Negative: Commercial Facial Recognition Privacy Act (S.847)

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan passes the Commercial Facial Recognition Privacy Act of 2019, a bill introduced into Congress but never enacted. It requires affirmative consent for many commercial applications of facial recognition to use someone’s picture. Note that it isn’t talking about law enforcement and it has a specific exclusion in the bill that says it does not apply to security cameras and loss prevention in stores.

Negative: Commercial Facial Recognition Privacy Act (S.847) 3

INHERENCY 3

1. State & Local initiatives are happening in Status Quo, and they’re better 3

States and cities are doing what CFRP is trying to do, with their own initiatives 3

Founders’ Criterion: Anyone with a plan should justify why the Federal government should do it, rather than the States 3

State action is better than federal: Experimentation among the states develops & spreads new and better ideas 3

2. Industry standards 4

Industry is developing self-regulatory standards on facial recognition and privacy 4

HARMS / SIGNIFICANCE 4

1. No clear definition of the “privacy” they’re trying to protect 4

We don’t agree on what is “private” and what is “public” any more. And you probably don’t know either 4

2. No impact 4

Facial recognition is so widespread that no one cares and no one has any reasonable expectation of privacy 5

Corporate facial recognition doesn’t violate any expectation of privacy 5

3. Hype & Exaggeration 5

Fear of facial recognition technology is just like past fears of technology that didn’t do any harm 5

SOLVENCY 6

1. “Security” loophole 6

AFF law specifically allows facial recognition for “security” purposes 6

Definition of “security application” 6

Impact: Drop any harms or advantages from the round involving security surveillance, because they can’t solve them 6

DISADVANTAGES 6

1. Creating the crime of offending someone – violates human rights 6

Link: The bill requires the facial recognition controller to guess what might be offensive to someone else 6

Link: There are no objective legal guidelines about what’s offensive or reasonable 7

Link: Violations of section 3 (like guessing wrong about offending someone) are punished by Section 4 of the bill 7

Impact: Human rights violated. Criminalizing emotional distress upsets the balance between upholding safety and preserving core values of free expression and notice to defendants 7

2. First Amendment violation #1: Collecting data 8

Link: Commercial Facial Recognition Privacy Act bans “collecting” facial recognition data. 8

Link: Banning public photography violates the First Amendment. Impact: Harms society by removing access to information and denying human rights 8

3. First Amendment violation #2: Sharing data 8

Link: CFRP Act bans “sharing” any facial recognition data 8

Link: Government banning communication of information about someone violates the First Amendment, even when you claim it’s for upholding “privacy” 9

Impact: Compromising Freedom of Speech is really bad. It’s the foundation of nearly all other human rights 9

A/T “But it’s a corporation / commercial activity” – Doesn’t matter, constitutional protection still applies 9

4. Lost social benefits and missing children 10

You’d want more facial recognition if it helped find your missing daughter 10

Facebook pictures help solve crime 10

Facial recognition has multiple positive impacts that outweigh the bad 10

Negative: Commercial Facial Recognition Privacy Act (S.847)

INHERENCY

1. State & Local initiatives are happening in Status Quo, and they’re better

States and cities are doing what CFRP is trying to do, with their own initiatives

Nicole Sakin 2021 (non-member contributor) published by International Association of Privacy Professionals, Will there be federal facial recognition regulation in the US? 11 Feb 2021 <https://iapp.org/news/a/u-s-facial-recognition-roundup/> (accessed 16 Oct 2021)

In the absence of a federal law regulating facial recognition, state and city laws have filled the gap. However, there have been attempts by Congress to pass federal legislation that puts guardrails around the use of the technology. While several bills in the 116th Congress focused on facial recognition, including 2019’s [Commercial Facial Recognition Privacy Act](https://www.congress.gov/bill/116th-congress/senate-bill/847), 2020’s [Ethical Use Of Facial Recognition Act](https://www.congress.gov/bill/116th-congress/senate-bill/3284/text), and [Facial Recognition and Biometric Technology Act of 2020](https://www.congress.gov/bill/116th-congress/senate-bill/4084/text), none of them moved past introduction. The [George Floyd Justice In Policing Act](https://www.congress.gov/bill/116th-congress/house-bill/7120/text) and [Advancing Facial Recognition Act](https://www.congress.gov/bill/116th-congress/house-bill/6929/text?r=1&s=1) progressed a little further in the legislative process but were not adopted. On the state level, there have recently been laws introduced in [Alabama, Maryland](https://iapp.org/news/a/facial-recognition-bills-proposed-in-maryland-alabama/) and [Washington](http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf#page=1) state.

Founders’ Criterion: Anyone with a plan should justify why the Federal government should do it, rather than the States

Michael S. Greve 1999 (cofounder and executive director of the Center for Individual Rights and an adjunct fellow of American Enterprise Institute) REAL FEDERALISM – Why It Matters, How It Could Happen <https://books.google.com/books?id=x3kViV5h-O0C&pg=PA11&lpg=PA11&dq=federalism+founders&source=bl&ots=0WctqI-VKL&sig=iaatTqW6f-rlV3rtNM65mzE0D8Y&hl=en&sa=X&ved=0ahUKEwi4yv7gm7zWAhVi4oMKHWFGA904ChDoAQhPMAc#v=onepage&q=federalism%20founders&f=false> (accessed 16 Oct 2021)



State action is better than federal: Experimentation among the states develops & spreads new and better ideas

Prof. Graeme Boushey 2012. (Robert Wood Johnson Scholar in Health Policy Research at Univ of Michigan and assistant professor at Univ of California, Irvine) Punctuated Equilibrium Theory and the Diffusion of Innovations POLICY STUDIES JOURNAL, January 2012 <http://onlinelibrary.wiley.com/doi/10.1111/j.1541-0072.2011.00437.x/full>

Although federalism makes policy coordination difficult, it also creates opportunities for considerable policy innovation, as municipal, county, and state governments develop new policies to address local concerns. Federalism encourages venue shopping, a process where activists and interest groups strategically exploit the multiple venues of government to secure support for their legislative programs (Baumgartner & Jones, 2009; Holyoke, 2003; Pralle, 2003). This process increases the number of new ideas entering the political systems and can create conditions where “new ideas or policy images may spread rapidly across linked venues, thus setting in motion a positive feedback process” (Baumgartner & Jones, 2009, p. 240).

2. Industry standards

Industry is developing self-regulatory standards on facial recognition and privacy

Michael McLaughlin 2020 (Research Analyst, Information Technology and Innovation Foundation) testimony Before the California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation Hearing on “Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges” March 10, 2020 <https://www2.itif.org/2020-california-facial-recognition-testimony.pdf> (accessed 16 Oct 2021)

Finally, industry has developed voluntary self-regulation and principles to foster the responsible use of the technology. For example, in 2011, the digital signage industry adopted a set of voluntary privacy and transparency guidelines for the use of facial recognition and facial analysis. This standard offers detailed guidance for how to provide clear and meaningful notice to consumers and under which conditions consumers should be able to opt-in or opt-out of data collection. In 2012, the U.S. Federal Trade Commission (FTC) published a staff report that recommended a series of best practices for business use of facial recognition technology. The report, which was the result of a workshop and eighty public comments, identified numerous best practices, including that companies should establish “appropriate retention and disposal practices for the consumer images and biometric data that they collect.” The FTC’s recommendations also included that businesses should provide clear notices that they are using facial recognition, provide consumers the opportunity to opt-out of facial recognition use, and that companies should not use the technology to identify anonymous images of an individual without their consent. For example, a company should not use the technology to identify an individual walking to work to learn their identity without the individual being aware. In addition, in February 2014, the National Telecommunications and Information Administration (NTIA) in the U.S. Department of Commerce launched a multi-stakeholder process on commercial use of facial recognition. In June 2016, a group of stakeholders reached a consensus on a set of best practices that offered guidelines for protecting consumer privacy. Many of the technology companies that make facial recognition technology have also published their own principles for developing and using the technology. For example, Microsoft’s president Brad Smith has outlined six principles—fairness, transparency, accountability, nondiscrimination, notice and consent, and lawful surveillance—that will guide how Microsoft develops and 5 deploys facial recognition technology. Amazon likewise has developed guidance for its facial recognition customers, created an acceptable use policy, and published its recommendations for federal legislation. Indeed, many of the leading facial recognition technology vendors, including Google, RankOne, and Trueface, have released similar principles. More recently, the U.S. Chamber of Commerce’s Technology Engagement Center (C\_TEC), whose members include facial recognition vendors, developers, users, and other stakeholders, drafted a set of policy principles for facial recognition that called for a single national regulatory framework that would promote beneficial uses of the technology while mitigating risks.

HARMS / SIGNIFICANCE

1. No clear definition of the “privacy” they’re trying to protect

We don’t agree on what is “private” and what is “public” any more. And you probably don’t know either

Mark Rasch 2018 (Cyber Law Editor) SECURITY CURRENT 29 June 2018 “Privacy is Dead. Long Live Privacy” <https://securitycurrent.com/privacy-is-dead-long-live-privacy/> (accessed 16 Oct 2021)

Privacy is dead because we can’t agree on what we mean by “privacy” generally, and “private information” in particular. We can’t agree on who “owns” that information, and what rights individuals and entities have to collect, store, process or use that information. On the flip side, we don’t agree on what is “public” information. You saunter to the local shopping mall and buy a pair of faded denim jeans at the local Gap — in full view of dozens of other customers and security cameras. Private? Public? When you parked in the mall lot, with your vanity license plate (GO CAPS) prominently displayed on the back of your car – public? The window stickers which advertise your life membership in the NRA or Sierra Club — private information?

2. No impact

Facial recognition is so widespread that no one cares and no one has any reasonable expectation of privacy

Riya Anchi 2020 (JD candidate at Penn. State Univ. Law School) Facial Recognition Technology: A Fourth Amendment Violation? 24 Feb 2020 PENN STATE LAW REVIEW https://www.pennstatelawreview.org/the-forum/facial-recognition-technology-a-fourth-amendment-violation/

Furthermore, it is also unlikely that society recognizes “the expectation of privacy from facial recognition technology in public places” as reasonable. Today, the use of video surveillance systems in public places is commonplace.  Most people are aware of the use of these surveillance systems.  It is improbable that people would not expect to be subjected to some form of video surveillance in public places. Because video surveillance is the basis of facial recognition, it is unlikely that society would view the expectation of privacy from the use of such technology as reasonable.

Corporate facial recognition doesn’t violate any expectation of privacy

Susan McCoy 2002 (JD candidate, John Marshall Law School) O'BIG BROTHER WHERE ART THOU?: THE CONSTITUTIONAL USE OF FACIAL-RECOGNITION TECHNOLOGY, JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW, Spring 2002 <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1143&context=jitpl> (accessed 16 Oct 2021)

No individual can reasonably expect to maintain privacy in a public forum. Facial-recognition technology will be implemented in public places, such corporate and government buildings, busy sidewalks, sports events and airports. These public places are analogous to open fields. Courts have held there can be no legitimate and reasonable expectation of privacy in an open field.

3. Hype & Exaggeration

Fear of facial recognition technology is just like past fears of technology that didn’t do any harm

Michael McLaughlin 2020 (Research Analyst, Information Technology and Innovation Foundation) testimony Before the California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation Hearing on “Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges” March 10, 2020 <https://www2.itif.org/2020-california-facial-recognition-testimony.pdf> (accessed 16 Oct 2021)

Fifth, the fear of facial recognition technology that has led to calls for bans is similar to claims about other technologies that have not had their fears realized. For example, in the 1960s, many people feared transistors would spell the end of privacy, with miniature electronics used to eavesdrop on private conversations. In the early 2000s, privacy advocates called for bans of radio frequency identification (RFID) chips, which use radio waves to transmit data, in several use cases, including on government identification documents. These advocates warned that stores, governments, and even terrorists would use RFID to track the movements of individuals. For example, the Electronic Frontier Foundation (EFF) argued that a 2005 U.S. State Department proposal to require RFID chips in passports would turn passports into “terrorist beacons,” stating “that's precisely what they'll become if we allow the State Department to move ahead with this plan.” The fears of stores, governments, or terrorists tracking individuals with RFID never materialized. Moreover, just as transistors did not give rise to widespread eavesdropping, neither will facial recognition lead to pervasive surveillance.

SOLVENCY

1. “Security” loophole

AFF law specifically allows facial recognition for “security” purposes

Section 3-e-2 of the Commercial Facial Recognition Privacy Act of 2019 (the Affirmative’s Plan) <https://www.govtrack.us/congress/bills/116/s847/text> (accessed 16 Oct 2021)



Definition of “security application”

Section 2(9) of the Commercial Facial Recognition Privacy Act of 2019 (the Affirmative’s Plan) <https://www.govtrack.us/congress/bills/116/s847/text> (accessed 16 Oct 2021)



Impact: Drop any harms or advantages from the round involving security surveillance, because they can’t solve them

Affirmative has a duty to now separate out how much of their harms come from security surveillance and how much of them come from other areas, since their plan explicitly rules out solving for security applications. Who is doing facial recognition for purposes other than security? They have to answer that and prove it’s a significant problem.

DISADVANTAGES

1. Creating the crime of offending someone – violates human rights

Link: The bill requires the facial recognition controller to guess what might be offensive to someone else

Section 3c of the Commercial Facial Recognition Privacy Act of 2019 (the Affirmative’s Plan) <https://www.govtrack.us/congress/bills/116/s847/text> (accessed 16 Oct 2021)



Link: There are no objective legal guidelines about what’s offensive or reasonable

Avlana K. Eisenberg 2015. (Lab Fellow, Edmond J. Safra Center for Ethics, Harvard Law School; Lecturer on Law, Harvard Law School) MICHIGAN LAW REVIEW March 2015 “Criminal Infliction of Emotional Distress” <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1195&context=mlr> (brackets added) (accessed 16 Oct 2021)

While to one person unwanted communication may be threatening based on past experience (either with the person initiating the communication or, quite possibly, with someone entirely unconnected to the present event), to another it may be a minor inconvenience. Indeed, one person might consider an ex-boyfriend’s condolence card a thoughtful gesture, while another person might find the same card to be offensive and disturbing. As a society, we do not have clear, objective guidelines to discern which reaction is more likely—let alone reasonable—which suggests that it would be very difficult to develop a consensus as to what constitutes emotional injury significant enough to trigger criminal culpability. This lack of consensus about what constitutes emotional injury, combined with the varying (and often unpredictable) reactions of the people receiving the communication, makes CIED [Criminal Infliction of Emotional Distress] scenarios uniquely murky, especially when compared with the archetypal assault case that involves impending physical harm.

Link: Violations of section 3 (like guessing wrong about offending someone) are punished by Section 4 of the bill

Section 4 of the Commercial Facial Recognition Privacy Act of 2019 (the Affirmative’s Plan) <https://www.govtrack.us/congress/bills/116/s847/text> (accessed 16 Oct 2021)



Impact: Human rights violated. Criminalizing emotional distress upsets the balance between upholding safety and preserving core values of free expression and notice to defendants

**[“Notice to defendants” is a human right to be aware of what conduct is illegal so they can avoid doing it. People have to be “on notice” of what’s legal and what’s not in order to make decisions in their lives. If the law is so vague that people don’t know they’ve violated it until they’re arrested, then people can’t live their lives freely.]**

Avlana K. Eisenberg 2015. (Lab Fellow, Edmond J. Safra Center for Ethics, Harvard Law School; Lecturer on Law, Harvard Law School) MICHIGAN LAW REVIEW March 2015 “Criminal Infliction of Emotional Distress” <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1195&context=mlr> (brackets added) (accessed 16 Oct 2021)

As awareness of emotional harm increases, so does impatience with the implicit approach for not doing enough. Yet we should not be too quick to reject this approach even if it seems to address emotional harm insufficiently in a particular situation. We should also resist assuming that, to account adequately for emotional harm, we must explicitly criminalize the infliction of emotional distress. While that view is perhaps an outgrowth of the broader impulse to bring emotions to the forefront in law, it is too extreme. Instead, we should work within the implicit approach’s system of compromise to identify conduct that causes severe emotional harm and to explicitly prohibit such behaviors. Otherwise, we risk upsetting the precarious balance between protecting the safety and well-being of citizens and preserving core values such as free expression and notice to defendants.

2. First Amendment violation #1: Collecting data

Link: Commercial Facial Recognition Privacy Act bans “collecting” facial recognition data.

Taylor Hatmaker 2019 (journalist) 14 Mar 2019 “Bipartisan bill proposes oversight for commercial facial recognition” <https://techcrunch.com/2019/03/14/facial-recognition-bill-commercial-facial-recognition-privacy-act/> (accessed 16 Oct 2021)

On Thursday, Hawaii Senator Brian Schatz and Missouri Senator Roy Blunt [introduced a bill](https://www.blunt.senate.gov/news/press-releases/blunt-schatz-introduce-bipartisan-commercial-facial-recognition-privacy-act) designed to offer legislative oversight for commercial applications of facial recognition technology. Known as the[Commercial Facial Recognition Privacy Act](https://www.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act), the bill would obligate companies to first obtain explicit user consent before collecting any facial recognition data as well as limiting companies from freely sharing facial recognition data with third parties.

Link: Banning public photography violates the First Amendment. Impact: Harms society by removing access to information and denying human rights

Steve Schlackman 2020 (photographer and Patent Attorney with a background in marketing) Is Street Photography Legal? 15 Aug 2020 <https://abj.artrepreneur.com/is-street-photography-legal/> (accessed 16 Oct 2021)

As a general rule, if a photographer is shooting from a *public space*, such as a street or a park, he or she will usually have the right to do so without the consent of the subjects. Generally speaking, if you can see it from a public space, you can take a picture of it. Ok, but why do photographers have such latitude?  The legal reasoning, at least in the United States, stems from the First Amendment’s*freedom of expression* clause and the long line of Supreme Court decisions that have interpreted it.  The Founding Fathers believed that a free society is one in which a person can speak his or her mind without fear of reprisals by those in power or by those who may disagree. Our society is based on the idea that everyone is better off when people may freely create and express themselves, and when information flows unencumbered, to ensure an informed citizenry.

3. First Amendment violation #2: Sharing data

Link: CFRP Act bans “sharing” any facial recognition data

Cross apply the same first link card in DA #2. It says the bill not only limits collecting but sharing facial data as well.

Link: Government banning communication of information about someone violates the First Amendment, even when you claim it’s for upholding “privacy”

Prof. Eugene Volokh 2000 (law professor, UCLA Law School) FREEDOM OF SPEECH, INFORMATION PRIVACY, AND THE TROUBLING IMPLICATIONS OF A RIGHT TO STOP PEOPLE FROM SPEAKING ABOUT YOU, Stanford Law Review Vol. 52 No. 5 May 2000 <https://poseidon01.ssrn.com/delivery.php?ID=782003117027013004125122095019119089020016006059021006029106001097092085029102023065064106123110078072025043021025030071003102093068070122117031073027010093124006086019091068102015110125114&EXT=pdf&INDEX=TRUE> (accessed 16 Oct 2021) (ellipses and brackets in original)

Privacy is a popular word, and government attempts to “protect our privacy” are easy to endorse. Government attempts to let us “control . . . information about ourselves” sound equally good: Who wouldn’t want extra control, especially of things that are by hypothesis personal? And what fair-minded person could oppose requirements of “fair information practices”? The difficulty is that the right to information privacy—the right to control other people’s communication of personally identifiable information about you—is a right to have the government stop people from speaking about you. We already have a code of “fair information practices,” and it is the First Amendment, which generally bars the government from “control[ling the communication] of information” (either by direct regulation or through the authorization of private lawsuits), whether the communication is “fair” or not. While privacy protection secured by contract turns out to be constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.

Impact: Compromising Freedom of Speech is really bad. It’s the foundation of nearly all other human rights

Prof. Stephen J. Wermiel 2018. (professor of practice of constitutional law at American University Washington College of Law) The Ongoing Challenge to Define Free Speech (article is undated but says it was written 227 years after the ratification of the Bill of Rights in 1791) <https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/the-ongoing-challenge-to-define-free-speech/the-ongoing-challenge-to-define-free-speech/> (accessed 6 Oct 2021)

Freedom of speech, Supreme Court Justice Benjamin Cardozo declared more than 80 years ago, “is the matrix, the indispensable condition of nearly every other form of freedom.” Countless other justices, commentators, philosophers, and more have waxed eloquent for decades over the critically important role that freedom of speech plays in promoting and maintaining democracy.

A/T “But it’s a corporation / commercial activity” – Doesn’t matter, constitutional protection still applies

Prof. Eugene Volokh 2000 (law professor, UCLA Law School) FREEDOM OF SPEECH, INFORMATION PRIVACY, AND THE TROUBLING IMPLICATIONS OF A RIGHT TO STOP PEOPLE FROM SPEAKING ABOUT YOU, Stanford Law Review Vol. 52 No. 5 May 2000 <https://poseidon01.ssrn.com/delivery.php?ID=782003117027013004125122095019119089020016006059021006029106001097092085029102023065064106123110078072025043021025030071003102093068070122117031073027010093124006086019091068102015110125114&EXT=pdf&INDEX=TRUE> (accessed 16 Oct 2021)

Some might argue that there’s something inherently un-speech-like in corporations communicating to other corporations, but there’s no reason why this would be so. To begin with, the corporate status of the speaker or the listener can’t be relevant; surely it can’t matter for privacy purposes whether customer information is communicated by and to corporations, partnerships, or sole proprietorships. And the Court has specifically held that speech doesn’t lose its constitutional protection because the speaker is a corporation, which makes sense for various reasons, among them that almost all media organizations are corporations.

4. Lost social benefits and missing children

You’d want more facial recognition if it helped find your missing daughter

Susan McCoy 2002 (JD candidate, John Marshall Law School) O'BIG BROTHER WHERE ART THOU?: THE CONSTITUTIONAL USE OF FACIAL-RECOGNITION TECHNOLOGY, JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW, Spring 2002 <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1143&context=jitpl> (accessed 16 Oct 2021)



Facebook pictures help solve crime

Michael McLaughlin 2020 (Research Analyst, Information Technology and Innovation Foundation) testimony Before the California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation Hearing on “Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges” March 10, 2020 <https://www2.itif.org/2020-california-facial-recognition-testimony.pdf> (accessed 16 Oct 2021)

First, facial recognition has increased public safety. For example, in April 2019, a California law enforcement officer saw a Facebook post about a missing young girl. The officer used facial recognition technology to find online sex trafficking advertisements that featured the missing girl. These matches led to more traditional police work, and within weeks, the recovery of the child. Facial recognition has also helped identify individuals committing crimes ranging from shoplifting and check forgery to armed robbery and murder.

Facial recognition has multiple positive impacts that outweigh the bad

Michael McLaughlin 2020 (Research Analyst, Information Technology and Innovation Foundation) testimony Before the California State Assembly Privacy and Consumer Protection Committee and the Assembly Select Committee on Emerging Technologies and Innovation Hearing on “Shaping the Future of Facial Recognition Technology in California: Identifying Its Promises and Challenges” March 10, 2020 <https://www2.itif.org/2020-california-facial-recognition-testimony.pdf> (accessed 16 Oct 2021)

Finally, bans or moratoriums limit the positive uses of facial recognition. Facial recognition has already helped find missing individuals, identify individuals who committed serious crimes, such as armed robbery, and prevent potentially dangerous people, such as sex offenders, from entering school facilities. A ban or moratorium not only limits negative uses of facial recognition but positive uses as well.