The Two Faces of Facial Recognition Technology (February 2021)

Neil A. Chilson and Taylor D. Barkley[1]

***Abstract*—The use of facial recognition technology, including facial detection, facial verification, and facial identification, is increasingly widespread in commercial and government applications. Some of these uses raise significant policy concerns, most prominently issues of privacy and algorithmic bias. To address these issues, facial recognition technology needs governance. There are two options: hard law and soft law. Hard law governance is made by courts and legislatures. It is relatively static and inflexible and often struggles to adapt to fast changing technologies and new use cases. Soft law is a broad category of governance approaches that set forth expectations but are not directly enforceable by government. Soft law is more agile and adaptive and can evolve alongside a technology, although those same characteristics come with downsides. We argue in this paper that soft law and hard law both have key roles when it comes to governing facial recognition technology. Soft law governance will best enable benefits and address risks of facial recognition in commercial uses. However, government use of facial recognition will in many cases need hard law constraints. In fact, unless such government uses are subject to targeted and clear hard law constraints, soft law approaches to commercial facial recognition will struggle to gain legitimacy.**

***Index Terms*— algorithmic bias, facial identification, facial recognition, hard law, image recognition, , law enforcement, policy, privacy, soft law, surveillance**

I. Introduction

THE face is the most public part of human bodies. We usually recognize or identify someone by their face. Our brains are wired to quickly spot faces – even in arrangements of inanimate objects – and to instantly identify the emotions they convey.

Thanks to the increased ubiquity of digital cameras and advances in computer vision algorithms, computers can now identify, recognize, and interpret images of faces. This facial recognition technology (FRT) is a powerful tool that has already proven its utility in commercial uses. And it has provoked concern, especially when used by governments, and especially when used by law enforcement.

When considering how to govern new technologies such as FRT, there are two categories of alternatives. The traditional approach is "hard" law – legislation enacted and enforced by government. The other broad category is "soft law", which Arizona State University law professor Gary Marchant describes as frameworks that "set forth substantive expectations but are not directly enforceable by government, and include approaches such as professional guidelines, private standards, codes of conduct, and best practices." [1]

Soft law has certain characteristics that separate it from hard law. It is more agile, flexible, and easier to adopt because it avoids the procedural and legal requirements of hard law. Questions of legal authority, geographic jurisdiction, and conflict of mandatory laws are not issues for soft law. And it generally encourages collaborations between stakeholders rather than adversarial proceedings that typify hard law.

These characteristics make soft law a good candidate for governance in certain circumstances. Where an area is rapidly evolving; where the benefits, risks, and trajectories of change are inherently uncertain; and where the technology has an extremely wide scope of applications across many industries – in these circumstances the ability of soft law to evolve quickly, to try many different overlapping solutions, and to span jurisdictions make it far preferable to hard law, which is either impossible to adopt or rapidly outdated.

Of course, as Marchant and Tournas note, the very strengths of soft law in some circumstances are disadvantages in others. Soft law avoids procedural requirements at the cost of transparency and inclusiveness. It is frequently nonbinding, which can mean uncertainty and a lack of redress for those affected by the governed tech. And it can lack effectiveness and credibility with the public. In situations where there is a narrower application of a technology, where the benefits and risks are easier to assess, where questions of legal authority and geographic jurisdiction are less important, and where the outcomes of potential abuse are known to be serious and likely, soft law may not be the right tool.

We argue in this paper that soft law and hard law both have key roles when it comes to governing facial recognition technology. Soft law governance will best enable benefits and address risks of FRT in commercial uses. However, government use of FRT will in many cases need hard law constraints. In fact, unless government FRT uses are subject to targeted and clear hard law constraints, soft law approaches to commercial FRT will struggle to gain legitimacy.

Submitted September 1, 2020. This work was supported by the authors' employer as part of their normal duties.

N.A. Chilson is with the Charles Koch Institute, Arlington, VA 22201 USA. Previously he was the Chief Technologist at the Federal Trade Commission (e-mail: neil.chilson@cki.org).

T.D. Barkley is also with the Charles Koch Institute, Arlington, VA 22201 USA (e-mail: taylor.barkley@cki.org).

II. What is Facial Recognition Technology?

Facial recognition technology (FRT) is a subset of computer vision that focuses on processing images of human faces. FRT itself can be subdivided into three related categories of analysis. Facial detection is the ability of software to recognize that an image contains a picture of a human face, and usually include the ability to demarcate where within the image the face or faces are. Sometimes facial detection includes identifying facial features as well, such as eyes, noses, and mouths. They also may build wireframe mesh models of the three-dimensional representations of a face from the input images. Facial detections algorithms may be trained on large datasets of faces, but when running they do not require such databases. They can also operate in real time, even on mobile phones. For example, Snapchat or Instagram filters that manipulate video – giving a photograph sunglasses or rabbit ears – use facial detection algorithms.

Facial verification builds on facial detection to determine whether two different images contain a picture of the same person. Facial verification algorithms seek to do this even for photos with different formats, angles, and lighting. A facial verification algorithm may rely for its input on a facial detection algorithm that identifies and extracts features from faces in two different photos; the facial verification algorithm then seeks to establish whether the faces are the same. Like facial detection, facial recognition algorithms do not need large databases of photographs to operate, although the algorithms may have been trained on such large databases.

Finally, there is facial identification. Facial identification is the process of, given an image of a face, identifying which face in a large collection of pictures of other people that best matches the given image. In concept, this is as simple as running a facial verification algorithm against a large library of recorded faces. Unlike facial detection and facial verification, facial identification algorithms require a large database of photographs – or a large database of facial models derived from such a database of photographs. Sometimes this database of photographs is tied to the identities of actual humans. This is what many people mean when they colloquially say, "facial recognition."

Each of these subsets of facial recognition technologies require different amounts and kinds of data about individuals and enable different uses (or abuses). Thus, the specific policy challenges for each category are different.

III. FRT Offers Significant Benefits

FRT is already in use and the potential future uses of the technology offer attractive benefits. While most commercial applications only emerged in the past five years, facial recognition technology is already a widely deployed technology because it can be useful, convenient, and fun. For example, Apple's Face ID uses facial verification to enable iPhone users to easily unlock their phones. We've already mentioned some of the entertaining and impressive photo and video filters built by SnapChat and Facebook to overlay or modify video of faces. Google Photos uses FRT to group photos with one individual together, making it easy to, for example, search for all the pictures of you and your Aunt Sally together. Other widely deployed uses include border entry security, suspect searches, and retail store security.

Facial detection software is commonly and widely used in app photo filters on popular apps like Facebook, Snapchat, Instagram, iMessage, and many others. Deploying the same technologies that can identify a face for security reasons, the technology in these instances is able to overlay cosmetic changes for users merely by recognizing a face from other parts of the body or the environment within the view of the smartphone's sensors. Mastercard and Apple allow individuals to use their facial image to pay for products online and in-person with a credit card. Covergirl, a cosmetics company, uses FRT to help customers decide on types of makeup that match well with their skin tones. Major retailers, including Lowes, Walmart, Target, and Saks Fifth Avenue, use FRT to identify instances of theft in their stores and determine whether consumers enjoy their shopping experience. These applications provide consumers with innovative new shopping experiences and allow businesses to better protect themselves from fraud and theft.

Uses of FRT by public and private actors also helps to increase individuals' safety. In the government setting, law-enforcement authorities have used FRT to track missing individuals and identify wanted criminals. The NYPD credits FRT for helping officers apprehend an accused rapist within 24 hours of his first attack. These instances demonstrate that law enforcement use of FRT is not without positive potential. Taylor Swift's security team deployed FRT at a concert in 2018 to determine whether any of her potential stalkers entered the crowd.

In addition to physically deployed FRT systems, FRT has helped streamline smartphone security. With the introduction of the iPhone X in 2017, its Face ID capability, and subsequent deployment of FRT by other smartphone manufacturers, FRT has since replaced fingerprint scanners as the default security mode for smartphones. It has proven effective and seamless. FRT on these devices can integrate with apps to enable payments, password protectors, health data and other apps that grant access to sensitive services or personally identifiable information (PII). It has streamlined commerce on the smartphone. For example, an item selected in the Safari browser can be purchased with a credit card stored in Apple Wallet which is protected with Face ID.

Similarly, FRT has also been successfully deployed on major photo and image services like Facebook, Google, and Amazon Photos. Google's Nest cameras utilize FRT so consumers can recognize "familiar faces" as people approach their homes. Amazon has not yet integrated FRT into its Ring camera system although it is an option they are considering.

In the near future, FRT deployment could mean more efficient security, inventory management, and payments processes, enabling stores to shift their focus to customer experience and reduce their real estate footprint. Collecting information on customers' purchasing habits and integrating that data with FRT could allow businesses to create highly

specialized services for consumers. Stores could use FRT to identify individuals' shopping habits and provide them with customized discounts and merchandise offerings when they enter the store. FRT could be used to monitor wait times and mood in check-out or customer service lines, enabling real-time re-allocation of employees to assist customers where needed. And businesses could utilize FRT to not only prevent physical shoplifting, but to also prevent individuals from using stolen credit cards by authenticating their identity. These are all features regularly associated with high-end retail stores but as FRT drops in price, these could become features of all in-person retail.

IV. FRT Raises Policy Concerns

Observers of facial recognition technology have raised several concerns. The most prominent categories of concerns involve privacy and algorithmic bias. (Although there are other concerns, such as the ability to fool such systems into thinking one person is another.)

A. Privacy

People concerned with the privacy implications of FRT worry that uses of FRT will expose accurate personal data to unknown or undesired parties. For example, using facial recognition on a collection of social media posts could identify a group of people that frequently hang out together. Recognizing the same face on multiple cameras across a city downtown could be used to virtually follow an individual, showing where they went and what path they took. Sentiment analysis (using FRT to judge the emotional response of an individual) could reveal information about someone's shopping preferences in a grocery store. Other critics of the technology argue that the government's use of FRT will discourage individuals from participating in peaceful protests for fear of state surveillance.

As mentioned in the introduction, your face, at least when in public areas or on other's property, isn't exactly private. In theory, FRT-related privacy concerns could be replicated by a human observer. Someone could review social media posts to identify someone's group of friends. An investigator could tail someone across town or look at security camera footage to do the same. A waiter or clerk might recognize a customer, identify their mood, and accommodate them accordingly. The difference is that FRT potentially allows what would be very labor-intensive work to be done rapidly and at relatively low cost – and therefore more frequently.

B. Bias

Many are worried that FRT can and is biasing decision-making and creating discriminatory effects. Facial identification algorithms can produce both false negatives (failing to find a match to an individual in the database even though they are included in the database) and false positives (finding an incorrect individual as a match). Research has demonstrated that some FRT systems are less accurate at identifying black faces. Other recent studies of government FRT databases have shown troubling problems when it comes to misidentifying Asians, African Americans, Native Americans, and Pacific Islanders. In Detroit, a mistaken identification from FRT led police to arrest an innocent man. Indeed, because of how many of these algorithms are trained, they may be less accurate when applied to subgroups of the population that are not well represented in the training data. While other computational applications that rely on large data sets raise similar concerns about bias, the FRT concerns are particularly poignant because they are evaluating photos, and, in a very literal way, judging people by their skin color.

Bias is but one concerning form of inaccuracy. For example, there is evidence that as photographic databases grow larger, the number of false positives can rise because there are many people who look like others.

V. Consequences of Hard Law Approaches to Commercial FRT

Motivated by these concerns, a handful of states have enacted laws to regulate commercial uses of facial recognition technology. While the evidence is not conclusive, subsequent developments suggest that such laws have had unintended consequences for consumers and for innovation.

Three states – Illinois, Washington, and Texas – have passed "Biometric Information Privacy Acts," (BIPAs) which directly regulate the conditions under which facial recognition (and other collection of biometric information) may occur. At least eight other states have considered similar legislation. At the Federal level, several proposals have been floated but none have advanced.

The Illinois law was the first BIPA law passed (in 2008) and therefore is a good case study for the potential effect of BIPA laws. The Illinois law requires that companies describe how they will use biometric information, including "scans of face geometry," and obtain the customers' express written consent for any collection of BI. The law also imposes retention limits, data destruction requirements, and data security requirements. Thus far, the Illinois law is the only BIPA to allow a private right of action, with up to $5,000 per violation in statutory damages plus attorneys' fees and costs. And, interestingly, the Illinois law expressly exempts state and local governments from its requirements.

What have been the effects of the law? We're only beginning to see the effects on FRT because the technology has only in the past several years entered broad use. We can identify, however, some of the technologies that may be impacted by the law by looking at some of the early cases brought and the reactions by some companies.

The Illinois BIPA law has caused some companies to withdraw products or services in that state. For example, Sony does not sell its robot dog companion, Aibo, in Illinois. Google disables the facial-recognition features of its in-home Nest security cameras in Illinois. In Illinois and Texas (another state with a BIPA), Google blocks one feature of its "Arts and Culture" app that uses selfies to find users' doppelganger in a large database of paintings by recognized artists.

The most dramatic effect of Illinois' law however, has been in class action litigation. For about 10 years there was neither

state AG enforcement nor much private class action use of the law in raw numbers – although lawsuits had been brought against several of the major tech companies, United Airlines, the Kimpton hotel chain, and a grocery store chain. But on January 25, 2019, the Illinois Supreme Court held in Rosenbach v. Six Flags (Ill. 2019) that plaintiffs do not have to demonstrate actual harm to establish that they are "aggrieved" under the Act. That opened the floodgates of class action lawsuits. Between the date Rosenbach was decided and the end of June 2019, 151 new class actions were filed under the BIPA – approximately one per day. Many of these lawsuits target employers who use biometric fingerprinting for employees punching in and out – a technology that reduces fraud and which poses little or no risk to consumers more generally. Rosenbach also triggered new or revived cases against Google and Shutterfly for use of FRT.

In short, while Illinois' BIPA and the associated litigation imposes clear costs on businesses and depriving Illinois residents of useful services, there is no evidence that the law is improving the lives of Illinois residents. Indeed, BIPA litigation is usually focused on technical violations of the law with no alleged harms.

VI. Commercial FRT Should Primarily Rely on Soft Law Approaches

For commercial uses, soft law alternatives have provided and promise to offer a better path forward, even for concerns about privacy and bias. Aside from the Fourth Amendment, antidiscrimination laws (discussed below) and the few state BIPA laws (mentioned above), soft law governs most FRT deployment.

Soft law provides flexibility for use cases over time. FRT is rapidly evolving and changing as it is developed, refined, and deployed by individuals all over the world. The FRT available in the next ten years – and the uses to which it is put – will differ significantly from the FRT available today. When hard law fails to anticipate technological developments and new use cases, it can hamper beneficial applications while completely missing harmful outcomes. Soft law allows for positive evolution because it does not try to rigidly anticipate all uses and outcomes; instead, it evolves alongside the technology.

Hard law also often focuses on preventing worse-case scenarios. As humans, we are typically better at imagining future harmful applications of something new than we are at grasping all the many ways different people might apply a technology to benefit their lives. But as Adam Thierer, a Senior Research Fellow at the Mercatus Center at George Mason University, has said, "We should avoid basing policy interventions on hypothetical worst-case scenarios, or else best-case scenarios will never come about." Soft law reacts to real world harms of FRT without trying to anticipate them all.

A. Types of Soft Law for FRT Governance

Soft law has many variants. Rather than list the full menu of soft law options and how they each apply to FRT, we focus on the approaches already governing commercial FRT today include social norms and behaviors, moral standards, labeling, education, private industry voluntary standards, and public pressure.

1) Social norms

Social norms are the default governing structure for most new technologies. Social norms and public accountability are the dominant governance structures for commercial FRT now. As companies and individuals deploy this technology, they rely on cultural frameworks of acceptability. Technology companies are integrating FRT when they work well and have a reasonable chance of being met with a positive consumer response. When errors do occur or consumers negatively respond, the technology is pulled or amended.

For example, Apple added FRT to the iPhone X, enabling users to unlock the device, verify payments, and use various entertainment features. Apple announced the FRT capability well ahead of launch with an emphasis on usability and privacy. Today, the system works well for most people and has generally been accepted. Compare the deployment and subsequent removal of FRT in 200 urban Rite Aid stores. Rite Aid used a system of cameras with FRT to match customers against a photo database of criminal suspects. When a match was made, the security agent in the store would receive a notification. Rite Aid did not publicize the deployment, appeared to have thought little about the privacy downsides, and failed to make the case for how this benefited consumers when the potential harm to consumers was considerable. When reporters uncovered the system, Rite-Aid disabled it to deal with the bad press and public outcry.

The downsides of social norm soft law is the delayed timeframe and the lack of clear leadership. When concerns run high and calls for "something to be done," a wait-and-see-as-culture-adapts approach is neither a satisfying way of redressing wrongs nor politically satisfying for politicians who demand a fix. Responsibility is diffused as well. No one organization, institution, or individual is responsible. We all are. It is an emergent order of governance.

2) Self-Censorship

Given the name, people might think that soft law is timid or lacks real world effect. But soft law responses can be quite severe. Large companies have generally shown caution in deploying FRT, publicly declaring their intentions and working to educate consumers on how data is collected and used. Some firms delay deploying this technology until it reaches an acceptable standard of accuracy. Indeed, some private companies are choosing not to deploy FRT at all. Such behavior, where firms make decisions on their own, should be encouraged. Soft law allows this diversity of responses.

3) Education

Educational efforts support the adoption of FRT. When Apple incorporated FRT in their iPhone X in 2017, consistent with its posture as a privacy-conscious brand, the company addressed privacy concerns by explaining to users that the identification data is stored locally on the phone and not shared with Apple. The feature is now widely used and little commented on.

4) Labeling

Labeling of FRT deployment offers another potential soft law solution. Closed circuit television (CCTV) monitoring

systems offer a relevant example for how FRT could be deployed in physical commercial settings. In retail settings, CCTV systems are often labeled to deter crime but also serve the purpose of notifying consumers that they are under surveillance. Labeling retail FRT uses would serve this dual purpose as well. Consumer products like Nest, Arlo, and others have democratized video monitoring systems as well as labeling practices. These products and local promotional programs include stickers that can be affixed to windows or walls notifying or warning individuals of the camera system. Such notifications are suggested and not required. Governments mandates could potentially require labeling by firms, services, or products that use FRT, but given that there are often other advantages to labeling beyond consumer disclosure, a mandate is probably unnecessary. And for consumer uses, government mandates would likely be unconstitutional and certainly unenforceable at scale. Soft law, norms-based incentives like labeling may be the most viable approach.

5) Voluntary Standards

Private associations, companies, and government entities can co-develop voluntary standards, best-practices, and guidelines to govern the deployment of commercial FRT. We've already seen examples. From 2013 to 2016 the National Telecommunications and Information Administration (NTIA), a government entity, convened a cross section of government, industry, academic, and consumer groups to develop a "Privacy Best Practice Recommendations" document for the use of commercial FRT. Private associations like the IEEE SA and the Security Industry Association (SIA) have developed standards. So have individual companies like Google and Microsoft. All of these organizations made their standards available to the public. Finally, coalitions, like the Partnership on AI which includes 96 organizations, formed to develop guidelines on the use of FRT. .

6) Private Certification

Private third-party validators or certification companies could be one part of a nascent set of solutions to mitigate bias risks. For example, private electronics manufacturers contract with third party product certification companies like UL to stress test consumer devices like plug-in air fresheners and toasters. Once the devices pass these stress tests, UL provides its stamp of approval to the product. Although testing the products is neither required by law nor funded by governments, it is required for some government benefits and has become a highly valued and respected validator of consumer products. A UL-style system could be one way of validating FRT systems before deployment, especially during the first wave of the technology. Indeed, a third-party validator may be the only way a company could re-build consumer trust in its FRT if something goes wrong.

7) Public Pressure Campaigns

Public pressure and backlash against commercial FRT deployment and public scrutiny are effective means of soft law governance. The Rite-Aid example described earlier demonstrates how public scrutiny and pressure can motivate companies to use FRT responsibly or eliminate its use all together. As another example, kiosks ostensibly for fan photos at a Taylor Swift concert in fact used FRT to identify known stalkers. A Rolling Stone article exposed the use of the technology, forcing the contractor that worked with Swift's security detail to publish a series of blog posts explaining how the technology was used, and seeking to address privacy, data security, and other concerns.

B. Addressing Specific FRT Concerns

Soft law approaches such as those discussed above can address many of the concerns of commercial FRT, including the most prominent concerns about privacy and algorithmic bias.

1) Addressing Privacy

People are concerned about the effect of FRT on privacy. There are some lessons from early reactions to the personal camera in the 19th century. The law review article frequently cited as kicking off the privacy rights discussion argued that "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of privacy and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" Yet social norms addressed most of the concerns presented by the camera. For instance, today in the United States, taking a close-up photo of a stranger without their permission is viewed as a rude and invasive gesture. Therefore, it rarely happens for non-celebrities. Similar concerns were raised with camera phones in sensitive locations like gym locker rooms. But social norms and rules by private establishments quickly addressed such concerns.

There is evidence that social norms and other soft law around FRT are evolving. As individuals and interest groups voice concerns about the safety, security, and privacy implications of FRT, businesses are creating and using FRT develop standards and best practices to address these concerns. The Security Industry Association notes that many biometric-technology companies develop best practice systems and provide training so that users avoid abusing FRT technologies. Industries that anticipate using FRT in their services and products, including the American Association of Motor Vehicle Administrators, developed FRT standards to protect the privacy and security of the information they collect and use. People with heightened concerns about FRT can also utilize emerging tools to hide from the technology. Several reports and studies show that the use of face masks, necessitated by the COVID-19 pandemic, can stymie the ability of FRT to identify individuals. Some clothing designers even incorporate patterns that make it difficult for FRT to detect and identify individuals' faces, allowing people to move about in public without fear of FRT surveillance.

2) Addressing Algorithmic Bias

Soft law can mitigate harms while maintaining an innovative framework, even for critical concerns like racial and gender bias. Completely unbiased and accurate systems are not achievable because FRT is dealing with data sets informed by human beings who themselves are biased. However, unlike human beings, FRT systems can be empirically tested for many kinds of bias and thus can be improved over time. Furthermore, in commercial contexts bias is usually an unprofitable trait, and companies typically have financial incentives to ensure that

their algorithms accurately characterized individuals. But firms will undoubtedly make mistakes. Soft law can help mitigate errors inherent in these systems prior to deployment and can help correct errors after deployment.

3) Existing Hard Law

There is a role for hard law in governance of commercial FRT regarding bias and privacy. In fact, existing hard law already prohibits discrimination against protected classes of people. And existing federal and state privacy laws also apply here. These technology-neutral laws can and should be enforced, regardless of the technology involved.

VII. Many Government Uses of FRT Are or Should Be Subject to Hard Law

Consumers can be harmed by commercial misuse of technology. But only governments possess the power to fine and imprison under the color of law, so sturdy guardrails on government are required to protect civil liberties. Existing government collection and use of information about individuals is already legally, even constitutionally, restricted. How these restrictions play out with FRT technology remains to be seen. But whether the hard law comes through courts or through legislation, there are good reasons to place definite restrictions on government use of FRT.

All current government uses of FRT technology are subject to hard law restrictions such as the Fourth Amendment and other legal constraints. But courts are still figuring out what that means for new technologies, including FRT. The Fourth Amendment prohibits government officials from conducting "unreasonable searches and seizures" absent a valid warrant. Courts have generally decided which searches are unreasonable by evaluating whether the defendant had a reasonable expectation of privacy, and courts have generally held that people do not have a reasonable expectation of privacy from normal observation when in public spaces. For this reason, law enforcement can, for example, generally record video of individuals in public spaces without needing a warrant.

The Supreme Court has recently indicated that technology that makes it much more efficient to gather bulk information about an individual can, absent a warrant, violate the Fourth Amendment – even if gathering that information manually is constitutionally valid. For example, in United States v. Jones, the Court found that attaching a GPS tracking device to a suspect's car was a Fourth Amendment search, even though police officers do not need a warrant to tail cars on public roads. And in Carpenter v. United States, the Court held that the government needs a valid warrant to obtain cell phone location history that provides a "detailed, encyclopedic, and effortlessly compiled" record of where an individual has been.

FRT seems likely to enable similarly efficient surveillance methods, but constraints on government use are unclear. For example, FRT applied to publicly recorded security camera footage could be used to trace an individual's path across a city, similar to Jones. But whereas the law enforcement officials in Jones collected only information about his car's movements, this FRT technique could be used for every single individual captured on the footage. Constitutional law may impose such restrictions, but it may also be appropriate to examine legislation in this area, as some already have.

Even beyond surveillance, there are many other government uses of FRT that raise concerns. How can identifications of individuals using FRT be used as evidence at trial? What needs to be disclosed to defending counsel? How long should validly collected facial data be retained?

These important governance questions need solutions, and while we are strong believers in the soft law approach for most commercial uses, we believe there is a strong need for hard law constraints on government uses, for three reasons.

First, soft law cannot adequately constrain government uses. Soft law is, by definition, not mandatory or binding. Participants are persuaded to participate, not coerced – although participants can be subject to government enforcement. (For example, if a company falsely claims that it follows an industry code of conduct, the Federal Trade Commission could sue the company for deception.) As such, soft law cannot constrain government uses. Without hard law restrictions, purely soft law restrictions on government uses of FRT would lack redress. Federal agencies are not subject to general consumer protection law such as that enforced by the FTC. Nor are they particularly susceptible to other forces, such as market constraints or budgetary constraints, that incentivize participation in soft law mechanisms.

Second, the downsides of hard law are less pronounced when applied to government use of FRT. Hard law regulation of technology is often difficult because one cannot anticipate all future use cases of a technology. But in countries with limited government – where the scope and purpose of government action is constitutionally or otherwise constrained – the FRT use cases for government are likewise limited to law enforcement, national security, and other legitimate exercises of government authority. As a result, policy makers can more easily and accurately identify how government will use a technology like FRT and can likewise more accurately identify the consequences of misuse. Similarly, because the scope of government authority changes very slowly, if at all, hard law governing government uses will stay current longer.

Third, hard law restrictions on government uses are necessary to make soft law credible for commercial uses. One of the greatest concerns about commercial uses of FRT is how government might apply such capabilities. Those concerns will be unaddressed if no hard law constrains government use of FRT, or if government can evade those constraints by outsourcing to companies. Government abuses of commercially-available technologies would undermine the credibility of any soft law governance of that sector. Thus, credible soft law frameworks for FRT will require hard law restrictions on how government can obtain and use commercial FRT.

Hard law restrictions on law enforcement use would also provide clearer guidance to commercial entities deploying FRT for purposes of safety and security. For instance, what if an FRT system flags a customer as a known shop lifter and prompts the store manager on site to call the police? Clarity about how police can or cannot use that information in prosecution of the

customer will help companies make better-calibrated choices about when to involve law enforcement.

A. *Examples of Hard Law Approaches*

State and local legislatures provide some templates for how hard law approaches to law enforcement could protect civil liberties and help commercial FRT maintain credibility work.

Some cities have issued flat bans on law enforcement uses of FRT. According to the Lawfare blog, "Eight cities in California and Massachusetts have banned government use of facial recognition altogether, while Portland, Oregon, is considering going further by banning both public- and private-sector use of the technology. Three states have banned the deployment of facial recognition in police body cameras." This list seems likely to grow. Flat bans, however, are a fragile governance approach. They prohibit even compelling use-cases. If a tragically missed opportunity triggers the withdrawal of such a ban, the remaining governance structure will be underdeveloped and untested.

The Facial Recognition Technology Warrant Act, introduced by Senators Coons (D-Del.) and Lee (R-UT) provides a better example of a hard law approach to government use. That bill would require federal law enforcement to get a probable cause warrant in order to use FRT to track an individual for more than 72 hours. The warrant requirement does not apply to a single identification of an individual, if no there is no subsequent attempt to track the individual. This type of approach allows the deployment of the technology in the law enforcement toolbox, but under constraints that are consistent with past practice.

VIII. Conclusion

Commercial uses of FRT should be subject to a soft law governance approach, but government uses need hard law constraints. Unfortunately, most FRT legislation has taken the exact opposite approach, applying inflexible hard law restrictions on commercial uses while entirely exempting government applications. This is perversely driving FRT business models and investment to overemphasize government use cases, where the risks of harm from flawed technology are much higher. To ensure that the beneficial commercial uses of FRT can continue to develop under a soft law framework, we need to protect civil liberties – by using hard law to constrain government FRT uses.

Acknowledgment

We are extremely grateful for Parker Kobayashi's research assistance on this paper.

References

[1] John Villasenor, "Soft law as complement to AI regulation," Jul. 31, 2020, Brookings Inst., [Online]. Available: https://www.brookings.edu/research/soft-law-as-a-complement-to-ai-regulation/.

[2] G. Marchant and L. Tournas, "Indirect enforcement of 'soft law' governance of artificial intelligence."

[3] James Le, "Snapchat's filters: How computer vision recognizes your face" Jan. 28, 2018, [Online]. Available: https://medium.com/cracking-the-data-science-interview/snapchats-filters-how-computer-vision-recognizes-your-face-9907d6904b91.

[4] E. Klarreich, "Hello my name is…" *Comm. of the ACM,* vol. 57, no. 8, [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/2632040.

[5] "ITIF technology explainer: What is facial recognition?," Apr. 8, 2020, [Online]. Available: https://itif.org/publications/2020/04/08/itif-technology-explainer-what-facial-recognition.

[6] Steve Knopper, "Why Taylor Swift is using facial recognition at concerts," Dec. 13, 2018, [Online]. Available: https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.

[7] Rayna Hollander, "Here's when facial recognition will be standard on phones" Feb. 12, 2018, [Online] Available: https://www.businessinsider.com/facial-recognition-standard-on-smartphones-2018-2.

[8] "Amazon has considered facial recognition in its doorbells," Nov. 19, 2019, [Online]. Available: https://www.marketwatch.com/story/amazon-has-considered-facial-recognition-in-its-ring-doorbells-2019-11-19.

[9] Sergio Mannio, "How facial recognition will change retail," May 8, 2020, [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/#5b7942d13daa.

[10] Ryan Weber, "Thinking beyond checkouts to improve the Customer Experience at Grocery Stores," [Online] Available: https://www.retail-insider.com/retail-insider/2020/1/thinking-beyond-self-checkouts-to-improve-the-customer-experience-in-grocery-stores

[11] Ryan Weber, "Thinking beyond checkouts to improve the Customer Experience at Grocery Stores," [Online]. Available: https://www.intelli-vision.com/smart-retail/

[12] Zhe Zhou et. al, "Invisible mask: Practical attacks on face recognition with infrared," Mar. 13, 2018, [Online]. Available: https://arxiv.org/pdf/1803.04683.pdf

[13] Clare Garvie and Jonathan Frankle, "Facial-recognition software might have a racial bias problem," Apr. 7, 2016, [Online]. Available: https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/

[14] Jon Porter, "Federal study of top facial recognition algorithms finds 'empirical evidence' of bias," Dec. 20, 2019, [Online]. Available: https://www.theverge.com/2019/12/20/21031255/facial-recognition-algorithm-bias-gender-race-age-federal-nest-investigation-analysis-amazon.

[15] Billy Easley, "Facing the future of facial recognition" *J. of James Madison Inst.* no. 57, [Online]. Available: https://www.jamesmadison.org/wp-content/uploads/2019/09/Journal_Fall2019_09_FacialRecognition.pdf.

[16] "Why is aibo not for sale in Illinois?," Nov. 26, 2018, [Online]. Available: https://www.sony.com/electronics/support/articles/00202844.

[17] Christopher Koopman, "The new identity politics," Apr. 19, 2019, [Online]. Available: https://medium.com/cgo-benchmark/the-new-identity-politics-7aef5997ffe2.

[18] Megan Wollerton, "Aibo's dark side. Why Illinois bans Sony's robot dog," Apr. 1, 2019, [Online]. Available: https://www.cnet.com/news/what-sonys-robot-dog-teaches-us-about-biometric-data-privacy/.

[19] Ally Marotti, "Google's art selfies aren't available in Illinois. Here's why:" Jan. 16, 2018, [Online]. Available: https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.

[20] Seyfarth Shaw, "Biometric privacy class actions by the numbers: Analyzing Illinois' hottest class action trend," Jun. 28, 2019, [Online]. Available: https://www.workplaceclassaction.com/2019/06/biometric-privacy-class-actions-by-the-numbers-analyzing-illinois-hottest-class-action-trend/.
[21] Adam Thierer, "The connected world: Examining the internet of things," in *Testimony before the Senate Committee on Commerce, Science, and Transportation*, Washington D.C., (2015).
[22] Jeffrey Dastin, "Rite Aid deployed facial recognition systems in hundreds of U.S. stores," Jul. 28, 2020, [Online]. Available: https://www.reuters.com/investigates/special-report/usa-riteaid-software/.
[23] "IBM CEO's letter to congress on racial justice reform" Jun. 8, 2020, [Online]. Available: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/
[24] "Privacy multistakeholder process: facial recognition technology," Jun. 17, 2016, [Online]. Available: https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology.
[25] "Our approach to facial recognition" [Online]. Available: https://ai.google/responsibilites/facial recognition/.
[26] Rich Sauer, "Six principles to guide Microsoft 's facial recognition work," Dec. 17, 2018, [Online]. Available: https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/.
[27] "Understanding facial recognition Systems," Partnership on AI, Feb. 19, 2020, [Online]. Available: https://www.partnershiponai.org/facial-recognition-systems/.i
[28] Melanie Ehrenkranz, "The mystery of that Taylor Swift face recognition kiosk has been solved" Feb. 15, 2019, [Online]. Available: https://gizmodo.com/the-mystery-of-that-taylor-swift-face-recognition-kiosk-1832653921
[29] Samuel D. Warren and Louis D. Brandeis, "The right to privacy," *H. L. R*. vol. 4, no. 5, pp. 193 – 220, Dec. 1890.
[30] "Face facts: dispelling common myths associated with facial recognition technology," Security Industry Association, [Online]. Available: https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf.
[31] "Face facts: Dispelling common myths associated with facial recognition technology," Security Industry Association, [Online]. Available: https://www.securityindustry.org/wp-content/uploads/2019/06/facial-recognition-20193.pdf.
[32] "NIST launches studies into masks' effect on face recognition software," NIST, Jul. 27, 2020, [Online]. Available: https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software.
[33] Aaron Holmes, "These clothes use outlandish designs to trick facial recognition software into thinking you're not human" Jun. 5, 2020, [Online]. Available: https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10.
[34] *Carpenter v. United States*, 585 U.S. 2018.
[35] *United States v. Jones*, 565 U.S. 2012.
[36] Sam duPont, "On facial recognition, the U.S. isn't China – Yet," Jun. 18, 2020, [Online]. Available: https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet,
[37] Sam duPont, "On facial recognition, the U.S. Isn't China – Yet," Jun. 18, 2020, [Online]. Available: https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet.
[38] "Sen Coons, Lee bill requires court orders for law enforcement use of facial recognition technology," Nov. 14, 2019, [Online]. Available: https://www.coons.senate.gov/news/press-releases/facial-recognition-tech-sens-coons-lee-bill-requires-court-orders-for-law-enforcement-use-of-facial-recognition-technology

Neil A. Chilson was born in Denver, CO, USA in 1977. He received a B.S. in computer science at Harding University, Searcy, Arkansas in 1999; a M.S. in computer science from University of Illinois, Urbana-Champaign, Illinois in 2005; and a J.D. from The George Washington University School of Law, Washington, District of Columbia, in 2007.

Since 2018, he has been the Senior Research Fellow for Technology and Innovation at the Charles Koch Institute in Arlington, Virginia, where he develops policy positions and strategy that guide the organization's grantmaking and other investments. He hold a similar title at Stand Together, where he publicly advocates for technology policy frameworks that enable permissionless innovation. In 2017, acting Federal Trade Commission Chairman Maureen Ohlhausen appointed him acting Chief Technologist for the Commission. In that role he established the FTC's Cryptocurrency Working Group and informational injury. From 2014 to 2017, he served as an attorney advisor to Ohlhausen, advising her on nearly every significant technology policy matter to come before the Commission, including cases and reports related privacy, data security, network neutrality, and cryptocurrency. From 2007 to 2014, he was an associate at Wilkinson Barker Knauer, LLP, where he focused on telecommunications regulation, including wireless, wireline, and satellite matters. His work has been published in *Newsweek*, *Washington Post*, *Issues*, the *Georgetown Technology Law Review*, the *Pepperdine Law Review*, and the *Wall Street Journal*. He is currently writing a book titled, "Getting Out of Control: Enabling Emergent Order in Public Policy and Personal Life."

Mr. Chilson is a member of the Association of Computing Machinery and the Federalist Society.

Taylor D. Barkley was born in Mission Viejo, CA, USA in 1986. He received the B.A. in history and political science Taylor University, Upland, Indiana in 2009.

From 2011 to 2012, he was a Program Associate for Academic Student Programs at the Mercatus Center at George Mason University. From 2012 to 2017 he was the Assistant Director of Outreach for Technology Policy at the Mercatus Center. In 2017 until 2018 he was the Government Affairs Manager at the Competitive Enterprise Institute. Since 2018 he has been a Program Officer for Technology and Innovation at the Charles Koch Institute in Arlington, Virginia. He is the co-author of one book, articles published by *Scientific American, Real Clear Policy*, *Light Magazine,* The Institute for Faith, Work, and Economics, and *Human Progress.* His research interests include issues at the intersection of culture, society, religion, and technology, artificial intelligence, automated systems and the future of work, and the societal impact of social media.

Mr. Barkley is a member of the American Enterprise Institute's Faith and Public Life Ideas Council.