Written Statement of Brenda Leong
Before the U.S. House of Representatives
Committee on Oversight and Reform
Rayburn House Office Building
Washington, D.C. 20515
January 15, 2020

I. Introduction

Thank you for the opportunity to testify today. My name is Brenda Leong, and I am Senior Counsel and Director of AI and Ethics at the Future of Privacy Forum (FPF). FPF thanks the Committee Chair and Ranking Member for convening today's hearing, and for working to address the privacy and civil liberties challenges of commercial uses of facial recognition technology.

FPF is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. We believe that the power of information technology is a net benefit to society, and that it can be well-managed to control risks and offer the best protections and empowerment to consumers and individuals.

FPF has a substantial portfolio of work regarding the intersection of privacy and facial recognition. We analyze policy proposals and provide feedback to policymakers. We speak with stakeholders – including leaders from the corporate, public sector, and non-profit communities – to exchange best practices and knowledge regarding commercial uses of facial recognition systems. After an extensive development process with developers and current and prospective enterprise users of these systems, we published Privacy Principles for Facial Recognition

Technologies in Commercial Applications,[1] and created an educational graphic for Understanding Facial Detection, Characterization, and Recognition Technologies.[2] These Principles define a benchmark of privacy requirements for those commercial situations where technology collects, creates, and maintains a facial template that can be used to identify a specific person – enabling beneficial applications and services, while providing the necessary protections for individuals.

The consumer-facing applications of facial recognition technology continue to evolve and appear in new contexts. There are several main services and functions that benefit from facial recognition technology, including: (1) safety and security; (2) access and authentication; (3) photograph and video storage identification and organization; (4) accessibility to platforms, accounts, or services, and (5) marketing and customer service. There are also, however, specific concerns about the privacy protections needed for the responsible use of this expanding technology. Any regulatory or legislative guidance must be designed to drive responsible data use by those businesses and online platforms developing and using facial recognition technology in commercial settings, to establish a foundation of protections for personal data that is deserving of user trust, and to inform the conversation on the specifics of the technology and the technical and policy protections available. Whether driving industry best practices, informing consumer expectations, or assisting policymakers regarding the various technologies discussed, new business practices and consumer needs may evolve and warrant ongoing evaluation.

---

[1] Future of Privacy Forum, Privacy Principles for Facial Recognition in Commercial Uses, September 2018, https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf

[2] Future of Privacy Forum, Understanding Facial Detection, Characterization, and Recognition Technologies, September 2018, https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.

II. Facial Recognitions Systems Collect and Use Sensitive Data.

When is your face just a photo and when is it a "biometric identifier?" Facial recognition systems are particularly sensitive because they involve a unique part of the human body, one that is directly related to our identity and has the potential to infringe upon our concept of self in public, private, and commercial contexts. This impacts our ability to feel anonymous or obscure in public or in large crowds.[3]

Thus, privacy discussions about the personal data generated by facial recognition systems must necessarily consider the heightened considerations for sensitive data, as well as reflect the larger debate around ubiquitous surveillance concerns. But there is not a consensus about whether personal privacy and digital data protections at a comprehensive level are sufficient,[4] or whether it's particularly important in this case to focus laws on this technology in isolation. Under either strategy, both consumers and businesses should be able to rely on substantive protections and certainty as to how biometric data is collected and used.

In addition to the sensitivity of the data itself, the design choices during development affect system outputs and the decisions they inform. Commercial enterprises increasingly rely on automated decisions (i.e. medical, professional, financial, legal determinations). It is the responsibility of individuals, institutions, and society to be aware of this power, and evaluate the

---

[3] Woodrow Hartzog and Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343 (2015), https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/10.

[4] Council of Foreign Relations, January 30, 2018, Reforming the U.S. Approach to Data Protection and Privacy, https://www.cfr.org/report/reforming-us-approach-data-protection and see also Cameron Kerry, Brookings Institute, July 12, 2018, Filling in the gaps in US Data Privacy Laws, at https://www.brookings.edu/blog/techtank/2018/07/12/filling-the-gaps-in-u-s-data-privacy-laws/

impacts these systems have, and for policymakers to carefully consider the potential harms that must be mitigated in order for the benefits of such systems to be fully realized.[5]

It will not always be clear to the general public who owns or operates the surveillance cameras around them, who has access to the data being generated, whether the data collected is subject to facial recognition analysis, and if so, by whom, for what purposes, or subject to what protections and controls. Both the service providers, and the enterprise platforms bear some responsibility to consider the privacy and social implications of how their system recommendations ultimately impact individuals.[6]

III. Not All Camera-based Systems Are Created Equal. Understanding Each Technology, With Its Capabilities and Limitations, Is Fundamental.

Understanding how particular image-analysis technology systems work is a critical foundation for effectively understanding and evaluating the risks of facial recognition. The media, the public, and even the designers and producers of various image-based systems inconsistently use the term facial recognition to refer to other image-based technology related to faces that does not necessarily involve individual identification.

The various types of facial scanning systems are generally understood to occur along a spectrum from facial detection systems where no Personally Identifiable Information (PII) is collected; through facial characterization, where a single image is evaluated but no personal templates are created or enrolled; to facial verification and identification systems, which create,

[5] Solon Baracas, and Andrew D. Selbst, "Big Data's Disparate Impact," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2016. Available at https://papers.ssrn.com/abstract=2477899.)

[6] Understanding bias in algorithmic design," Impact. Engineered, September 5, 2017. Available at https://medium.com/impact-engineered/understanding-bias-in-algorithmic-design-db9847103b6e.

store, and compare personal facial templates. These four levels of facial image software each have different use cases, benefits and risks, and privacy implications.[7]

The most basic applications use facial detection, such as what you might see through your camera – the small square overlay that moves around to frame the face(s) of the people in your field of vision. This technology finds what is 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 uses that simply need to establish when a person is present. Data collected by detection programs is not a template, is not identifiable, linked, or linkable to individuals, and does not typically require privacy protections.

The next level is called facial characterization, also sometimes facial analysis, or more recently, emotion detection. In this case, the camera is still not creating a database template or seeking matches among multiple images, but more detailed information is being observed and collected by analyzing the image. An interactive billboard at a bus stop, or a screen mounted above a product display might be used to collect information such as gender, approximate age range, and potential emotional indicators ("smiling," "sad"), that can be combined with other data such as how long the person looked at the screen, or where else they went within the store. This can give advertisers useful information about shoppers' reactions, based on type: young women responded favorably; older men moved away indifferently.

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." Like detection, facial characterization programs do not routinely create or retain

[7] Future of Privacy Forum, Understanding Facial Detection, Characterization, and Recognition Technologies, September 2018, https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf.

personably identifiable facial templates. Facial characterization technology is evolving rapidly, however, particularly those systems purporting to have emotion detection capabilities, and should continually be evaluated when used in new contexts for the potential future PII that may be implicated.

What the term "facial recognition" accurately encompasses are the personalized levels: 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, and 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, a building may hold a database with all the building employees enrolled in it, their templates created and stored. 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 further evaluation. In verification, the system does not look at any other templates or attempt to identify the person if they do not match the initial entry. The output is a simple "yes" or "no" to validate the claimed identity.

By contrast, the final category of facial recognition is identification, known as a one-to-many matching process. In this case, it 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 video tape at a public venue, or an image from a camera on-scene – creates a template, and then attempts to match it against

whatever dataset is made available. In the one-to-many scenario, the system may come back with multiple possible matches. Threshold match settings can be preset to varying levels of sensitivity (based on the desired default for false positives or false negatives), but ultimately a human should review any suggested matches for a final decision on whether the selected person has been successfully identified.

To clarify, identification systems do not create photos. They create templates. When the face is scanned, the system isn't taking a picture, it is creating a point-based design derived from your facial structure that is generated by proprietary software. That is, every company's system does it differently, and they are typically not interchangeable. The generated overlay is a template which is then turned into a number string consisting of 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, the scan is made, the created template is then stored, and the data will be linked with a tag or code to connect to the full record of any other personal information collected or retained about that individual.[8]

When the person returns to be verified (or a person or image is selected for identification to be attempted), the system performs a current scan of the face, creates a new template, and then compares against the enrolled file(s) for a match. When a matching template is found, the person has potentially been identified. This process likely takes less than a second, and for any reputable

[8] Biometrics Explained. IBIA, 2018, at https://www.ibia.org/download/datasets/4346/IBIA-Biometrics-Explained-final-final-web.pdf.

system, no digital image is ever stored with the template,[9] and no biometric can be recreated from the template.[10]

Identification is most commonly used in security contexts, such as identifying someone shoplifting against a data set of known shoplifters, or clearing 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. Many times the current collected images from "the wild" will be lower quality, images of people in hats, in shadows, or captured from odd angles. Any potential match or matches will likely be at lower levels of certainty, and a human official should be engaged prior to taking any actions based on the system's outputs.

The sufficient level of accuracy for any system varies based on application and context. On an iPhone, Apple's system is verifying an image stored locally on the device. Apple's system, called FaceID, uses an infrared camera, a depth sensor and a dot projector to map 30,000 points on a face and create an 3D 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 detail and level of certainly for this match yield roughly a false positive rate of 1 in 10 million. This is an entirely acceptable standard for phone access but is far below the standards that would be required for terrorist watchlists. It should not be sufficient for criminal prosecution.[11]

---

[9] Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies, FTC, 2012, at https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

[10] As in an example: Facial Recognition with Biometric Encryption in Match-on-Card Architecture for Gaming and Other Computer Applications, Privacy by Design, Canada, 2014, https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-facial-recognition-biometric.pdf.

[11] Angwin, Julia, Jeff Larson, Surya Mattu, and Laura Kirchner. "Machine Bias." ProPublica, May 23, 2016. Available at https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing).

IV. Different Image-Based Systems Pose Different Levels of Risk Relative to Their Benefits and Must Be Assessed and Addressed Accordingly.

Historically, your image wasn't easily collected, tracked, shared or weaponized by either commercial entities or governments. But now it can be. The amount of information sought from faces outstrips any other biometric – the similar challenges we face with genetic data is the only thing that comes close.

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 two main considerations regarding security for these types of systems. One is the traditional security evaluation of the network security of the data itself, once collected. Established best practices apply, including some specific to biometrics such as not retaining a copy of the original digital image (face or fingerprint, for example), or if for some reason it is necessary to the context, retaining them in separate files unlinked to either the created template, or other PII.

But secondly, and somewhat specific to biometric systems, is how close to "perfect" the system operates. This means, can the system be spoofed? – that is, access gained without the actual person's face present, using a photo, rubber mask, or other substitute. High quality facial recognition systems rate very high on anti-spoofing evaluations, 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 considering the risk is to compare biometric systems to available alternatives, such as passwords, where they are almost always a more secure option.

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 higher likelihood that the data would be magnitudes harder to exploit in any broad-based 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 having the biometric alone isn't enough to gain access.

A relevant core privacy principle here is Data Quality and Integrity, the requirement that individual data and data sets are "accurate, relevant, timely and complete."[12] The challenges for current facial recognition systems achieving sufficient accuracy across demographic variations such as race, ethnicity, and gender, are well-documented[13], although they are improving all the time. Recent NIST testing has shown that for the best systems available in the market today, the different in accuracy across demographic groups were undetectable.[14]

System reliability is not the only concern. There is also the potential for bad actors to use facial recognition to unfairly or illegally discriminate. For example, a retail chain might create its own dataset of "known" offenders without any clear standards for who is targeted, no practice by which they are notified or can appeal their inclusion, and create the potential of sharing such lists with other companies, resulting in individuals being broadly denied service without any due process. These and related harms must be considered when assessing appropriate use cases and associated protections.

Privacy concerns cross into both commercial and governmental spheres. Government misidentification can lead to innocent people on "watch lists," with increased risk of bad results for minorities and other at-risk populations. The ethical considerations of where and how to use facial recognition systems exceed the boundaries of traditional privacy considerations. By using

---

[12] Department of Homeland Security, Privacy Policy Guidance Memorandum, 2008, https://www.dhs.gov/sites/default/files/publications/privacy_policyguide_2008-01_0.pdf.
[13] Hardesty, Larry. "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems." MIT News, February 11, 2018. Available at http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.
[14] NISTIR 8280, Facial Recognition Vendor Test, Part 3. December 2019, at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

machine learning programs as the underlying foundation, these systems are built on existing systems that reflect human biases, and automate them.[15] Having "humans in the loop" will not mitigate this; trained programmers must test and audit systems for bias and be able to recommend corrective measures. The social impacts of this are only beginning to be understood.[16]

There are many beneficial use cases for facial recognition systems. For individual users, there are many convenient services, some as simple as tagging people while sorting and organizing photos. Several companies offer tools that incorporate facial detection, characterization, and/or identification to assist the blind and low vision communities. There are screen readers that provide audio or braille user interfaces for people who are blind or have low vision. Hotels and conferences are working to create a seamless experience based on facial recognition systems for their members and registrants who have opted-in to such a service, traveling from taxi, to lobby, to room, or checking 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.[17] They can do so

---

[15] Nicole Turner-Lee, Paul Resnick, and Genie Barton, Brookings Institute, Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms, May 2019, https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

[16] Hadhazy, Adam. "Biased Bots: Artificial-Intelligence Systems Echo Human Prejudices." Princeton University, April 18, 2017. Available at https://www.princeton.edu/news/2017/04/18/biased-bots-artificial-intelligence-systems-echo-human-prejudices.

[17] NBC News, Tom Costello, Ethan Sacks, August 23, 2018, New Facial Recognition Tech Catches First Imposter at DC Airport, https://www.nbcnews.com/news/us-news/new-facial-recognition-tech-catches-first-impostor-d-c-airport-n903236.

generally with decreased costs, increased efficiencies, and consistently greater accuracy than humans. New uses are being imagined and developed all the time.[18]

Some use cases may not inherently be either good or bad. Profiling shoppers, tracking online preferences and personalizing recommendations or experiences are features some consumers value, but others strongly oppose. Tying these services to the appropriate consent level is important.

The privacy and liberty challenges are real.[19] In addition to achieving sufficient accuracy for their intended use cases, concerns about real time surveillance societies have led to significant reservations about their reliability from a civil liberties standpoint. The decision by some municipalities to legislatively ban all use of such systems by government agencies reflects these heightened concerns.[20]

The discussion so far has focused on systems that can be objectively tested and measured for their use purposes, such as the accuracy testing done by NIST.[21] When it comes to characterization and "emotion detection" systems, there is the further problem that these systems are largely based on bad or incomplete and unproven science.[22] Although these systems are not

---

[18] Don't judge a book by it's cover…but it might judge you?, Slate, 2015, https://slate.com/technology/2015/02/this-book-only-opens-if-its-facial-recognition-software-decides-you-are-nonjudgmental.html

[19] Sydell, Laura. "It Ain't Me, Babe: Researchers Find Flaws In Police Facial Recognition Technology." NPR.org, October 25, 2016. Available at https://www.npr.org/sections/alltechconsidered/2016/10/25/499176469/it-aint-me-babe-researchers-find-flaws-in-police-facial-recognition.

[20] Graham Vyse, Cities Ban Government Use of Facial Recognition, July 2019, https://www.governing.com/topics/public-justice-safety/gov-cities-ban-government-use-facial-recognition.html.

[21] NISTIR 8280, Facial Recognition Vendor Test, Part 3. December 2019, at https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

[22] Science Daily, from Association for Psychological Science, July 18, 2019, Emotion Detection Applications Built on Outdated Science, Report Warns, at https://www.sciencedaily.com/releases/2019/07/190718085318.htm.

currently used to create PII or link conclusions to personal records, they potentially could be. The idea that a single image should be analyzed to determine that it definitively expresses happiness, anger or fear, and that such analysis can or should be used to inform targeting within a commercial relationship is controversial, at least.[23]

Research has shown that a variety of human observers will decide differently that a person is smiling, or not, based on many factors such as the race, gender, and culture of each party, as well as many contextual details. Even if all observers somehow agree that a look is a smile, to take the leap to the smile meaning the person feels "happy", and then further extrapolate that feeling happy represents some behavior or characteristic of the individual in a characteristic or definitive way is still largely in the realm of science fiction.

The regulatory challenges to these issues are great. Even relatively straightforward legal questions such as liability for misuse or malfunction immediately prove complex when there are manufacturers, programmers, enterprise users, consumer facing businesses, and individual consumers who all may bear some level of responsibility. When considering the scope of industries hoping to use this technology in some way – from educational and financial institutions to retail establishments – the potential impacts on individuals are mind-boggling.[24]

---

[23] Jay Stanley, ACLU, Experts Say "Emotion Recognition" Lacks Scientific Foundation, July 18, 2019, at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/experts-say-emotion-recognition-lacks-scientific.

[24] CBInsights, Like it or Not, Facial Recognition Is Already Here. These are the Industries It Will Transform, April 2019, https://www.cbinsights.com/research/facial-recognition-disrupting-industries/.

V. Congress Can Address the Legal Challenges Around Facial Recognition Technology and Provide Standards and Protections.

FPF has long supported a baseline, comprehensive federal privacy law. We are encouraged by the opportunities for bipartisan collaboration on such a law in this Congress. A baseline federal privacy law would necessarily include heightened protections for sensitive personal information such as facial recognition data and other biometric identifiers.

Recent federal privacy legislation discussions have also included questions around preemption for state legislation as well as compatibility with other existing privacy related regulatory language. In addition, when considering privacy legislation, the challenge remains as to whether, or how, to single out particular technologies for unique requirements or attention.

Currently, several state and federal laws and regulations govern the collection or use of personal data, where facial recognition data could be considered one type of such data. These laws and regulations include, but are not limited to, the Gramm-Leach-Bliley Act,[25] the Health Insurance Portability and Accountability Act,[26] the Children's Online Privacy Protection Act,[27] the California Online Privacy Protection Act,[28] the Electronic Communications Privacy Act,[29] Section 5 of the Federal Trade Commission Act,[30] and state UDAP ("Unfair or Deceptive Acts or

[25] 15 USC §6801. Protection of Nonpublic Personal Information, at https://www.law.cornell.edu/uscode/text/15/6801.
[26] 45 CFR Part 160, Part 162, and Part 164.
[27] 15 U.S. Code § 6501. Children's Online Privacy Protection Act, at https://www.law.cornell.edu/uscode/text/15/6501.
[28] California Code Chapter 22, Internet Privacy Requirements, Section 22575, at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC.
[29] 18 USC Chapter 119—Wire And Electronic Communications Interception And Interception Of Oral Communications, at https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.
[30] Federal Trade Commission Act, Section 5, Unfair or Deceptive Acts or Practices, at https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

Practices") laws.[31] The states of Illinois,[32] Texas,[33] and Washington[34] all have passed commercial biometrics laws that include facial imaging and scans, with detailed protections and requirements. Additionally, the FTC has provided recommendations[35] specific to the use of facial recognition technology, suggesting that companies using facial recognition technologies do the following:

- Take steps to ensure consumers are aware of facial recognition technologies when they come in contact with them;
- Provide consumers with clear notice about how facial recognition features or technology work, what data is collected, and how the data will be used;
- Provide consumers with choices as to data collection and use;
- Design their services with consumer privacy in mind;
- Develop reasonable security protections for the information they collect, and sound methods for determining when to keep information and when to dispose of it; and
- Consider the sensitivity of information when developing their facial recognition products and services.

These recommendations provide an existing and reasonable foundation for any regulations targeted to facial recognition systems. However, there are potential unintended consequences of

---

[31] National Consumer Law Center, Unfair and Deceptive Acts and Practices, https://www.nclc.org/issues/unfair-a-deceptive-acts-a-practices.html.
[32] 740 ILCS 14, Biometric Information Privacy Act, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
[33] Texas Business and Commerce Code, Sec. 503.001. Capture Or Use Of Biometric Identifier, https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.
[34] Chapter 19.375 RCW, Biometric Identifiers, https://app.leg.wa.gov/RCW/default.aspx?cite=19.375.
[35] FTC Recommends Best Practices for Companies That Use Facial Recognition Technology, 2012, https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.

taking a sectoral approach to biometric technologies.[36] Varying vocabulary and non-standard definitions of biometrics, particularly as related to images and facial scans or templates, make it difficult to compare requirements across jurisdictions or even use cases. Likewise, treating facial recognition and characterization systems together under a shared approach may cause confusion around the digital photo itself, and make it unclear both to businesses and individuals when and how different digital files are impacted, and what permissions or protections apply.

Should Congress pursue facial recognition-specific legislation, there are several key points which should provide the foundation, as described in our Privacy Principles.[37] While not sufficient to address all concerns, consent remains the critical factor, and should be tiered based on the level of personal identification collected or linked, and the associated increasing risk levels.

- No unique biometric identifier should be created and maintained over time without appropriate consent.
- For commercial applications using verification or identification systems, the requirement should be an "opt-in" model, that is, a default of express, affirmative consent consistent with existing FTC definitions, accepted practices, and expectations. Exceptions to this express consent requirement should be limited and narrow.

[36] Mercatus Center, The State of State Data Laws, Part 3: Biometric Privacy Laws and Facial Recognition Bans, August 2019, at https://www.mercatus.org/bridge/commentary/state-state-data-laws-part-3-biometric-privacy-laws-and-facial-recognition-bans.

[37] Future of Privacy Forum, Privacy Principles for Facial Recognition in Commercial Uses, September 2018, https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf.

    - Use cases involving unique persistent identifiers (lacking links to other personal data) would require only opt-out consent options.
    - Facial detection and characterization systems that, as described, collect no personally identifiable information, do not require consent.
- Facial recognition applications should be held to standards that are fair and in line with consumer expectations, such as articulating the benefits and privacy practices to consumers and providing opportunities for consumers to make choices to mitigate or avoid risks.
    - Determine whether a proposed use is compatible with expectations by considering factors to include the context of collection; a reasonable awareness of how the data will be used; whether facial recognition is merely a feature of a product or service or integral to the service itself; and how the collection, use, or sharing of facial recognition data will likely impact the consumer.
    - Require consideration for how the use of facial recognition technology will impact both consumers who purposefully avail themselves of products or services which incorporate that technology as well as consumers who incidentally come into contact with these systems or cannot reasonably avoid a company's use of facial recognition technology.
    - Give special consideration to the age, sophistication, or degree of vulnerability of those individuals, such as children, in light of the purposes for which facial recognition technology is used, including whether additional levels of

transparency, choice, and data security are required. This includes awareness and compliance with any additional legal requirements that may apply.

- Require companies implementing facial recognition systems to develop and publish privacy policies describing their use of facial recognition systems in clear terms with a detailed description of the data collected. Privacy policies, educational help centers, and other materials are ways to ensure consumers and other stakeholders can understand the collection, use, retention, and appeal or deletion rights for individuals.
- Require data security practices and procedures commensurate with the sensitivity of the facial recognition data, the context in which facial recognition technology and facial recognition data is employed or used, the likelihood of harm to consumers, and other relevant factors. As with all personal data, provide data security appropriate to the sensitivity of facial recognition data when collected, shared, when at rest and in transit, and when used for research or product improvement purposes.

VI. Conclusion

The use of facial recognition systems is not solely responsible for the ethical and social privacy problems being considered today, of course. They are being implemented in a world already facing the problems of biased human systems.

Similar battles regarding other identification and tracking systems with important social implications have been waged before. The problem of whether private citizens should be required to have government-issued documentation verifying their personal identity 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 efficiencies and security against protections for individual rights and freedoms.

When they were first implemented, passports were offensive, and the later requirement that they include a photo shocked the public consciousness; such developments were widely contested and denounced.[38] Our country has routinely and consistently resisted the call for a federally issued national ID card.[39] REAL ID requirements for state licensing have been controversial since they were implemented.[40] These historical discussions reflect the ongoing need to determine the appropriate balance of technological, legal, and policy standards and protections, along with the underlying threshold question of whether some systems are simply too high risk to implement regardless of perceived benefits.

Technology has only accelerated the practice of identification and tracking of people's movements, whether by governments, commercial businesses, or some combination thereof, leading to the real concerns about an ultimate state of ubiquitous surveillance. How our society faces these challenges will determine how we move further into the conveniences of a digital world, while continuing to embrace our fundamental ideals of personal liberty and freedom.

---

[38] Tao Tao Holmes, Atlas Obscura, Passports Were Once Considered Offensive, and Perhaps They Still Are, December 2015, https://www.atlasobscura.com/articles/passports-were-once-considered-offensive-perhaps-they-still-are.
[39] Government Technology, What's Wrong With A National ID Card, 1996, https://www.govtech.com/magazines/gt/Whats-Wrong-With-a-National-ID.html.
[40] NPR, The REAL ID Act Raises Privacy Issues, 2005, https://www.npr.org/templates/story/story.php?storyId=4632952.