CASE STUDY

FACIAL RECOGNITION

This is part of a set of materials developed by an interdisciplinary research team at Stanford University, led by Hilary Cohen, Rob Reich, Mehran Sahami, and Jeremy Weinstein. Their original use is for an undergraduate course on ethics, public policy, and technology, and they have been designed to prompt discussion about issues at the intersection of those fields. This case was written by Jared Bennett.

Stanford | ETHICS TECHNOLOGY & PUBLIC POLICY

I. Introduction: An about face on facial recognition?

For two days in April 2018, Facebook CEO Mark Zuckerberg testified before the Senate Judiciary and Commerce Committees in a joint session watched closely by members of Congress, the media, and millions of concerned Facebook users. They watched his face for clues as to how the company would respond to multiple controversies, including the revelation that consulting firm Cambridge Analytica had gained access to the data of millions of Facebook profiles, and used it to try and shape public opinion about politics in the United States and Europe.

Zuckerberg ended up acknowledging another controversy brewing behind the scenes. It's a dispute that hasn't garnered the same attention as other recent Facebook entanglements, but what's at stake is one of the most personal sources of data imaginable: your face.

Fourteen years after Zuckerberg launched Facebook in his Harvard dorm room, the company has become the undisputed champion of facial recognition, the process of using software to identify or verify an individual based on unique facial patterns. Facebook uses facial recognition to identify users in photographs uploaded to the platform and has filed patents for more expansive uses such as retail security and payment processing.

But the technology is already nearly ubiquitous. Users might interact with facial recognition for convenience while unlocking an iPhone with Apple's FaceID, for example, or more surreptitiously, find themselves identified by the facial recognition technology used by police and security services to monitor physical spaces around the world.

When Zuckerberg's day on Capitol Hill arrived, Facebook had recently announced new uses for facial recognition and revamped its privacy settings to give users more control over facial recognition. "The words 'face recognition' can make some people feel uneasy, conjuring dystopian scenes from science fiction," Facebook's Deputy Chief Privacy Officer **Rob Sherman** wrote in a blog post explaining the changes in December 2017.[1] However, Sherman wrote, "we believe we have a responsibility to build these features in ways that deliver on the technology's promise, while avoiding harmful ways that some might use it."

Critics were still surprised, however,[2] when Zuckerberg talked about the need for "special consent for sensitive features like face recognition in his testimony."[3] The privacy community has been harping for years on the special threats to privacy, anonymity, and free speech posed by facial recognition technology used without checks and balances: Facebook's own face recognizing tool is more accurate than the Federal Bureau of Investigation's.[4] But many worry that progress comes at the expense of users' privacy.

Cambridge Analytica turned data about Facebook users' interests and friends into a list of potential targets for political ads with the aim of influencing or manipulating American and British voters. The controversy served to illustrate that as technology progresses, more and more of our lives can be mined for data. Once it's collected, we might not like, or even know, how even seemingly innocuous data we willingly hand over is used.

---

[1] Rob Sherman, "Hard Questions: Should I Be Afraid of Face Recognition Technology?" Facebook Newsroom, December 19, 2017 https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/

[2] Louise Matsakis, "As Zuckerberg Smiles to Congress, Facebook Fights State Privacy Laws," *WIRED*, April 12, 2018. https://www.wired.com/story/despite-zuckerberg-pledge-facebook-fights-state-privacy-laws/

[3] Testimony of Mark Zuckerberg, Hearing Before The United States Senate Committee on the Judiciary and the United States Senate Committee on Commerce, Science and Transportation, April 10, 2018, https://www.judiciary.senate.gov/imo/media/doc/04-10-18%20Zuckerberg%20Testimony.pdf

[4] Russell Brandom, "Why Facebook is beating the FBI at facial recognition," The Verge, July 7, 2014, https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition

Data derived from physical properties that can identify its source is called "biometric data,"[5] and its use raises important questions surrounding data collection and privacy in public spaces. When we appear in public, what information about ourselves do we have a right to keep hidden, and from whom? Where do we draw the line between innovative and potentially intrusive technology? And what do companies or government agencies that use biometric data owe to the subjects of data collection? We can approach these questions by taking a deeper like into facial recognition and its history.

II. The power and potential of facial recognition

The first facial recognition systems were invented[6] in 1964. Those early tools made use of essentially a book of mug shots[7] to mathematically identify criminal suspects.

Even the technology's early pioneers could scarcely imagine what it would look like down the road. **Joseph Atick** began working on facial recognition in the 1990s and now works as an industry consultant. Initially an enthusiast, over the years he's become skeptical of facial recognition and its potential for abuse. "It pains me to see a technology that I helped invent being used in a way that is not what I had in mind in respect to privacy," Atick told the Center for Public Integrity in 2017.[8]

Atick was born in Jerusalem in 1964, the same year as facial recognition. Atick's childhood was marked by conflict centering on ethnic and religious identity. He vividly remembers seeing an identity booklet that listed his name, address, and religion.

The experience shaped his view that markers of personal identity are vital, something to be protected and disclosed only when there is a level of trust between parties. Central to Atick's concept of identity is control over who can access identifying information. "You assert your identity," Atick said. "You don't want your identity controlled or maintained without you having a say."

Atick today speaks widely about the beneficial uses and potential dangers of facial recognition and biometric information around the globe. His technology has been used to identify known terrorists, prevent identity fraud, and most recently to provide identification for people who wouldn't otherwise have one. (For a detailed list of current use cases of facial recognition, see Exhibit 1.)

Facial recognition is poised to be big business. The market for the technology is expected to hit $9.6 billion by 2022.[9] Some of the companies involved in the deployment of facial recognition have attempted to establish a framework for its use that protects the privacy of individuals. Microsoft, for example, formed a new group called the AETHER Committee (which stands for "AI and Ethics in Engineering and Research") to advise the company on ethical questions, including reducing bias and creating an ethical framework for facial recognition technology.[10]

---

[5] For a complete list of biometric data types, see the Biometrics Institute: https://www.biometricsinstitute.org/types-of-biometrics

[6] Dr.S.B.Thorat, S.K.Nayak, Jyoti P Dandale, "Facial Recognition Technology: An analysis with scope in India", 2010. https://pdfs.semanticscholar.org/4e14/fe029506ba2031c37de8e32bf885e61d2a27.pdf

[7] Ibid

[8] The information in this section comes from interviews with Joseph Atick conducted in July 2017.

[9] Rachna Singh, "Global Opportunity Analysis and Industry Forecast, 2015 - 2022" *Allied Market Research*, 2016. https://www.alliedmarketresearch.com/facial-recognition-market

[10] Brad Smith, "Facial recognition technology: The need for public regulation and corporate responsibility", Microsoft Blog, July 13, 2018, https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

In summer 2018, Microsoft went further and asked that the technology be formally regulated by government. It's unusual for tech companies to invite legal regulation, but Microsoft argues that without sensible regulation, marketplace competition will fail to navigate wisely between social responsibility and marketplace success. "We believe," argued Microsoft, "that the only way to protect against this race to the bottom is to build a floor of responsibility that supports healthy marketplace competition. And a solid floor requires that we ensure that this technology, and the organizations that develop and use it, are governed by the rule of law."[11]

As new corporate and regulatory frameworks take shape, there are consistent themes and tenets emerging. For example, most frameworks require that inclusion in a facial recognition database be permitted only when there is a clear and legitimate reason for a subject to be included. Most privacy advocates also agree that subjects of facial recognition should be given notice that they are being identified. This is generally the case in what is known as "constrained" facial recognition, which refers to situations where the subject being identified is in a controlled setting. Constrained facial recognition is common in security settings like airport checkpoints or identification systems that unlock devices like the iPhone Face ID. The physical features of the subject are scanned in person with the subject's knowledge. The subject's face is knowingly presented to be scanned and variables like posture, lighting and expression are usually controlled.

But as technology has progressed, the holy grail of facial recognition has become building a system that recognizes faces as a human can – that is, independent of the factors that make recognizing an image in everyday settings technologically challenging. This is unconstrained facial recognition or facial recognition "in the wild."[12]

The way Atick sees it, social media, and Facebook especially, has changed the game. People now freely provide information to governments and companies where in the past they might have been reticent. "We don't even know we are building the database for big brother," Atick said. "We just want to share photos with our friends."

Facebook introduces facial recognition

When Facebook entered the world of facial recognition in 2010, it did so hesitatingly.

Facebook initially introduced a system to detect faces in an image without recognizing or labeling them. Facebook's Photos product manager Sam Odio said in 2010: "This isn't photo recognition." The company wanted to stay away from facial recognition, a tool Odio labelled "a very touchy subject."[13]

But in 2011 Facebook introduced facial recognition as "Tag Suggestions."[14] When Tag Suggestions is enabled, Facebook scours photos for biometric data templates. If a match is found using facial recognition, Facebook will suggest individuals to be "tagged" in the photo, creating a link between the photo and the subject's Facebook profile.

Facebook's researchers have made great strides in unconstrained facial recognition. The company's research team has developed a facial recognition tool called DeepFace that can identify faces in

[11] Brad Smith, "Facial recognition: It's time for action", Microsoft Blog, Dec. 6, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

[12] Dr.S.B.Thorat, S.K.Nayak, Jyoti P Dandale, "Facial Recognition Technology: An analysis with scope in India", 2010. https://pdfs.semanticscholar.org/4e14/fe029506ba2031c37de8e32bf885e61d2a27.pdf

[13] Caroline McCarthy, "Facebook Photos get high resolution, bulk tagging", *CNET News,* September 30, 2010, https://www.cnet.com/news/facebook-photos-get-high-resolution-bulk-tagging/

[14] Matt Hicks, "Making Photo Tagging Easier," Facebook blog, December 15, 2010, https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/

photos or video, even real time live feeds, where subjects are not directly facing a camera, in motion or partially obscured.[15] Facebook can also identify people by their clothing and posture,[16] and the company has applied for patents on technologies that detect people's emotions based on their facial expressions.[17]

Facebook's facial recognition technology is the best in the business, but nearly every approach to facial recognition uses a common four-step process: detection, alignment, faceprint creation, and classification.[18] (See Exhibit 2 for more information on Facebook's facial recognition process.) Often, the photos and videos used to identify individuals have backgrounds, multiple faces, slightly hidden or rotated faces, or other factors that require pre-processing before the specific faces can be used. As such, the first step in identifying a face is determining what in a given image is a face and what can be ignored.

Once an individual face is identified within an image, the subsection of the image containing that face is analyzed to determine the face's angle of rotation and any stretch or compression that has distorted its shape. With these measurements, graphical models undo the rotation and distortion and realign the image so that the face is directed towards the camera and has the same size and proportions as the images in the facial database.[19]

After the system generates a flat, forward-facing representation of the subject, the technology converts the face into a faceprint, or a mathematical representation of the face's features.

With a mathematical representation of a face and its unique features, the final step is to compare this faceprint to all other faceprints in the facial database to find close matches. Once candidate matches are found, the system decides which person the face belongs to if it belongs to anyone in the database at all.

As with any machine learning model, a larger dataset to train on usually increases the model's accuracy, so facial recognition algorithms tend to work best with large facial databases. No database is as large as Facebook's. In a 2014 presentation, a Facebook engineer explained that data to train its algorithm is "practically infinite" with about 300 million photos uploaded to the social network every day. [20] The results reflect this advantage. DeepFace boasts an algorithm that achieved 97.35% accuracy in 2014, functionally equivalent to the human-level facial recognition accuracy of 97.53%.[21]

When Facebook introduced Tag Suggestions, the feature was turned on by default and it was up to users to "opt out" of facial recognition rather than "opt in" to its use. Facebook has grappled with this subtle but key distinction ever since.

[15] Dr.S.B.Thorat, S.K.Nayak, Jyoti P Dandale, "Facial Recognition Technology: An analysis with scope in India", 2010. https://pdfs.semanticscholar.org/4e14/fe029506ba2031c37de8e32bf885e61d2a27.pdf

[16] Aviva Rutkin "Facebook can recognize you in photos even if you're not looking," *New Scientist*, June 22, 2015. https://www.newscientist.com/article/dn27761-facebook-can-recognise-you-in-photos-even-if-youre-not-looking/

[17] Facebook Inc patent for "Techniques for emotion detection and content delivery" February 25, 2014, https://patents.google.com/patent/US20150242679A1/en

[18] Yaniv Taigman, Ming Yang, Marc' Aurelio Ranzato, Lior Wolf, "DeepFace: Closing the Gap to Human Level Performance in Face Verification," Facebook research, June 24, 2014 https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

[19] Jessica Gabel Cino, "Facial recognition is increasingly common, but how does it work?" *The Conversation,* April 4 2017, http://theconversation.com/facial-recognition-is-increasingly-common-but-how-does-it-work-61354

[20] Yaniv Taigman, "Web-Scale Training for Face Identification," Facebook AI research, http://www.cs.tau.ac.il/~wolf/deeplearningmeeting/pdfs/deepface_masterclass.pdf

[21] Yaniv Taigman, Ming Yang, Marc' Aurelio Ranzato, Lior Wolf, "DeepFace: Closing the Gap to Human Level Performance in Face Verification," Facebook research, June 24, 2014 https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

Users can always turn off facial recognition tools if they are uncomfortable with the technology, Facebook says. Privacy advocates, however, find that argument unconvincing. If those users were automatically enrolled in a facial recognition database, could they really have given their consent in the first place?

Biometric data is inherently more sensitive than other forms of data. When other identifiers such as social security numbers or account passwords are compromised in a data breach or cases of identity theft, the victims have recourse. People can always change a social security number or select a new password to prevent this information from misuse. Changing the physical structure of one's face is a more difficult task.

Facial recognition can also be used on individuals without their knowledge, whereas most other forms of data collection typically require some action from the user. Data created by Facebook activity, for example, is only created when users like posts or pages. Data is similarly created when users click ads on Google search results or visit certain web pages. Even other forms of biometric data require the user to actively participate in the data collection process. Retina and fingerprint scans, for example, can only be done at proximity with cooperation from the subject.

Facial recognition is different. It can be done from afar and work on large crowds. Security cameras equipped with facial recognition software can scan and identify faces serendipitously, without the knowledge or consent of subjects. The development of facial recognition has transformed the way we think about data collection and privacy because of how little it requires from the user and how discreetly it can be deployed.

Facebook's own facial recognition tool was built with data from photographs most users did not know were being parsed for facial data. This information gap is one of the main criticisms levied on Facebook's use of facial recognition. Facebook users believe they are uploading images to share with friends and family and are likely unaware that these images are used to train a facial recognition tool and to develop proprietary faceprints for Facebook to add to its database. Should companies be required to obtain consent from users to include faceprints in a facial database? Because of the sensitive, personal nature of facial recognition, privacy advocates argue that the technology should be subject to a higher standard when it comes to the issue of consent.

Ensuring the public is informed and approving of companies' use of facial recognition is in the industry's best interest, researchers at the National Academy of Sciences have said. "The success of large-scale or public biometric systems is dependent on gaining broad public acceptance of their validity. To achieve this goal, the risks and benefits of using such a system must be clearly presented. Public fears about using the system, including . . . concerns about theft or misuse of information, should be addressed," the academy wrote in 2010.[22]

In filings with the Securities and Exchange Commission, however, Facebook makes a different argument regarding consent. The filing reads, "regulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices could adversely affect user growth and engagement."[23] Companies have a financial and technological incentive to be "data maximalists," gathering as much user data as possible. Any action which might make users think twice about sharing certain forms of data could undermine this goal.

---

[22] "Biometric Recognition: Challenges and Opportunities," National Academy of Sciences, September 2010, http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059722.pdf

[23] Facebook Inc Form 10-k filed with the Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/1326801/000132680117000007/fb-12312016x10k.htm

This dichotomy has made the introduction of facial recognition for commercial use controversial and the process of finding common ground between proprietors and privacy advocates difficult. The National Telecommunications Information Administration brought together stakeholders in 2015 from the technology industry and privacy communities to discuss potential regulation and best practices for the use of facial recognition. Nine privacy groups walked away from the talks after 16 months of negotiation because it became clear, the groups say, that companies including Facebook "wouldn't even agree to the most modest measures to protect privacy" like obtaining opt-in consent before deploying facial recognition on users.[24]

III. The privacy implications of facial recognition

Facial recognition demands rigorous consent procedures because of its potential to threaten or violate people's privacy.

A violation of privacy doesn't necessarily involve the gathering of potentially incriminating or embarrassing information, according to **Daniel J. Solove**, a researcher and privacy law professor at George Washington University Law School. Instead, privacy is harmed when information about an individual is used in ways that could manipulate or alter the individual's behavior. "A privacy problem occurs when an activity by a person, business, or government entity creates harm by disrupting valuable activities of others," Solove writes.[25] "These harms need not be physical or emotional; they can occur by chilling socially beneficial behavior (for example, free speech and association) or by leading to power imbalances that adversely affect social structure (for example, excessive executive power)."

Facial recognition can create such power imbalances and significantly alter the behavior of its subjects. The technology's relationship to surveillance carries implications for social control and civil liberties, while the asymmetrical nature of its use — subjects of facial recognition may have no idea their data is colle cted or how it is used — can lead to further abuses once that information is processed.

Civil liberties

Facial recognition data is perhaps most widely used in the public sector by government and law enforcement agencies, as a 2016 study by The Georgetown Law Center on Privacy and Technology illustrates. The study, aptly titled "The Perpetual Lineup," points to one Federal Bureau of Investigation database containing 117 million facial records on American Adults compiled from the State Department and local DMVs, totaling about 48 percent of the adult American population.[26] The report goes on to discuss the lack of accountability and transparency associated with these tools. Few agencies monitor use of the technology, have a publicly available privacy policy, or even require the algorithm to meet an accuracy threshold.[27]

---

[24] Jennifer Lynch, "EFF and Eight Other Privacy Organizations Back Out of NTIA Face Recognition Multi-Stakeholder Process," Electronic Frontier Foundation, June 16, 2015, https://www.eff.org/deeplinks/2015/06/eff-and-eight-other-privacy-organizations-back-out-ntia-face-recognition-multi

[25] Daniel J. Solove, "'I've Got Nothing to Hide' and other Misunderstandings of Privacy," San Diego Law Review, Vol. 44, 2007, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

[26] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, "The Perpetual Lineup," Georgetown Law Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/

[27] Ibid

The U.S. Constitution enshrines the right of American citizens "peaceably to assemble, and to petition the Government for a redress of grievances." Facial recognition technology, with its potential to track and monitor subjects without their knowledge, gives pause to privacy advocates and politicians alike because of its potential to infringe this right. In 2017, Jason Chaffetz, at the time a Republican Congressman representing Utah, convened a hearing of the House Committee on Oversight and Government Reform to discuss law enforcement's use of facial recognition technology. Chaffetz said that facial recognition has its benefits, but "can be used in a way that chills free speech and free association by targeting people attending certain political meetings, protests, churches or other types of places in public."[28]

Facial recognition surveillance has already been used in ways that make civil libertarians shudder. Police in Baltimore used the technology during the 2015 protests that followed the death of Freddie Gray while in police custody. During the unrest that followed, law enforcement agencies used information from Geofeedia, a social media monitoring tool, to monitor and track protesters and ran social media images through a facial recognition database to find participants with outstanding warrants.[29]

Both the FBI and the Department of Homeland Security have acknowledged the potential chilling effect facial recognition could impose on the exercise of free speech, but Georgetown's Center on Privacy and Technology found that "almost none of the agencies using face recognition have adopted express prohibitions against using the technology to track political or other First Amendment activity."[30]

Training material from the Department of Justice instructs investigators to use information from social media to help reveal vast amounts of information about subjects, including associates and location information. The material includes a screenshot of the Facebook photo tagging process.[31]

Many local law enforcement agencies have contracts with private companies to deploy their facial recognition efforts. One such example is Amazon's facial detection product, Rekognition, which makes use of a database featuring tens of millions of faces[32] and can recognize up to 100 faces in an image. It works on video and offers a feature called "people tracking" which identifies and follow a face throughout a video.[33]

The ACLU says Rekognition's ability to "identify persons of interest" raises "the possibility that those labeled suspicious by governments — such as undocumented immigrants or black activists — will be seen as fair game for Rekognition surveillance."[34] Amazon has partnerships to deploy Rekognition with Orlando, Florida and Washington County Sheriff's Office in Oregon. In neither city could the ACLU find evidence that the public was informed or provided the opportunity to consent of the use of facial recognition.

---

[28] Video of the House Committee on Oversight and Government Reform hearing available here: https://oversight.house.gov/hearing/law-enforcements-use-facial-recognition-technology/

[29] Jessica Guynn, "ACLU: Police used Twitter, Facebook to track protests," *USA Today,* October 11, 2016, https://www.usatoday.com/story/tech/news/2016/10/11/aclu-police-used-twitter-facebook-data-track-protesters-baltimore-ferguson/91897034/

[30] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, "The Perpetual Lineup," Georgetown Law Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/

[31] Training material obtained by the Electronic Frontier Foundation available here: https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf

[32] Ranju Das, "Amazon Rekognition Announces Real-Time Face Recognition, Support for Recognition of Text in Image, and Improved Face Detection," AWS Machine Learning Blog, November 21, 2017, https://aws.amazon.com/blogs/machine-learning/amazon-rekognition-announces-real-time-face-recognition-support-for-recognition-of-text-in-image-and-improved-face-detection/

[33] Amazon Rekognition FAQs: https://aws.amazon.com/rekognition/faqs/#Video_Analytics

[34] Matt Cagle, "Amazon Teams Up With Law Enforcement to Deploy Dangerous New Face Recognition Technology," ACLU Northern California, May 22, 2018, https://www.aclunc.org/blog/amazon-teams-law-enforcement-deploy-dangerous-new-face-recognition-technology

This news drew criticism from the Congressional Black Caucus. "It is quite clear that communities of color are more heavily and aggressively policed than white communities," the caucus wrote in a letter to Amazon CEO Jeff Bezos. "We are seriously concerned that wrong decisions will be made due to the skewed data set produced by what we view as unfair and, at times, unconstitutional policing practices."[35] The letter urges Bezos to proceed with caution when developing facial recognition.

In another infamous example, researchers at Stanford's Graduate School of Business reported they could use facial recognition to predict sexual orientation of subjects[36] when shown a photograph from a dating site. Even though many were skeptical of the study's conclusions, reactions surfaced new questions about the ways that facial recognition could be deployed to identify, label, or act on intimate aspects of our life.[37]

Social control

In his book *Discipline and Punish,* French intellectual Michel Foucault describes a "panopticon" in which information about the daily lives of the observed is gathered indiscriminately. That information is then funneled behind a shadowy curtain where the information is used to pull levers of power inaccessible by the observed. Knowing they could be observed at all times, the observed police their own actions and alter their lives to avoid drawing attention. But the flow of information travels in one direction. The observed is "the object of information, never a subject in communication," Foucault says.

It's not difficult to see traces of the panopticon – and the associated implications for power and social control – in modern life. Research has shown that excessive police surveillance of Muslim communities in New York City and New Jersey in the years after 9/11 had a chilling effect on activities otherwise protected by the First Amendment.[38] The subjects of surveillance were less likely to attend mosques they thought were under government surveillance or to practice religion in public.

Technology makes such constant observation possible. Data gleaned from online activities, physical location,[39] or even home appliances,[40] can go on to inform what ads we see or impact other sensitive spheres of our lives.[41] Though we are used to being tracked online, facial recognition allows us to be tracked in the real world in real time, following us even into situations where we would expect some level of anonymity.

---

[35] The text of the May, 24, 2018 letter from the Congressional Black Caucus is here: https://cbc.house.gov/news/documentsingle.aspx?DocumentID=898

[36] Yilun Wang, Michal Kosinski, "Deep Neural Networks are more accurate than humans at Detecting Sexual Orientation from Facial Images," Journal of Personality and Social Psychology, 2017, https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/wang_kosinski.pdf

[37] Heather Murphy, "Why Stanford Researchers Tried to Create a 'Gaydar' Machine," *The New York Times*, October 9, 2017, https://www.nytimes.com/2017/10/09/science/stanford-sexual-orientation-study.html

[38] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, https://www.eff.org/wp/law-enforcement-use-face-recognition

[39] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 10, 2018 https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[40] Maggie Astor, "Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared," *The New York Times*, May 25, 2017, https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html

[41] Report by Upturn, "Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace," October 29, 2014, https://www.upturn.org/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf

China's government is looking to create a database containing facial records of all Chinese citizens for use by national and local authorities.[42] The database will tap into a surveillance network of more than 170 million cameras controlled by China's largest, government-owned television broadcaster, CCTV,[43] and expand the deployment of facial recognition glasses, which law enforcement officers use to surveil citizens in ways that fixed cameras cannot.[44] In April 2018, Chinese police were able to locate, identify, and arrest a wanted suspect among a crowd of 60,000 people at a concert using facial recognition. According to the Wall Street Journal, the Chinese Ministry of Public Security, China's national police force, "called for the creation of an 'omnipresent, completely connected, always on and fully controllable' nationwide video-surveillance network as a public-safety imperative."[45] The technology may also be used to realize China's vision for a "citizen score" which assigns every citizen a grade based on data from social media, websites visited and other inputs.[46]

Individuals often participate in protests or other demonstrations with the understanding that they will be one of many faces in the crowd. Is it possible that facial recognition products developed for other contexts could be used in ways that challenge this assumption? **Alvaro Bedoya** suggests they might. After all, a company like Facebook regularly provides personal information on its users when requested by law enforcement agencies.[47] "A lot of people participate in protests these days," explained Bedoya, the executive director of the Center on Privacy and Technology. "If I'm a government official and I want a list of people who attended this event, what's stopping me from saying 'give me all the automatic tags that you found in the faces at this protest" using facial recognition?

A panoply of private companies have begun to harness the power of facial recognition for use in other unexpected settings as well. One company, Face-Six LLC, has developed a technology called Churchix, which is designed to track attendance and participation at churches and schools. Churchix works when customers upload photos of their members, or students in a classroom setting, and in this way identifies the individuals the customer wants Churchix to track.[48]

Reliability

Privacy and trust can be violated even after data is gathered in a consensual manner. In the case of facial recognition, the technology may be inaccurate or unreliable and lead to dubious conclusions. The FBI's facial recognition database reports its system is "incapable of accurate identification at least 15 percent of the time."[49] Like all forms of facial recognition, the tool is less accurate when recognizing faces in images with different backgrounds or lighting, or when identifying someone in a video or low-resolution image.

The FBI avoids assigning responsibility for the accuracy of its tool by classifying the list of potential matches as "investigative leads" rather than positive identification of subjects. The FBI only ensures that the "candidate will be returned in the top 50 candidates" 85 percent of the time "when the true candidate exists in the gallery."[50]

---

[42] Stephen Chen, "China to build giant facial recognition database," *South China Morning Post*, October 12, 2017, https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any

[43] "Chinese man caught by facial recognition at pop concert," *BBC News*, April 13, 2018, https://www.bbc.com/news/world-asia-china-43751276

[44] Shannon Liao, "Chinese police are expanding facial recognition sunglasses program," *The Verge*, March 12, 2018, https://www.theverge.com/2018/3/12/17110636/china-police-facial-recognition-sunglasses-surveillance

[45] Josh Chin, Liza Lin, "China's All Seeing Surveillance State Is Reading Its' Citizens Faces", *The Wall Street Journal,* June 26, 2017, *https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020*

[46] Mariel Meyers, "China turns to tech to monitor, shame and rate citizens," *CNET News*, April 25, 2018 https://www.cnet.com/news/china-turns-to-tech-to-monitor-shame-and-rate-citizens/

[47] "Information for Law Enforcement Authorities," Facebook, https://www.facebook.com/safety/groups/law/guidelines/

[48] More information on Churchix here: https://churchix.com/

[49] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, https://www.eff.org/wp/law-enforcement-use-face-recognition

[50] Ibid

Facial recognition technology is known to be less accurate when identifying people of certain races and gender. Researchers at the MIT Media Lab, led by Joy Buolamwini, an African-American computer scientist, found that facial recognition systems used by major companies were up to 35 percent less accurate for dark-skinned women than light-skinned men ("Microsoft's error rate for darker-skinned women was 21 percent, while IBM's and Megvii's rates were nearly 35 percent.").[51] The concern is not merely about the accuracy of the tools, but the questions of fairness and justice that such disparate results can raise when deployed in the real world.

Buolamwini's findings serve to reinforce the fact that the performance of facial recognition strongly depends on the data on which it is trained. Disproportionate arrest rates associated with African American males result in that population being overrepresented in mugshot databases, and the likelihood for false positives, when a facial recognition tool falsely identifies a face, is therefore much higher. The Seattle Police Department's claim that its facial recognition technology "does not see race,"[52] belies a fundamental misunderstanding of the technology used to find criminal suspects.

Ulterior uses

Any data that is collected and stored is subject to breach and misuse. Facial recognition data is no exception.

In 2013, the National Security Agency's Inspector General revealed that agency workers had used surveillance records to spy on spouses and romantic partners.[53] And in 2015, sensitive data stored in databases maintained by the Office of Personnel Management was stolen, including records on biometric information, financial history, and addresses of more than 25 million people.[54] The Government Accountability Office called out the FBI itself in 2007 for its weaknesses in data security.[55]

Private companies have also faced challenges by not disclosing how the data they collect (or of which they facilitate collection) will be used and by whom. For example, Apple initially allowed third-party app developers access to some of its facial recognition data without users' consent. After scrutiny, Apple said it would require third-party developers to publish a privacy policy in order to access this data, but privacy experts still harbor concerns that bad actors will find loopholes or that Apple will be unable to police who is tapping into the data.[56] Google also allows app developers to use the Android face camera for advertising and creating facial databases with users' consent.[57]

---

[51] Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *The New York Times*, February 8, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[52] Clare Garvie, Alvaro Bedoya, Jonathan Frankle, "The Perpetual Lineup", Georgetown Law Center on Privacy & Technology, October 18, 2016, https://www.perpetuallineup.org/

[53] Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology," Electronic Frontier Foundation, February 12, 2018, https://www.eff.org/wp/law-enforcement-use-face-recognition

[54] Ibid.

[55] Government Accountability Office, "FBI Needs to Address Weaknesses in Critical Network," April 30, 2007,https://www.gao.gov/products/GAO-07-368

[56] Geoffrey A. Fowler, "Apple is sharing your face with apps. That's a new privacy worry," November 30, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/11/30/apple-is-sharing-your-face-with-apps-thats-a-new-privacy-worry

[57] Ibid

IV. Facebook's trouble with facial recognition

Critics scrutinized Facebook's use of facial recognition from the very start. Facebook announced in 2012 it was purchasing the Israeli firm Face.com "to help provide the best photo experience" for Facebook users, a spokesperson said at the time.[58] Right away, privacy advocates had questions for the company. The announcement led then-Senator **Al Franken**, Democrat from Minnesota, to hold a hearing of the Senate Judiciary Committee's Subcommittee on Privacy Technology and the Law to discuss Facebook's forays into facial recognition.

Franken noted that users had to go through six pages of privacy settings before the stumbling upon the words "facial recognition." (See Exhibit 3). He confronted Facebook's then-Privacy and Policy manager Rob Sherman about the opt-out nature of Facebook's facial recognition technology. Franken said:

"I think this information is so sensitive that it's the kind of thing users have to consciously opt themselves into … How can users make an informed decision about facial recognition in their privacy settings if you don't actually tell them that you are using facial recognition?"[59]

Sherman responded by saying that "Facebook is an opt-in experience."

"People choose to be on Facebook because they want to share with each other," Sherman said. "We think that it's the right choice to let people who are uncomfortable with it to decide to opt-out."

Franken also asked Sherman if Facebook would ever sell the faceprints it has developed to third parties. Sherman was unable to answer this question.

"It's difficult to know what Facebook will look like five or 10 years down the line, so it's hard to respond to that," he said.[60]

Facebook Chief Privacy Officer Erin Egan echoed that uncertainty in 2013 when she told Reuters: "Can I say that we will never use facial recognition technology for any other purposes [other than suggesting who to tag in photos]? Absolutely not.[61]"

Facebook filed two patents in December 2017 that provide clues as to how the company plans to use facial recognition in the future. These patents are titled "Facial Recognition Identification for In-Store Payment Transactions" and "Using Facial Recognition and Facial Expression Detection to Analyze In-Store Activity of a User" and describe tools brick-and-mortar stores can use to process payments and to determine when a customer may need assistance based on their facial expressions.[62]

The company was seemingly caught off guard by the public criticism of its facial recognition practices. Facebook offered an apology for the muddled introduction of facial recognition. "We should have been more clear during the roll-out process when this became available" to users, Facebook said in a blog post that has since been removed.[63] Facebook suspended Tag Suggestions

---

[58] Bianca Bosker, "Facebook Buys Facial Recognition Firm Face.com: What It Wants With Your Face", *HuffPost*, June 19, 2012, https://www.huffingtonpost.com/2012/06/19/facebook-buys-face-com_n_1608996.html

59 Hearing transcript available here: https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf

[60] Jared Bennett, "Saving Face: Facebook Wants Access Without Limits," The Center for Public Integrity, July 31, 2017, https://www.publicintegrity.org/2017/07/31/21027/saving-face-facebook-wants-access-without-limits

[61] Ibid

[62] Facebook's patent filing is available here: http://www.freshpatents.com/-dt20171109ptan20170323299.php. More are described in the EPIC complaint here: https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf

[63] EPIC complaint before the Federal Trade Commission filed April 6,2018, https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf

later in 2012 and re-launched the program in 2013 with a Facebook post which said the company had made "improvements to the tool's efficiency." When the company re-launched facial recognition it did so on a default opt-out basis, without making significant changes to the consent process.[64]

Facebook began another overhaul of its facial recognition practices in late 2017. The company explained the tool's usefulness as a security measure. Facial recognition can be used to notify users when they appear in images or videos they aren't tagged in and can help find fraudulent accounts that impersonate other Facebook users. Facebook also added the disclaimer that the tool is not available in certain areas and is turned off for individuals under the age of 18. The company also introduced a simplified way to opt-out of its facial recognition tools with a single on/off switch.[65]

As part of Facebook's "Hard Questions" series, Sherman explained these changes to its facial recognition policies and wrote, "when we first introduced this feature in 2010, there was no industry standard for how people should be able to control face recognition. We decided to notify people on Facebook and provide a way to disable it in their account settings at any time." Sherman asserted that Facebook worked for over a year to develop the best policies for facial recognition based on feedback from users and made clear that Facebook has no plans to develop facial recognition features that would "tell strangers who you are."[66]

Hard questions from elected officials can be embarrassing, but a potentially more damaging accusation was made in April 2018 by the privacy advocacy group Electronic Privacy and Information Center (EPIC).

In 2011, Facebook settled allegations that it misled users regarding their privacy settings by entering a consent decree with the Federal Trade Commission (FTC).[67] The decree ordered that Facebook "take several steps to make sure it lives up to its promises in the future, including giving consumers clear and prominent notice and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established.[68] Potential penalties for violating the order could climb to $40,000 per violation per day.

EPIC alleged in a complaint to the Federal Trade Commission that Facebook violated the 2011 agreement with the FTC by making changes to its facial recognition practices that "exposed users' covered information in a way that materially exceeded the restrictions imposed by their privacy settings. Moreover, Facebook did not provide users with clear and prominent notice nor obtain their affirmative express consent before enacting these changes."[69]

In its complaint to the FTC, EPIC noted that Facebook's new 2018 facial recognition practices "notifies users when their biometric face print is detected on an image, even if it has not been tagged by another user." This is problematic, EPIC says, because it "derives biometric data from Facebook users

---

[64] Emil Protalinski, "Facebook re-enables Tag Suggestions facial-recognition feature in the US, on by default for all" *The Next Web*, February, 1, 2013, https://thenextweb.com/facebook/2013/02/01/facebook-re-enables-tag-suggestions-facial-recognition-feature-in-the-us-on-by-default-for-all/ and Appendix 13

[65] Joaquin Quiñonero Candela, "Managing Your Identity on Facebook With Face Recognition Technology", Facebook newsroom, December 19, 2017, https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/

[66] Rob Sherman, "Hard Questions: Should I Be Afraid of Face Recognition Technology?" Facebook Newsroom, December 19, 2017 https://newsroom.fb.com/news/2017/12/hard-questions-should-i-be-afraid-of-face-recognition-technology/

[67] Federal Trade Commission press release: https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

68 Ibid

[69] EPIC complaint before the Federal Trade Commission filed April 6,2018, https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf

in a materially different manner than Facebook represented when they first collected the data using Tag Suggestions."[70]

The process of opting out of facial recognition on Facebook is still unclear, EPIC agues in its complaint. The company does not present a clearly labeled "opt-out button" but rather links to the privacy settings page, where users must find and change the settings for facial recognition on their own. What's more, many people are still unaware that Tag Suggestions is based on facial recognition technology that carries major implications for privacy, EPIC says: "Tag Suggestions dates back five years. Many users remain unaware that Tag Suggestions applied to them by default in 2013, and that there is a choice to opt-out."[71]

The lawsuit

This dispute came to a head in 2015, when a class action lawsuit was filed against Facebook in state court in Illinois, alleging the company "secretly amassed the world's largest privately held database of consumer biometrics data" without informing users or offering the chance for consent. The case, *Licata vs Facebook,* has emerged as a flash point for facial recognition technology with major implications for privacy and data collection. The consequences could be immense — an award of up to $5,000 to every Facebook user in Illinois who fits the class description.[72]

Carlos Licata created his Facebook account in 2009 but it wasn't until 2015 that he realized Facebook was collecting data he never planned on sharing with the company: the geometry of his face.

Licata never gave Facebook permission to collect his faceprint template and add it to the facial database the company had been building behind the scenes. He felt his privacy had been violated.

But unlike most Facebook users, Licata had recourse in the form of what was at the time an obscure data privacy law. The Illinois state legislature passed a one-of-a-kind biometric privacy law called the Biometric Information and Privacy Act (BIPA) in 2008.

BIPA requires companies that collect biometric data to obtain written consent before gathering data from users and to provide clear, specific policy guidelines that lay out what the data will be used for and for how long it will be held. (See Exhibit 5 for the full text of BIPA.)

Licata filed a lawsuit with representation by Edelson PC, a controversial law firm that has played a major, if niche, role in using privacy laws to put a check on technology companies' collection and use of data. The lawsuit claims that Facebook "actively conceals from its users that its Tag Suggestions feature actually uses proprietary facial recognition software to scan their uploaded photos." The complaint goes on to note that "Facebook doesn't disclose its wholesale biometrics data collection practices in its privacy policies, nor does it even ask users to acknowledge them."[73]

Facebook attempted to have the case thrown out, claiming that Licata and two other named plaintiffs had lack of standing because the collection of biometric data presented no real-world harm to users. U.S. District Judge James Donato disagreed, explaining that "Facebook insists that the collection of biometric information without notice or consent can never support Article III standing without 'real-world harms' such as adverse employment impacts or even just 'anxiety.' That contention exceeds

[70] Ibid

[71] Ibid

[72] Licata v Facebook complaint available on Document Cloud: https://www.documentcloud.org/documents/3553107-Facebookamendedcompt.html

[73] Licata v Facebook complaint available on Document Cloud: https://www.documentcloud.org/documents/3553107-Facebookamendedcompt.html

the law."[74] Judge Donato argued that the alleged violation of privacy was enough to allow class participants to sue.

As recently as April 2018, Facebook's lawyers have denied the claims of the Licata lawsuit and said they will defend the company vigorously.[75]

Other companies have been subject to similar lawsuits, including Snapchat,[76] Google and Shutterfly.[77] Google's Arts and Culture app contains a feature that runs facial recognition software on headshots users take with their cell phone cameras to find a work of art that matches the user's face. The feature was wildly popular, but Google turned this function off in Illinois and Texas for fear of running afoul of BIPA.[78]

The law

The Illinois State Legislature passed BIPA in 2008, the year before Licata created his Facebook account. The law requires companies to inform users, in writing, of the biometric identifiers they collect and for how long they will store that data. BIPA also mandates that companies obtain written consent from users before collecting and storing such data. BIPA defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry,"[79] and includes a private right of action, meaning any resident of the state of Illinois can sue companies for privacy violations under BIPA.

BIPA passed in 2008 after a fingerprint scanning company operating in Illinois went bankrupt and floated the idea of selling its database of fingerprints to pay off creditors. The company, Pay by Touch, allowed customers to link credit cards and bank accounts and to pay for purchases at select grocery stores and gas stations by scanning their fingerprints. This spooked lawmakers concerned with what would happen to sensitive data customers had entrusted to Pay by Touch. BIPA was drafted with the help of the Illinois chapter of the American Civil Liberties Union and passed in 2008.[80] When BIPA first passed, it did so without significant corporate opposition.[81]

According to Chad Marlow, advocacy and policy counsel at the ACLU, Illinois' BIPA sets a fair and effective example of biometric data regulation. "The Illinois law is a very stringent law. But it's not an inherently unreasonable law. Illinois wanted to protect its citizens from facial recognition technologies online."[82]

---

[74] EPIC complaint before the Federal Trade Commission filed April 6,2018, https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf

[75] Ally Marotti, "Facebook could be forced to pay billions of dollars over alleged violations of Illinois biometrics law," *The Chicago Tribune*, April 17, 2018 http://www.chicagotribune.com/business/ct-biz-facebook-tagging-privacy-lawsuit-20180417-story.html

[76] "Illinois Residents Sue Snapchat Over Face-Scanning Technology" NBC 5 Chicago, July 25, 2016, https://www.nbcchicago.com/news/local/illinois-residents-sue-snapchat-388133992.html

[77] Justin O. Kay, "The Illinois Biometric Information Privacy Act" Drinker Biddle & Reath, LLP, http://www.acc.com/chapters/chic/upload/Drinker-Biddle-2017-1-BIPA-Article.pdf

[78] Jeffrey Neuburger, "Google App Disables Art-Selfie Biometric Comparison Tool in Illinois and Texas," *New Media and Technology Law Blog*, January 18, 2018, https://newmedialaw.proskauer.com/2018/01/18/google-app-disables-art-selfie-biometric-comparison-tool-in-illinois-and-texas/

[79] Biometric Information Privacy Act: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

[80] Dune Lawrence, "Do you own your own Faceprints?" *Bloomberg Businessweek*, July 7, 2016, https://www.bloomberg.com/news/articles/2016-07-07/do-you-own-your-own-fingerprints

[81] Ben Sobel, "Commentary: Facial recognition tech is everywhere, but may be illegal," *The Washington Post*, June 11, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal

[82] Jared Bennett, "Saving Face: Facebook Wants Access Without Limits," The Center for Public Integrity, July 31, 2017, https://www.publicintegrity.org/2017/07/31/21027/saving-face-facebook-wants-access-without-limits

For the first few years of its existence BIPA went largely unnoticed. Since the *Licata* lawsuit, however, it has been under near constant scrutiny.

In 2016, Facebook lawyers argued the Licata case should be dismissed because BIPA only applies to physical, in-person scans of biometric data, not to photos or videos. The judge disagreed with Facebook's reading of BIPA, but just 21 days later an amendment to BIPA was filed in the state legislature that would have limited the law's scope to cover only in-person scans. The amendment was eventually withdrawn by the sponsor after backlash from public interest groups. Facebook expressed support but denied directly lobbying for the amendment.

Instead, sources told the Center for Public Integrity the amendment was championed by CompTIA, a trade group which represents technology and telecommunications companies. CompTIA told the Center for Public Integrity that Facebook was among its members, but Facebook doesn't list CompTIA among the groups it works with to advance its policy goals.[83]

CompTIA, among other associations representing technology companies, claims BIPA is unreasonable and leads to unnecessary lawsuits that could deprive people of the security and fraud prevention benefits that come with facial recognition. CompTIA published a blog post in 2016 explaining that BIPA was problematic due to its vagueness and unclear definitions for terms like "consent, what constitutes data for the purpose of profit, facial recognitions, etc."[84]

[Facebook's direct lobbying has increased in recent years. Since 2009, Facebook's lobbying spending has gone up fifty times. It is no coincidence that 2009 also marks the year the last major consumer privacy law passed through Congress. See Exhibit 4 for more data regarding the political activities of large tech companies.]

In April 2018, the same week Mark Zuckerberg told Congress his company recognized the need for special consent for tools like facial recognition, BIPA faced yet another amendment attempt. The amendment, which privacy advocates said would render BIPA unenforceable in many circumstances,[85] was supported by the Illinois Chamber of Commerce's Tech Council,[86] which includes Facebook as a dues paying member. Facebook has also made financial contributions to the campaigns of several the amendment's sponsors.[87]

During the early 2017 legislative session, seven states drafted new biometric privacy laws. Montana, Washington, Alaska, Connecticut, and New Hampshire all introduced bills to regulate biometric data and facial recognition. Only Washington's legislature was able to pass a bill, one privacy advocates say is drastically watered down from its original form. The law exempts biometric data pulled from photographs, video or audio recordings. This is similar to the carve out sought by CompTIA in Illinois and would effectively free Facebook from liability under the new law. (Excerpts from Washington's law and the proposed legislation in Montana are included as Exhibit 6 and Exhibit 7.)

---

[83] Facebook's policy on political engagement is found here: https://newsroom.fb.com/news/h/facebook-political-engagement/

[84] Elizabeth Hyman, "The Practical Applications of Biometrics: It is not just about Tom Cruise's Eyes," CompTIA, August 8, 2016, https://www.comptia.org/about-us/newsroom/blog/comptia-blog/2016/08/08/the-practical-applications-of-biometrics-it-is-not-just-about-tom-cruise-s-eyes

[85] A letter outlining the concerns of privacy groups to Illinois Senate Telecommunications and Information Technology Committee can be found here: https://consumerfed.org/wp-content/uploads/2018/04/public-interest-groups-oppose-amendment-to-BIPA.pdf

[86] Tyler Diers, Technology Council Newsletter, February 25, 2018, http://myemail.constantcontact.com/Technology-Council-Newsletter-.html?soid=1109152397846&aid=ddA4c7TeoaA

[87] Facebook contributions to sponsors found here https://illinoissunshine.org/contributions/4837124/ and here https://illinoissunshine.org/contributions/4812075/

Lobbyists from CompTIA and Facebook, among other technology companies, all played an active role in shaping Washington's biometric privacy law. The Electronic Frontier Foundation pulled its support for the law in 2016 after key changes weakened the law. The statute "appears to have been tailored to protect companies that are using facial recognition," EFF senior staff attorney Adam Schwartz said.

Most of the major tech companies supported Washington's law by the time it passed the legislature. Facebook did not. One of the law's sponsors, Democratic Representative Jeff Morris, told the Center for Public Integrity that Facebook objected to the inclusion of "behavioral biometrics" in its categories of protected data. Behavioral biometrics refers to data derived from how a person moves, their posture or gait in videos.

There is no federal law regulating how companies collect or use biometric data. The Government Accountability Office determined in 2015 that "the privacy issues that have been raised by facial recognition technology serve yet another example of the need to adapt federal privacy law to reflect new technologies."[88] The lack of attention to biometric privacy laws at the federal level has placed the burden on states to enact sensible privacy protections.

GDPR

The European Union (EU) has been more aggressive in policing consumer privacy issues than U.S. federal or state governments. The EU passed the General Data Protection Regulation (GDPR) in April 2016 after four years of debate. The GDPR went into effect in May 2018, applying to all companies that handle personal data of individuals in the EU[89] and carrying potential fines that can climb as high as 17 million euro for violations.[90]

The GDPR codifies a policy of "privacy by design" whereby safeguards against abuse of data are built into engineering process from the ground up, rather than appended to a product along the way.

Companies big and small are struggling to bring their technology into compliance with the sweeping new law. Facebook itself has asked users for explicit permission to use features like data from third party partners and the status of political, religious and relationship information found in user profiles[91] in the wake of the new law. The company announced it will ask permission from users to deploy facial recognition technology[92] as part of its compliance with the GDPR, but the issue is far from settled.

Back in 2012, when Facebook had just begun introducing facial recognition to its users, German and Irish privacy regulators put Facebook's facial recognition tools under a microscope. German investigators accused the company of "illegally compiling a huge database of members' photos without their consent."[93] The Office of the Data Protection Commissioner in Ireland completed an investigation of Facebook's compliance with European privacy laws, typically stricter than their American counterparts.

---

[88] "Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law," Government Accountability Office, July 30, 2015, https://www.gao.gov/products/GAO-15-621

[89] "What does the General Data Protection Regulation (GDPR) govern?" European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en

[90] Chris Foxx, "Google and Facebook accused of breaking GDPR laws," *BBC,* May 25, 2018, https://www.bbc.com/news/technology-44252327

[91] Erin Egan, "Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live," Facebook newsroom, April 17, 2018, https://newsroom.fb.com/news/2018/04/new-privacy-protections/

[92] Ibid

[93] Kevin J. O'Brien, "Germans Reopen Investigation on Facebook Privacy," *The New York Times*, August 12, 2015, https://www.nytimes.com/2012/08/16/technology/germans-reopen-facebook-privacy-inquiry.html

The data privacy commissioner in Hamburg, Germany ordered Facebook to destroy the faceprints it had gathered from European citizens and adjust its policy to obtain explicit consent from users before creating a file based on their facial data.[94] In response, Facebook shut facial recognition off throughout Europe in October 2012.

Now, Facebook has signaled to European regulators that it wants to bring facial recognition back to Europe and will ask users for permission before scanning their photos with facial recognition software.[95] But the situation becomes more complicated under the GDPR, which considers biometric data among the "special categories of personal data" requiring heightened justification and security to process.

Besides biometric data, other special category data include information about race or ethnicity, religious beliefs, political opinions, genetic and health data and information about sexual orientation. Data in these categories cannot be processed without explicit consent, with certain exceptions when the data collection would serve legally defined interests of the individual or society.[96]

Again, the issue of consent is a sticking point. The Irish Data Protection Commissioner says Facebook would need to obtain consent from every subject in a photo uploaded to Facebook to run facial recognition, not just the user uploading the image. "The Irish DPC is querying the technology around facial recognition and whether Facebook needs to scan all faces (i.e. those without consent as well) to use the facial recognition technology. The issue of compliance of this feature with GDPR is therefore not settled at this point" the commission said in a statement issued April 2018.[97]

One key component of the GDPR is the idea of *data minimization,* or limiting data collection to only what is needed to accomplish a task. Data needs to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed," according to Article 5 of the law.[98] Under this maxim, data collected for one purpose cannot be used for another without the consent of users and data should only be held for as long as necessary to complete the task at hand.[99]

Large companies like Facebook, Google and WhatsApp have already been subject of complaints filed by privacy groups in Europe. One such complaint raises issue with the "take it or leave it approach" to data collection where users must agree to the collection and use of their data for targeted advertising or simply not use the product or platform.[100] The GDPR prohibits the practice of requiring users to share broad categories of personal data as a condition of using a service. The privacy advocates who filed the initial complaint call this "forced consent" where access to the platform is contingent on consenting to data sharing that would otherwise be unnecessary.[101]

---

[94] Ibid

[95] Alex Hern, "Facebook to start asking permission for facial recognition in GDPR push," *The Guardian*, April 18, 2018, https://www.theguardian.com/technology/2018/apr/18/facebook-facial-recognition-gdpr-targeted-advertising

[96] Article 9 of the GDPR, "Processing of special categories of personal data" https://gdpr-info.eu/art-9-gdpr/

[97] Arjun Kharpal, "Facebook's facial recognition technology may not meet strict new EU data rules, a top watchdog says," *CNBC*, April 19, 2018, https://www.cnbc.com/2018/04/19/facebooks-facial-recognition-may-not-meet-gdpr-rules.html

[98] Article 5 of the GDPR, "Principles relating to processing of personal data" https://gdpr-info.eu/art-5-gdpr/

[99] Ibid

[100] Chris Foxx, "Google and Facebook accused of breaking GDPR laws," BBC, May 25, 2018, https://www.bbc.com/news/technology-44252327

[101] The full complaint is explained here: https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf

V. What's next for facial recognition

In 2014, artist Leonardo Selvaggio began selling prosthetic replicas (as well as a free paper version) of his own face. Selvaggio's idea was to flood facial recognition technology with his face, so that the people behind the masks could move about in public without fear of identification. "We don't believe you should be tracked just because you want to walk outside and you shouldn't have to hide either," the website for Selvaggio's project, called URME, reads. "Instead, use one of our products to present an alternative identity when in public."[102]

This idea echoes the main argument of a book entitled *Obfuscation* by privacy scholars **Finn Brunton and Helen Nissenbaum**, released in 2015 as "a user's guide for privacy and protest." Data collection has become so ubiquitous, Brunton and Nissenbaum argue, that it is not always possible to avoid being tracked online or in the physical world. And opting out of such tracking may not be worth the cost. As a result, the best approach to combatting pervasive digital surveillance, they argue, may instead be obfuscation, "the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects." Brunton and Nissenbaum describe methods of obfuscation whereby data is combined or changed to make it "more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable."[103]

Facial recognition is only one of the emerging technologies based on the collection of more and more personal data. Our location,[104] the strains of our voice,[105] even our nocturnal breathing patterns[106] can be turned into pieces of digitized humanity used to paint a surprisingly detailed picture of our lives. *Obfuscation* describes the ways individuals can take matters into their own hands to avoid such asymmetrical data collection, from donning masks in public to using online tools that flood data trackers with irrelevant information.

Individuals alone can't protect themselves from constant surveillance, however, and pervasive data collection is nearly a fact of life for most people. If individuals can no longer avoid exposing themselves to tools of data collection, architects of technology and policy can no longer avoid grappling with the ethical concerns to balance innovation with the right to certain standards of privacy.

This is no easy task. As the authors of *Obfuscation* explain, the priorities of individuals, for-profit companies and governments are often at odds when it comes to privacy. Companies have incentives to gather as much data as possible to either make available to advertisers or create a more granular understanding of their customer base and are unlikely to voluntarily restrict data collection. Governments rely on data to surveil or provide services to citizens and are slow to keep up with the fast pace of technological change.

---

[102] More information about URME Surveillance here: http://www.urmesurveillance.com/

[103] Finn Brunton, Helen Nissenbaum, "Obfuscation:
A User's Guide for Privacy and Protest" The MIT Press, September 2015, https://mitpress.mit.edu/books/obfuscation

[104] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times,* December 10, 2018 https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[105] Steve Lohr, John Markoff, "Computers Learn to Listen, and Some Talk Back," *The New York Times*, June 24, 2010, https://www.nytimes.com/2010/06/25/science/25voice.html

[106] Marshall Allen, "You Snooze, You Lose: Insurers Make The Old Adage Literally True," *ProPublica*, November 21, 2018, https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true

Engineers have a responsibility to build tools that are understood by the public and come with appropriate safeguards against invasions of privacy. Including principles of "privacy by design" as required by the GDPR and providing a robust disclosure of terms and services that allows users to understand just what data they are handing over can help companies avoid embarrassing headlines and losing the trust of users.

The future of facial recognition and other data collecting technologies will depend on answering an urgent set of questions: How can new technology be misused or used to target vulnerable communities? Do certain categories of data require special consent before collection? Can the varying priorities of individuals, companies and governments find balance when introducing new technology? As early facial recognition pioneer turned critic Joseph Atick warned the Center for Public Integrity, "there is such a thing as letting the genie out of the bottle."

Exhibit 1 - List of Facial Recognition use cases

Consumer products

- Apple's FaceID uses facial recognition to unlock newer models of the iPhones and iPad Pro. FaceID can also authorize payments with Apple Pay or made to the iTunes Store. Some Google devices have a similar tool called Trusted Face, but that capability has been disabled in newer models. Learn more: https://support.apple.com/en-us/HT208108
- Facial scanning technology developed by digital signage company Amscreen can tailor advertisements based on subjects age and gender. Learn more: https://www.bbc.com/news/technology-24803378
- Samsung SDS America and Diebold Nixdorf have introduced technology allowing bank customers to authenticate ATM transactions through facial recognition. Learn more: https://findbiometrics.com/atm-mobile-facial-recognition-406125/
- FaceFirst sells facial recognition tools retailers can use to identify and prevent shoplifters. Learn more: https://www.mcclatchydc.com/news/nation-world/national/article211455924.html
- At least one car company is replacing keys with facial recognition technology to unlock doors. Learn more: https://www.consumerreports.org/cars-driving/car-companies-show-off-face-recognition-and-high-tech-cockpit-features/

Homeland Security and public safety

- The New York State Department of Motor Vehicles says it has used facial recognition to identify "more than 21,000 possible cases of identity theft or fraud" since the capability was introduced in 2010. Learn more: https://www.governor.ny.gov/news/governor-cuomo-announces-major-facial-recognition-technology-milestone-21000-fraud-cases
- The U.S. has deployed facial recognition to Afghanistan and Iraq, where the U.S. military and local security forces use facial recognition to identify terrorist suspects. Learn more: https://www.nytimes.com/2011/07/14/world/asia/14identity.html
- The U.S. Department of Homeland Security uses facial recognition to help track down child predators. The technology can "correctly detect and recognize children's faces appearing in seized child exploitation imagery," DHS explained in a press release this year. Learn more: https://www.dhs.gov/science-and-technology/news/2018/03/06/snapshot-st-and-hsi-collaborate-technologies-save-children
- Indian officials reportedly identified 3,000 missing children in four days using facial recognition. Learn more: https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html
- Taylor Swift recently used facial recognition at the Rose Bowl stadium in Los Angeles to identify stalkers at a concert there. Learn more: https://www.rollingstone.com/culture/culture-lists/future-entertainment-technology-music-tv-movies-760659/facial-recognition-concert-security-760696/

Administration

- India's Aadhaar program assigns every citizen a biometric identity they can use to tap into resources like government benefits or access the financial system through banks. Aadhaar is not without its detractors, though. The system suffered a major data breach in 2017 and another in 2018 and has been challenged as unconstitutional in India's Supreme Court. Learn more: https://www.bloombergquint.com/aadhaar/2018/03/21/the-key-arguments-in-supreme-court-against-aadhaar
- JetBlue has partnered with technology company SITA to develop a check-in system based on facial recognition. Learn more: https://www.sita.aero/pressroom/news-releases/jetblue-and-cbp-biometric-boarding-trial-program-proves-success-of-sita-technology
- Stadiums can use FaceFirst to ID VIP customers or people banned from the arena. Learn more: https://www.facefirst.com/blog/facefirsts-face-recognition-system-for-sporting-events-is-making-news/
- Researchers have built facial recognition tools to detect genetic disorders like Down Syndrome. Learn more: http://www.ox.ac.uk/news/2014-06-24-computer-aided-diagnosis-rare-genetic-disorders-family-snaps
- Medical startup FDNA has developed Face2Gene, a mobile app that can match facial features with potential syndromes. Learn more: https://www.statnews.com/2017/04/10/facial-recognition-genetic-disorders/

Exhibit 2 - Facebook's facial recognition process

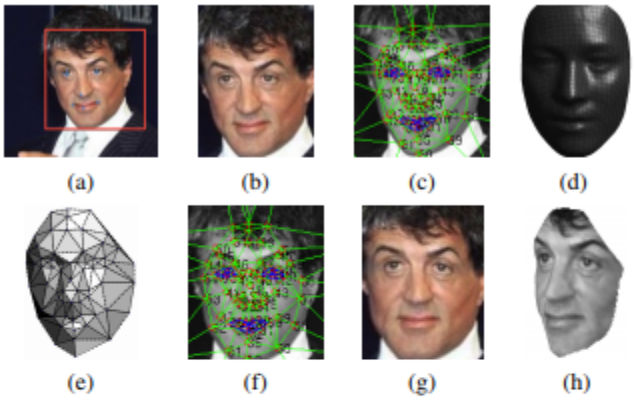


Figure 1. **Alignment pipeline.** (a) The detected face, with 6 initial fiducial points. (b) The induced 2D-aligned crop. (c) 67 fiducial points on the 2D-aligned crop with their corresponding Delaunay triangulation, we added triangles on the contour to avoid discontinuities. (d) The reference 3D shape transformed to the 2D-aligned crop image-plane. (e) Triangle visibility w.r.t. to the fitted 3D-2D camera; darker triangles are less visible. (f) The 67 fiducial points induced by the 3D model that are used to direct the piece-wise affine warpping. (g) The final frontalized crop. (h) A new view generated by the 3D model (not used in this paper).

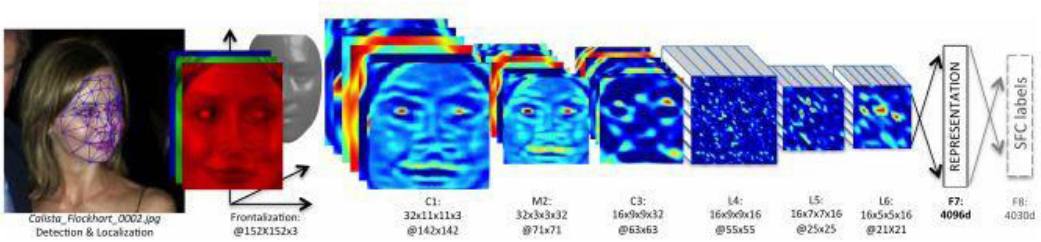
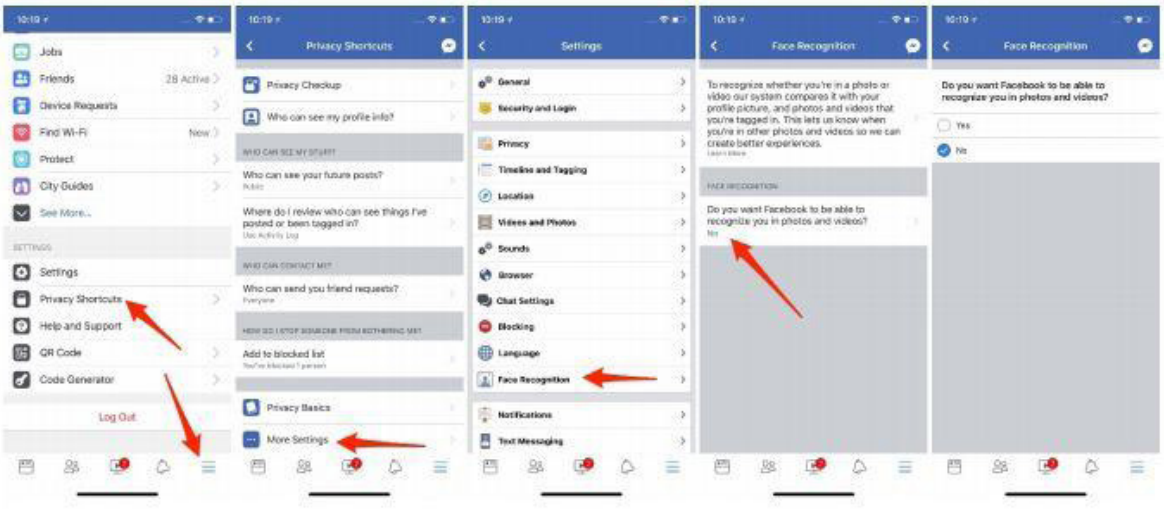


Figure 2. **Outline of the *DeepFace* architecture**. A front-end of a single convolution-pooling-convolution filtering on the rectified input, followed by three locally-connected layers and two fully-connected layers. Colors illustrate feature maps produced at each layer. The net includes more than 120 million parameters, where more than 95% come from the local and fully connected layers.

These illustrations are from "DeepFace: Closing the Gap to Human Level Performance in Face Verification", Facebook research, June 24, 2014 https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

Exhibit 3 - Multiple steps to facial recognition

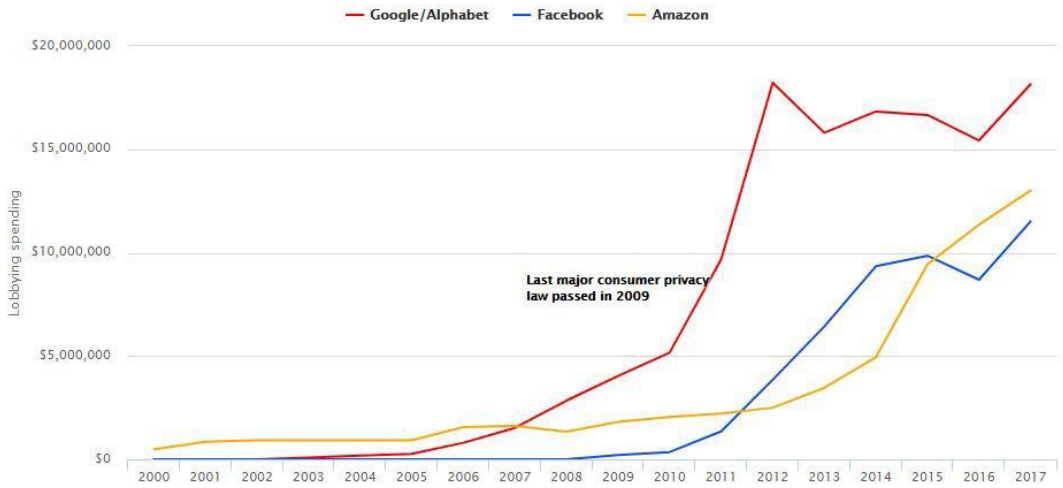


From https://epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf

Exhibit 4 - Lobbying and campaign contributions of tech companies

Facebook, Amazon and Alphabet lobbying

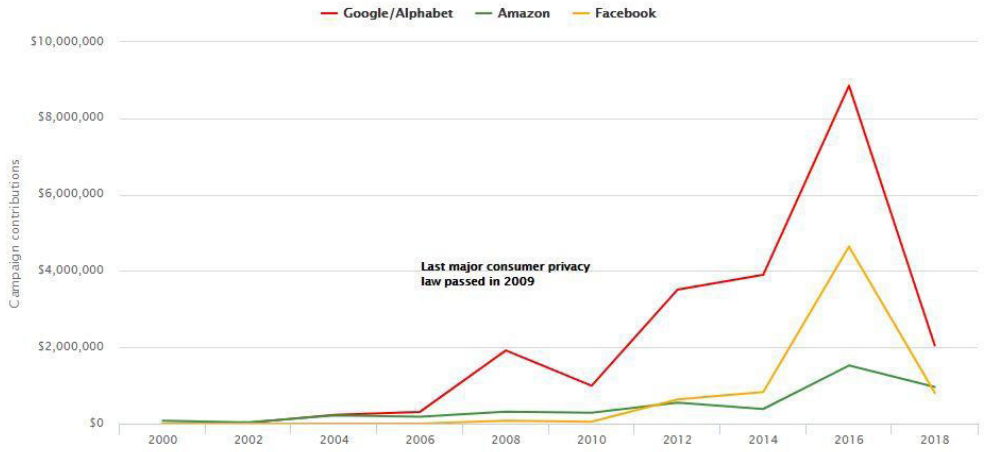
Lobbying spending by the top three internet companies.



Source: Center for Responsive Politics and Center for Public Integrity

Facebook, Amazon and Alphabet campaign contributions

Campaign contributions from employees and political action committees of three major internet companies since 2000. 2018 election cycle figures are based on data released March 29, 2018:



Source: Center for Responsive Politics and Center for Public Integrity

Facebook's state lobbying spending grows

State lobbying spending per year

	2010	2011	2012	2013	2014	2015	2016
Washington	$0	$0	$0	$0	$0	$0	$50,000
Florida	$0	$0	$0	$0	$0	$20,000	$55,000
Nebraska	$0	$0	$0	$0	$0	$54,950	$78,000
Texas	$0	$0	$0	$0	$0	$125,000	$50,001
Oregon	$0	$0	$0	$0	$41,240	$60,000	$0
Massachusetts	$0	$0	$0	$0	$60,000	$60,000	$0
Iowa	$0	$0	$0	$0	$60,000	$55,000	$60,000
New York	$0	$0	$40,000	$60,000	$68,000	$72,035	$148,000
California	$78,239	$176,850	$176,850	$191,099	$144,148	$158,432	$169,894

0 50k 100k 150k 200k

Source: National Institute on Money in State Politics

Exhibit 5 - The Illinois Biometric Information Privacy Act

(740 ILCS 14/) Biometric Information Privacy Act.

(740 ILCS 14/1)

Sec. 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/5)

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/10)

Sec. 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

(Source: P.A. 95-994, eff. 10-3-08.)

(740 ILCS 14/15)

Sec. 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or
biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
(2) the disclosure or redisclosure completes a
financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
(3) the disclosure or redisclosure is required by
State or federal law or municipal ordinance; or
(4) the disclosure is required pursuant to a valid
warrant or subpoena issued by a court of competent jurisdiction.
(e) A private entity in possession of a biometric identifier or biometric information shall:
(1) store, transmit, and protect from disclosure all
biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
(2) store, transmit, and protect from disclosure all
biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/20)
Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:
(1) against a private entity that negligently
violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
(2) against a private entity that intentionally or
recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
(3) reasonable attorneys' fees and costs, including
expert witness fees and other litigation expenses; and
(4) other relief, including an injunction, as the
State or federal court may deem appropriate.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/25)
Sec. 25. Construction.
(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.
(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.
(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.
(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.
(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.
(Source: P.A. 95-994, eff. 10-3-08.)
(740 ILCS 14/30)
Sec. 30. (Repealed).
(Source: P.A. 95-994, eff. 10-3-08. Repealed internally, eff. 1-1-09.)
(740 ILCS 14/99)
Sec. 99. Effective date. This Act takes effect upon becoming law.

(Source: P.A. 95-994, eff. 10-3-08.)

Exhibit 6 - An excerpt from Montana House Bill No 518

HOUSE BILL NO. 518

INTRODUCED BY N. MCCONNELL
A BILL FOR AN ACT ENTITLED: "AN ACT ESTABLISHING THE MONTANA BIOMETRIC INFORMATION PRIVACY ACT; PROHIBITING A PRIVATE ENTITY FROM COLLECTING, STORING, AND USING A PERSON'S BIOMETRIC DATA WITHOUT A PERSON'S CONSENT; ESTABLISHING PROCEDURES AND REQUIREMENTS FOR THE SALE, DISCLOSURE, PROTECTION, AND DISPOSAL OF BIOMETRIC INFORMATION; PROVIDING EXEMPTIONS; PROVIDING DEFINITIONS; CREATING A PRIVATE RIGHT OF ACTION AND ESTABLISHING PENALTIES; AND PROVIDING AN IMMEDIATE EFFECTIVE DATE."
BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. Section 1. Short title. [Sections 1 through 7] may be cited as the "Montana Biometric Information Privacy Act".
NEW SECTION. Section 2. Definitions. For purposes of [sections 1 through 7], the following definitions apply:
(1) (a) "Biometric data" means a biologic or behavioral characteristic that uniquely identifies and enables automated recognition of an individual, including but not limited to retina or iris scan, finger or palm print, voice recognition, hand or face geometry, facial imaging, facial recognition, gait recognition, vein recognition, or other
biologic or behavioral identifiers.
(b) The term does not include the following:
(i) written signature, demographic data, physical description, writing sample, tattoo description, or human biological sample used for valid scientific

screening or testing;
(ii) donated organ, tissue, blood, serum, or plasma stored on behalf of a potential recipient;
(iii) information captured from a patient in a health care setting or information collected and used for health care treatment, including an x-ray, MRI, PET scan, mammography, or other image of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing
or screening; or

(iv) a photograph or video, unless the photograph or video is collected, shared, or stored for use as a source of biometric data or for use as biometric information. A photograph or video that is used to aid a person who is blind or otherwise visually impaired is not biometric data for purposes of this subsection.

(2) "Biometric information" means any information based on a person's biometric data that is collected, stored, or used to identify an individual.
(3) (a) "Private entity" means any individual, partnership, corporation, limited liability company, association, or other group however organized.
(b) The term does not include a state or local governmental agency or a court, clerk of court, or a judge of a court in this state.
(4) "Writing" means a written or electronic communication that can be documented and is written in plain, easily understood language.

The rest of the introduced legislation can be found here: https://leg.mt.gov/bills/2017/BillPdf/HB0518.pdf

Exhibit 7 - Washington's Biometric Privacy Law

RCW 19.375.010

Definitions.
The definitions in this section apply throughout this chapter, unless the context clearly requires otherwise.
(1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. "Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.
(2) "Biometric system" means an automated identification system capable of capturing, processing, and storing a biometric identifier, comparing the biometric identifier to one or more references, and matching the biometric identifier to a specific individual.
(3) "Capture" means the process of collecting a biometric identifier from an individual.
(4) "Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. "Commercial purpose" does not include a security or law enforcement purpose.
(5) "Enroll" means to capture a biometric identifier of an individual, convert it into a reference template that cannot be reconstructed into the original output image, and store it in a database that matches the biometric identifier to a specific individual.
(6) "Law enforcement officer" means a law enforcement officer as defined in RCW 9.41.010 or a federal peace officer as defined in RCW 10.93.020.
(7) "Person" means an individual, partnership, corporation, limited liability company, organization, association, or any other legal or commercial entity, but does not include a government agency.
(8) "Security purpose" means the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value, including tangible and intangible goods, services, and other purposes in furtherance of protecting the security or integrity of software, accounts, applications, online services, or any person.

RCW 19.375.020
Enrollment, disclosure, and retention of biometric identifiers.
(1) A person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.
(2) Notice is a disclosure, that is not considered affirmative consent, that is given through a procedure reasonably designed to be readily available to affected individuals. The exact notice and type of consent required to achieve compliance with subsection (1) of this section is context-dependent.
(3) Unless consent has been obtained from the individual, a person who has enrolled an individual's biometric identifier may not sell, lease, or otherwise disclose the biometric identifier to another person for a commercial purpose unless the disclosure:
(a) Is consistent with subsections (1), (2), and (4) of this section;
(b) Is necessary to provide a product or service subscribed to, requested, or expressly authorized by the individual;
(c) Is necessary to effect, administer, enforce, or complete a financial transaction that the individual requested, initiated, or authorized, and the third party to whom the biometric identifier is disclosed maintains confidentiality of the biometric identifier and does not further disclose the biometric identifier except as otherwise permitted under this subsection (3);
(d) Is required or expressly authorized by a federal or state statute, or court order;
(e) Is made to a third party who contractually promises that the biometric identifier will not be further disclosed and will not be enrolled in a database for a commercial purpose inconsistent with the notice and consent described in this subsection (3) and subsections (1) and (2) of this section; or
(f) Is made to prepare for litigation or to respond to or participate in judicial process.
(4) A person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose:
(a) Must take reasonable care to guard against unauthorized access to and acquisition of biometric identifiers that are in the possession or under the control of the person; and
(b) May retain the biometric identifier no longer than is reasonably necessary to:
(i) Comply with a court order, statute, or public records retention schedule specified under federal, state, or local law;
(ii) Protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability; and
(iii) Provide the services for which the biometric identifier was enrolled.
(5) A person who enrolls a biometric identifier of an individual for a commercial purpose or obtains a biometric identifier of an individual from a third party for a commercial purpose pursuant to this section may not use or disclose it in a manner that is materially inconsistent with the terms under which the biometric identifier was originally provided without obtaining consent for the new terms of use or disclosure.
(6) The limitations on disclosure and retention of biometric identifiers provided in this section do not apply to disclosure or retention of biometric identifiers that have been unenrolled.
(7) Nothing in this section requires an entity to provide notice and obtain consent to collect, capture, or enroll a biometric identifier and store it in a biometric system, or otherwise, in furtherance of a security purpose.

The rest of the law can be found here: https://app.leg.wa.gov/RCW/default.aspx?cite=19.375r