, this is the type of system at use in criminal investigations. In order for law enforcement to have access to such images, a warrant, subpoena, court order, or some other legal process needs to be fulfilled, based on context, and local laws.

Once the legal standard has been met, it still takes some time to sift through the imagery. Unlike what happens on some popular television shows, a firm ID cannot be made in a matter of seconds. Instead, the reality is that the government must first obtain the videos, and then use an initial software program to run through them all and create a raw image gallery of all the people contained. These images will be lower quality, isolating images of people in hats, in shadows, or captured from odd angles. Then the templates of those images must be run against whatever dataset the police feel is applicable, such as mugshots, local Department of Motor Vehicle records, or others. Any potential match or matches will almost certainly be at low levels of certainty, and a human official will need to review them to see if any seem sufficiently reliable to follow up with further action.

The level of accuracy required in any system varies based on application and context. For an iPhone, Apple's system is verifying enrollment against a gallery of one, stored locally on the device. Apple's method, called FaceID, uses an infrared camera, a depth sensor and a dot projector to map 30,000 points on a face and create an three-dimensional scan. (The 3D technology is one of the ways to prevent access by someone simply holding up a picture of the phone's owner to gain access.) The level of detail required in the template, and the level of certainly in the match, are roughly at a false positive rate of 1-in-10 million. This is an entirely acceptable standard for phone access, but far below the standards that would be required for terrorist watchlists. FaceID on personal digital device is secure enough to use for digital payments through Apple Pay. It would not be sufficient for criminal prosecution (La 2018).

"But it's my face!"

One of the greatest areas of angst for those concerned about facial recognition systems is in the security of the data. There are at least a couple of ways to consider the security. One is "How close is it to "perfect" – can it be spoofed (access gained without the actual person's face present) or hacked (accessing the stored file of templates). High-quality facial recognition systems rate very well on such a scale, but no system is perfect, and critics have argued that even the small percentage of incorrect outputs of such a system make them unreasonably risky. Perhaps, however, a better way of ranking them is to compare them to available alternatives, such as passwords.

Biometric data, contained in a database of enrolled individuals, is almost certainly a more secure option than passwords. Passwords can be cracked fairly easily by "brute force" methods (such as running software that attempts patterned combinations of numbers and letters in alphanumeric code) if they're not strong – which most are not. And people tend to re-use them, so having someone's password from one account is likely to provide access to other accounts as well, which results in the password only being as safe as the weakest system on which it's stored. So if a server file of passwords and a server file of biometric templates are each breached, what are the risks?

Access to passwords yields immediately usable information to directly access individual accounts. And, as mentioned, each password might be useful to access other accounts as well. In contrast, a breach of a database of biometric data will yield only those binary numbers which cannot easily – if ever – be "back-engineered" into the template or the original image. This information cannot be used to access the associated account, nor is it likely to be the same system as used on any other accounts, since each platform is probably using a different vendor and the algorithms are not interoperable. Actually breaching a database of

biometric data may or may not be harder, depending on general network security, but if it were breached, there is a much higher likelihood that the data would be much harder to exploit in any systematic way. Finally, biometrics are almost always part of a 2-factor system – meaning they are only one piece of a multiple-step access process – and therefore just having the biometric isn't enough to gain access.

"I'd like a little privacy, please!"

A core privacy principle is known as "Data Quality and Integrity" – the requirement that individual data and data sets are "accurate, relevant, timely, and complete" (Homeland Security 2008). The challenge for current facial recognition systems is to achieve sufficient accuracy across demographic variations such as race, ethnicity, and gender, although they are improving all the time. Nevertheless, the ways in which facial recognition systems have fallen short, sometimes in rather spectacular fashion, have led to significant reservations about their reliability from the standpoints of privacy and civil liberties.

Privacy concerns cross into both the governmental and the commercial spheres. Government misidentification can lead to innocent people on watch lists, with an increased risk of bad results for minorities and other at-risk populations. Likewise, commercial companies may use facial recognition to unfairly or illegally discriminate. For example, a retail chain might create its own data set of "known" offenders without any clear standards for who is targeted, and no practice by which they are notified or can appeal their inclusion. What's more, retail chains may share such lists with other companies, potentially resulting in individuals being broadly denied service without any due process.

The ethical considerations of where and how to use facial recognition systems even exceed the boundaries of traditional privacy considerations. By using machine learning programs as the underlying foundation, these systems are built on existing data that reflect human biases, and automate them. Having "humans in the loop" will not correct this, unless those humans include trained programmers who can test and audit systems for systemic bias and recommend corrective measures. The social impacts of this are only beginning to be understood.

Having said all this, it should be noted that there are certainly many beneficial use cases for facial recognition systems. For individual users, there are many convenient services, some as simple as tagging people to help with sorting and organizing photos, all the way to "smart" glasses for visually impaired people, who use them to identify the people around them and navigate with increased independence. Hotels and conferences are working to create a seamless experience based on facial recognition systems for their members; registrants who have opted-in to such a service can theoretically travel from taxi, to lobby, to room, or check into a conference, with no delays, lines, or frictions along their path.

The law enforcement and national security benefits are likewise real. Facial recognition systems have already been key in identifying suspected terrorists or criminals. They can do so generally with decreased costs, increased efficiencies, and consistently greater accuracy than humans.

Some uses may not clearly be either good or bad. Profiling shoppers, tracking online preferences, and personalizing recommendations or experiences are features some consumers value, but others may not. Tying these options closely to the appropriate consent level is important.

Less beneficial uses, of course, abound. Many concerns involve government applications. Academics have done in-depth reviews of the impact of surveillance technology on minorities, religious groups, and other traditionally targeted or vulnerable populations (Georgetown Law 2017). They have likewise criticized the decision to implement facial recognition at airports (Nixon 2017) and in police operations.

Consider public demonstrations, especially with the increased occurrence of large-scale marches in recent years. Those who march for or against a cause understand that they're in public. They realize that people will see them and possibly recognize them, and that other attendees – including those they don't know, or don't see – may take their photo, and may post it online in places they'll never know about. Nevertheless, what they probably do not expect is that the government will have cameras or coverage that enable it to later collect and identify the images of many or most people present, and keep a file designating those individuals with some kind of code or tag for future reference.

In some countries, there are potentially few legal protections from such omnipresent surveillance of the populations. China, notably, seems eager to use facial recognition for everything from identifying jaywalkers (Zhao 2018) to dispensing toilet paper (Associated Press 2017). A government's ability to track its citizens has historically been shown to enable discrimination against targeted groups or individuals. When this is paired with cultures that espouse and protect fewer civil liberties to start with, the outcomes seem ominous.

But commercial entities have shown that their privacy practices may not be much better, collecting and exploiting the personal data of individuals, groups, and entire countries (*The Guardian 2018*). And the line between commercial and governmental access and use is frequently blurred and likely to become more so. The expectation that facial recognition systems will simply make these risks higher seems well-founded. While there are some examples of putting legal frameworks in place to push back against privacy challenges (EU GDPR 2018), these efforts number only a few so far, and they affect limited areas – such as the European Union or individual states in the United States.

The use of facial recognition systems is not solely responsible for the world's ethical and social privacy problems, of course. Instead, they are being implemented into a world already facing the problems of biased human systems – and even at their worst, facial tracking systems are still just one more tool in the tech box for governments who are already able to identify, target, and track individuals beyond anything imaginable in the past.

The same battles that have been fought in the United States for decades about national identification cards are raging over facial recognition systems. The problem of whether private citizens should be required to have government-issued documentation verifying their personal identities in order to access goods and services, seek employment, travel, or obtain government benefits long predates the current discussions related to digital identity systems and the use of facial recognition systems.

Whether past or present, these challenges are all based on the question of how to balance government efficiencies and national security against protections for individual freedoms and liberty. Running through this conversation is the underlying conception of privacy. Is it a fundamental right? What does it mean? Who gets to decide which conveniences are worth the tradeoffs they require? Are the protections for personal data offered by policy and law sufficient, or should technical and security protections always be required? Are some systems simply too high of a risk to implement, regardless of perceived benefits?

The past may offer a clue as to what to expect. When they were first implemented, passport photos were shockingly contested and denounced (Holmes 2015). They were not commonly required until after World War One. In the short 100 years since, technology has only accelerated the practice of government identification and tracking of people's movements, until today many societies face the realistic possibility of almost ubiquitous surveillance. How societies and cultures face these challenges will determine whether Orwell was entirely prescient, or we can choose a different path, embracing the continued ideal of personal liberty and freedom.

Acknowledgments

The author would like to thank the Future of Privacy Forum for its support.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Notes on contributor

Brenda Leong is senior counsel and director of strategy at the Washington, DC-based thinktank Future of Privacy Forum. She addresses the ethics and privacy issues around artificial intelligence, as well as biometrics, particularly facial recognition. She wrote "A Privacy Expert's Guide To Artificial Intelligence and Machine Learning" last fall, and co-authored "Beyond Explainability, A Practical Guide to Managing Risk in Machine Learning Models."

References

Associated Press. 2017. "China Introduce Facial Recognition Technolgoy to Dispense Toilet Paper." https://www.cbc.ca/news/technology/china-facial-recognition-toilet-paper-1.4052888

Bogle, A. 2015. "You Can Only Read This High-Tech Book if It Likes Your Facial Expression." February 2. https://slate.com/technology/2015/02/this-book-only-opens-if-its-facial-recognition-software-decides-you-are-nonjudgmental.html

Cullum, J. 2018. "Facial Recognition at Border Nets More Impostors than at Airports." *Homeland Security*, November 20. https://www.hstoday.us/federal-pages/facial-recognition-at-border-nets-more-impostors-than-at-airports/

EU GDPR. 2018. "EU General Data Protection Regulation." https://eugdpr.org

Georgetown Law. 2017. "The Color of Surveillance." https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2017/

The Guardian. 2018. "The Cambridge Analytica Files." https://www.theguardian.com/news/series/cambridge-analytica-files

Hartzog, W., and E. Selinger. 2018. "Facial Recognition Is the Perfect Tool for Oppression." *Medium*, August 2. https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

Holmes, T. T. 2015. "Passports Were Once Considered Offensive. Perhaps They Still Are." Atlas Obscura, December 9. https://

www.atlasobscura.com/articles/passports-were-once-considered-offensive-perhaps-they-still-are

Homeland Security. 2008. "Privacy Policy Guidance Memorandum." December 29. https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf

La, L. 2018. "10 Best Phones with Facial Recognition: IPhone X, Note 9, LG G7, and More." August 22. https://www.cnet.com/news/10-best-phones-with-facial-recognition-iphone-x-note-9-galaxy-s9-lg-g7/

Nixon, R. 2017. "Facial Scans at US Airports Violate Americans' Privacy, Report Says." *New York Times*, December 2017. https://www.nytimes.com/2017/12/21/us/politics/facial-scans-airports-security-privacy.html

Zhao, C. 2018. "Jaywalking in China: Facial Recognition Surveillance Will Soon Fine Citizens via Text Message." Newsweek, March 27. https://www.newsweek.com/jaywalking-china-facial-recognition-surveillance-will-soon-fine-citizens-text-861401