Chicago Council of Lawyers

POSITION STATEMENT:

Principles for Regulating Facial Recognition (and Other Biometric) Technology

Chicago Council of Lawyers - April 7, 2021

CONTENTS

750 NORTH LAKE SHORE DRIVE, FOURTH FLOOR, CHICAGO, ILLINOIS 60611
PHONE: (312) 988 – 6565 | EMAIL: CAFFJ@CHICAGOAPPLESEED.ORG

www.CHICAGOCOUNCIL.org

I. PURPOSE AND OVERVIEW

The purpose of this memorandum is to attempt to reach initial consensus on position of the Civil Liberties Committee of the Chicago Council of Lawyers as to the general principles that should govern regulation of facial recognition technology (and other forms of biometric information), as its use is becoming more widespread.[1] After reviewing some background information on the technology, we believe several principles should guide regulation of such technology.

First, we believe that the nature of the regulations will necessarily differ significantly, depending on whether the regulated parties are government actors or private parties. The significant differences between those two groups require different approaches.

Second, as a general matter, we believe that certain uses of such technologies by government entities should be barred or severely restricted unless and until independent standards are adopted and applied regarding the minimum required accuracy of the technologies in various circumstances.

Third, we believe that informed consent, freely given, is a general prerequisite to using an individual's identifying information. This is the essence of the philosophy underlying the European Union's General Data Protection Regulation (GDPR) and the Illinois Biometric Information Privacy Act (BIPA). We believe it is a sound limiting principle in most circumstances.

Fourth, we believe the government's uses of the technologies are subject to different concerns and a different weighing of competing interests than private parties' use of information. In many cases government units have special concerns (public safety, policing, national defense, public health) that merit increased access to and use of such information. However, government units have a much greater ability to compel collection and disclosure of information, making consent less available as a limiting principle. Government uses also pose a much greater potential for infringement on individual liberties. These competing concerns, combined with the limited usefulness of the consent paradigm, mean that limits on government entities need to be balanced and spelled out in more specific and circumscribed terms. The overriding principle should be that certain government uses of such technologies should be presumed prohibited unless *specifically* authorized by legislative bodies acting consistent with constitutional restraints.

Fifth, for private parties, we believe that *informed consent* should be the overriding limiting principle and that individuals' rights to obtain and control such information should be explicitly spelled out, as in the European Union GDPR and the Illinois BIPA.

Sixth, to be effective, we believe that minimum requirements should be spelled out at the federal level, with state and local governments having some leeway to impose stricter requirements to residents within their geographic borders.

[1] For some recent articles on this topic see, "A Need to Balance Privacy with Data Sharing" by David Deming *for The New York Times* (Feb. 21, 2021); "How One State Wrote Rules on Facial Recognition" by Kashmir Hill for *The New York Times* (Feb. 28, 2021); and "Your Face is not Your Own" by Kashmir Hill for *The New York Times Magazine* (March 21, 2021).

II. Background

a. The Technology and Its Uses

Facial recognition technology employs digital images of faces to identify individuals, utilizing the geometries of the face as well as distinguishing features of the eyes, nose, mouth, chin, cheeks, and forehead.[2] It is a much more sophisticated, widespread, and versatile version of the mugshot books police departments used as databases to help identify suspects in earlier eras. The biggest differences are that computer programs, rather than human witnesses, are now doing the comparison and identification of matches between the images and that the databases are much larger and are not limited to people with prior arrests.

The technology uses various algorithms to match features in different facial images by compiling many pieces of information about the geometry of a particular facial image in a large database and comparing that information to the data associated with other facial images in the database. Most facial recognition systems today utilize a form of "machine learning" to train the systems and to improve their accuracy over time.[3] In essence, such machine learning involves supplying the computer with a large database of images and instructing it to look for patterns that are useful in comparing and differentiating the images. The increasing technical capacities of computers to process large amounts of information with increasing speed and efficiency have made such systems possible.

However, biases inherent in the databases and the algorithmic design and programming can make the techniques more accurate for some populations and groups than for others.[4] A number of studies[5] have documented that some of the systems in use today have significantly higher error rates when attempting to identify the faces of people of color and women. In theory, these differences should diminish over time as the databases provided to the machine learning programs are broadened and the computers are programmed to look for different or more subtle features. Nevertheless, the accuracy of any particular identification will always be affected by the resolution of the image being compared, the lighting of the image, the angle of the image, the distance from the camera to the subject, the obfuscation of the image and other similar characteristics of the image being used.

---

[2] *See* Electronic Frontier Foundation (EFF) "Transition Memo to Incoming Biden Administration" at p.5. Accessible: https:/www.eff.org/wp/eff-transition-memo-incoming Biden-administration.

[3] *See* "A Gentle Introduction to Deep Learning for Facial Recognition," accessible at https://machinelearningmastery.com/introduction-to-deep-learning-for-face-recognition/.

[4] These problems have led many groups to call upon Congress to limit or ban use of facial recognition technology. *See* Rodrigo, Chris Mills (July 2, 2020) "Dozens of Advocacy Groups Push for Congress to Ban Facial Recognition Technology" for *The Hill*, accessible at https://thehill.com/policy/technology/505563-dozens-of-advocacy-groups-push-for-congress--to-ban-facial-recognition.

[5] *See generally*, "Algorithmic Justice League," accessible at https://www.aji.org/learn-more; Buolamwini & Gebru (2018) "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," accessible at http://proceedings.mit.press/v81/boulamwini18a/buoplamwini18a.pdf in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency 81*:77-91 (concluding that facial recognition software issued by IBM and Microsoft was less accurate when analyzing dark-skinned and feminine faces compared to light-skinned male faces. Other studies from MIT, the Georgetown Center for Privacy and Technology, and the ACLU have found similar biases in other facial recognition systems). *See also* "About Face," accessible at https://www.eff.org/aboutface.

Another thing that has made the spread of facial recognition technology possible and useful is the widespread distribution of images of our faces. Virtually everyone's images are stored in a public database of some kind. The availability of these images has been greatly enhanced by our society's uses of photo IDs (for licenses, education, employment, credit, and security clearances), the tremendous expansion of video cameras in public places, the rise of social media and photo sharing sites, and the ubiquity of cameras in our mobile phones. The combination of these things has enabled the creation of very large data sets comprising large portions of the population.[6]

b. The Players

The number of organizations and individuals utilizing facial recognition technologies has skyrocketed over the course of the past two decades. Governments have long been using such search capabilities in policing and intelligence activities to identify suspects and victims. Repressive regimes around the world have also begun using facial recognition systems to surveil and control their own citizens, most notably in China and some countries in the Middle East, but also including parts of Great Britain and Russia. Many governments have also been expanding their surveillance of their populations in public spaces for public safety reasons and large systems of connected cameras in such spaces have been created. In many cases, they are augmented by the increasing number of cameras monitoring private spaces.

Virtually all of the largest technology companies have played some role in creating such systems, including Google, Microsoft, Apple, and Facebook.[7] They, along with legions of smaller technology companies (like Palantir,[8] Clearview,[9] and others) have developed facial recognition systems or databases of various scopes and accuracies.

The use of such systems to identify individuals is not limited to government entities: retailers, advertisers, private security companies, educators, social media companies, computer manufacturers and many other private parties have begun to employ such systems for their own ends.[10] The list of "players" and uses is virtually unlimited.

c. Regulatory Possibilities

In considering what types of controls to place upon facial recognition (and other biometric information) technologies, it may be helpful to identify some of the possible techniques that

---

[6] A recently filed lawsuit in California against Clearview is challenging its scraping of websites for facial images as a violation of California's constitutional privacy rights (Case No. 1:21 cv 00038 mkv). Canada's privacy commissioner, Daniel Therrien, has deemed Clearview's practices as constituting "mass surveillance and it is illegal" under Canadian law (https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210203/). Clearview has also been a controversial player in marketing facial recognition software to police departments and private entities.

[7] Facebook has been sued in class actions in California for using facial recognition systems and stored images of Illinois residents without their consent, allegedly in violation of the Illinois Biometric Act. *See,* "Facebook will Pay $650 Million to Settle Class Action Suit Centered on Illinois Privacy Law," by Taylor Hatmaker in *Tech Crunch* (March 1, 2021) at https://techcrunch.com/2021/03/01/facebook-illinois-class-action-bipa/.

[8] For a broader article on Palantir, see "The All-Seeing Eye" by Michael Steinberger in *The New York Times Magazine* (Oct. 25, 2020) at p. 28.

[9] *Id* at 6.

[10] For example, *see* "Chinese Must Scan Faces to Get Phones" from *The Wall Street Journal* (Dec. 3, 2019) at p. A7; "Facial Recognition Marks Chinese Pajama Wearers" from *The New York Times* (Jan. 22, 2020) at p. A12; "Retailers, Beware: Shoppers Don't Like to Be Watched Online," from *The Wall Street Journal* (Aug. 3, 2020); "Face Scans are seen as Replacements for Tickets" from *The Wall Street Journal* (Aug. 3, 2020). *See generally*, "Biometrics Update," at https://www.biomtricupdate.com and https://www.biometricupdate.com/?posttype=all&s=facial+recognition.

could be employed to control them. The recommendations set forth in following sections employ different combinations of the strategies listed below.

The first and most obvious control strategy would be simply to prohibit the use of software utilizing facial recognition or other biometric information. Some organizations, such as the American Civil Liberties Union (ACLU), have proposed this approach for now.[11] However, the Chicago Council of Lawyers ("Council") believes this is not a viable strategy in practice, because the requisite databases and computer technology are too widespread – and the demand for them too intense – to effectively enforce an absolute prohibition. Essentially, this horse has already left the barn and we seriously doubt that any cowhand has the ability to bring it back. In addition, we believe that this technology can be valuable when used for legitimate purposes: for example, it has been reported that the FBI has used this technology as one method of identifying persons who invaded the United States Capitol Building on January 6, 2021.[12] However, this does not mean that flat prohibitions may not be useful for particular entities or uses.[13]

A second possible approach would be to limit the collection and distribution of the images (and other forms of biometric information) that such technologies rely upon. This is the strategy seemingly recommended by some scholars.[14] It is, in part, also the strategy that the GDPR relies upon by empowering individuals with rights to control the use of their images by private parties, and by requiring informed consent as prerequisite to the use of an individual's biometric information.[15] The system that the federal government has created to control distribution of medical information also provides a possible model or example of such a system.[16]

A third possible approach is to prohibit anyone (or specified entities) from using such identification technologies except for specifically approved purposes, such as allowing police departments to use facial recognition solely for the purpose of identifying possible suspects but prohibiting its evidentiary use in prosecuting or convicting individuals of unlawful activity. Such an approach obviously requires careful planning and thought as to how to enforce such limitations. The systems that the federal intelligence agencies use to corral uses of information about domestic citizens would be a possible example of such a system.

A fourth possible approach would be to establish private property rights in individuals with respect to their unique identifying information and eschew any government regulation. In

[11] *See*, https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/.
[12] *See e.g.*, "Digital Fingerprints are Identifying Capitol Rioters" by Darrell M. West (Jan. 19, 2021) for The Brookings Institution. Accessible: https://www.brookings.edu/blog/techtank/2021/01/19/digital-fingerprints-are-identifying-capitol-rioters/.
[13] See, "Why EFF Doesn't Support Bans on Private Use of Face Recognition" accessible at https://eff.org/deeplinks/2021/01/why-eff-doesn't-support-bans-on-private-use-of-face-recognition.
[14] *For example, see* Woodrow Hartzog's "Privacy's Blueprint" (arguing for more conscious regulation of the design of privacy protections on a spectrum of "obscurity") in *Harvard University Press*, 2018; Shoshana Zuboff's "The Age of Surveillance Capitalism" (generally discussing the dangers of "surveillance capitalism") *in Hachette Book Group*, 2019.
[15] Regulation (EU) 2016/679 of the European Parliament and of the Council; *See*, "What is GDPR, the EU's new data protection law?" accessible at https://GDPR.eu/what-is-the-gdpr.
[16] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, accessible at https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996.

essence, such a system would rely upon individuals suing or contracting to protect and enforce their property rights. While we support the recognition of such individual rights, we believe that relying solely on individuals' efforts to protect those rights is neither a realistic nor effective solution. Given the power, scope, and economic advantage of the governments and industries involved with such technologies, a broader, collective strategy is necessary to realistically protect the privacy interests at stake for all members of society.

III. Requiring Minimum Accuracy Standards

In the view of the Council, an appropriate first step in regulating facial recognition technology would be to require those creating and marketing such technologies to meet independently-developed accuracy standards for enumerated uses of the technology.[17] For example, the National Institute of Standards and Technology periodically tests the accuracy of facial recognition algorithms voluntarily submitted by vendors.[18] Regulators could use such standards to set minimum required levels of accuracy for specific uses of the technologies or products in question, especially such use by specified government agencies.

Creating such standards should not be particularly difficult—any image to be identified could be graded for resolution, lighting, angle of exposure and so on. The system could then be evaluated for accuracy by running a certain number of agreed images of various grades through the system. Presumably, some systems might perform differently depending on the degree of differentiation from a standard image of agreed upon quality. Systems could have multiple ratings depending on the type of image being evaluated. It would be reasonable to expect the industry and the government to cooperate in the creation of such standards. It would also be reasonable to expect such standards to be developed relatively quickly (and further refined as technology advances).

Unless and until such standards are created and applied, we would recommend imposing partial moratoriums on certain uses of facial recognition technology by various government agencies, such as law enforcement, as explained in greater detail below (see Section V).

IV. Requiring Meaningful Consent

A second important proposition would be to require that individuals have recognized privacy rights associated with their biometric information (including facial images) and that informed and meaningful consent should generally be required before anyone may utilize that image or information, even if publicly available. This is, in large part, the principle underlying such legislation as the GDPR and the Biometric Protection Acts adopted in Illinois and elsewhere.[19]

The GDPR is a very broad statute governing the data privacy of individuals in the European Union. It is based upon a number of key principles:

[17] There have been some calls for such regulation already, however, they are not necessarily focused narrowly on setting standards for accuracy in the technology. *See e.g.*, Burt, Chris (June 8, 2020): "Biometrics Experts Call for Creation of FDA-Style Government Body to Regulate Facial Recognition" at https://www.biometricupdate.com/202006/biometrics-experts-call-for-creation-of-fda-style-government-body-to-regulate-facial-recognition.
[18] *See e.g.*, https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html.
[19] *Id* at 15. For the Illinois Biometric Act, see 740 ILCS Sec 14 and https://enwikipedia.or/wik/Biometric_Information_Privacy_Act.

1. *Lawful, Fair &Transparent*: Any data collected on individuals must be gathered legally and users must be aware of the fact that the data is being collected.
2. *Purposeful*: The reason or purpose for the data collection must be clearly spelled out.
3. *Data Minimization*: The data collected must be the minimal amount needed for the stated purpose.
4. *Accuracy*: The data collected must be accurate.
5. *Storage Time Limits*: Reasonable limits should be placed upon the length of time the data can be retained.
6. *Security*: Reasonable steps must be taken to keep the data secure.
7. *Accountability*: Organizations collecting, processing, and/or storing data must be accountable to individuals for compliance.
8. *Meaningful Consent*: Informed and meaningful consent from an individual is required generally to collect a person's data. Such consent must also be "freely given" (which *does not include* consent provided as a contractual condition for receiving services if the processing of personal data is not necessary for the performance of the contract). The GDPR contains a number of other provisions intended to ensure that consent must be fully informed and explicitly given for the stated purposes of collection.

The GDPR differs from the general US approach in that companies collecting, storing, or processing personal data must be able to justify their activities under the GDPR framework. The regulations also require that people whose data has been breached must be notified. Substantial fines (of up to the greater of 20 Million Euros or 4% of a company's global revenue) can be imposed for violations.

The GDPR also recognizes that individuals have the following privacy rights in connection with their "personal data" (which is very broadly defined). Those rights include:

1. The right to be informed about what data is being collected and for what purposes;
2. The right to obtain access and copies of the individual's data on file;
3. The right to correct the data on file;
4. The right to be forgotten, or to erasure of the data;
5. The right to restrict processing of the data;
6. The right to portability of the data;
7. The right to withdraw consent or object to the processing of the data; and
8. The right to impose restrictions on the use of the data in automated processing or "profiling" applications.

The Illinois Biometric Information Privacy Act takes a more focused approach limited to the collection, retention and processing of "biometric data" regarding an individual. Biometric data is personal data about an individual's physical characteristics, such as DNA, fingerprints, facial geometry or images, hand, retinal or ear features, odor or characteristics such as voice prints, gait, gestures or typing rhythm. These are things that cannot be easily modified by an individual and are usually or can be used for identification purposes. Companies that collect biometric information

about state residents must comply with a comprehensive set of rules regarding the collection, retention, use and distribution of such information.

In general, BIPA requires such companies to:

1. Obtain informed consent prior to the collection of such information from the individual;
2. Limit disclosure and use of such information;
3. Maintain the security of such information and limit the time of its retention; and
4. Refrain from profiting from or selling the data.

Companies that violate the BIPA can be sued by individuals harmed by the violations and can be fined up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation. Some companies, including Facebook, Shutterfly, Google, and Clearview have been sued for using facial images and facial recognition technology without the individual's consent. There are exceptions for medical companies' use of medical information under HIPAA. BIPA also does not apply to government entities (see 740 ILCS 14/10).

In general, imposing a consent requirement to limit use of facial images and facial recognition technology has been rare due to the ease of obtaining publicly accessible facial images. However, the Illinois BIPA statute suggests that we should not abandon the use of consent as a limiting principle. Even if facial images are easily and publicly obtained, it may still make sense to prohibit their collection, retention, processing, and/or sale or transfer to others by the collecting party, particularly in a commercial context. With respect to government collection of such images for legitimate identification purposes, governments could still be prohibited from using or transferring the images to others except for their explicitly indicated purposes. For example, Secretaries of State could be prohibited from sharing or using driver's license photos for any purpose other than being reproduced on a physical license, absent a warrant or other similar safeguards.

V. Principles for Limiting Government Use of Facial Recognition Technology

Unlike some private parties, governments can usually claim legitimate needs to obtain and retain facial images of individuals. Such images may be necessary for identification purposes (in licenses, security passes, and law enforcement), as well as for public safety, reference, or research purposes. An absolute prohibition on the use of facial recognition technology by government entities is impractical for that reason, to say nothing of the already widespread distribution of facial image databases among such entities.

A more practical approach to regulating use of facial recognition technologies by such entities should rely upon the following general principles, which should apply to any use of a facial recognition database by a government agency, regardless of its source, public or private:

First, unless and until appropriate standards are developed for assessing and confirming the accuracy of such technologies, a temporary moratorium should be placed on specified government uses of them. For example, law enforcement and security entities should be permitted to use such images only to generate leads or establish probable cause with an appropriate warrant or similar

safeguard, but facial recognition matches should not constitute admissible evidence in criminal legal proceedings. Law enforcement should also be required to obtain a warrant (or comply with a similar safeguard) before running facial recognition searches.[20]

Second, government entities should be barred from specified uses of facial recognition technologies except to the extent explicitly authorized by the relevant legislative bodies.

Third, government entities should be barred from using the images in question except for the purposes stated.

Fourth, government entities may share such images with other government entities only under *explicitly defined* circumstances. Using such images for commercial purposes should be prohibited and government entities should be prohibited from sharing their facial recognition databases with private entities.

VI. Principles for Limiting Private Use of Facial Recognition Technology

For private entities, the primary guiding principles should rely upon the concept of fully informed consent and the recognition of individual privacy rights – like those found in the Illinois BIPA and the European GDPR. Thus, no private entity should be able to claim any right to use an individual's facial image without showing that it has first obtained a freely given and fully informed consent from the individual in question for each of the purposes for which the image may be used. An individual's consent should be subject to revocation, upon reasonable notice, and should not require any more burdensome process to be revoked or limited than the giving of the consent. Private entities should not have the right to transfer, sell, process, or share the images without the explicit consent of the person in question. Individuals should also have the right to obtain information about any images being retained. Private entities retaining such images should be obligated to maintain reasonable security measures and to inform individuals in the event the security for those images has been breached. Individuals should also have a private right of action to sue for violation of their rights.

VII. Jurisdictional Concerns

The most practical way to balance the interests between the need to regulate facial recognition technology in a manner that enables both governmental and commercial entities to design national systems that comply would be to do so at the federal level. Any decision about the extent and appropriateness of federal preemption is a sensitive issue that obviously needs to be weighed by Congress on an issue-by-issue basis. However, in the absence of any meaningful action by Congress, states and localities should remain free to adopt those measures restricting use of facial recognition technologies that they deem appropriate to protect their residents, consistent with the usual principles of federalism governing our nation.

[20] Massachusetts House Bill H. 2701, for example, would allow police to run searches against the state's driver's license database, but only with a warrant, and would require law enforcement agencies to publish annual transparency reports regarding those searches.

VIII. Next Steps

Going forward, the Civil Liberties Committee of the Chicago Council of Lawyers will use the principles stated in this policy memorandum in any attempt to draft or evaluate proposed federal, state, or local legislation (several state and local jurisdictions around the country have already adopted such legislation).

IX. Minority Addendum

The minority of the Civil Liberties Committee submits this addendum out of a concern that the majority did not sufficiently consider the idea of an out-right ban, rather than just a moratorium, on the use of facial recognition technology – particularly in the governmental sphere. In the private sphere, the recommendations for informed consent, narrowed use, time limits, opt-in and other safeguards set forth in this memorandum, which follow the path-breaking Illinois BIPA legislation, provide important principles for the preservation of individual privacy rights. It is in the governmental sphere where the need for a total ban arises.

There are three reasons for the majority's declination to consider a total ban on government use of facial recognition technology: first, the proverbial barn door cannot be shut on a technology that has already escaped its enclosure; second, a ban would stifle innovation, thus thwarting important future breakthroughs that may be beneficial; and third, a ban would hamper legitimate law enforcement purposes (such as to identify the January 6, 2021 insurrectionists). The minority questions these explanations for the following reasons:

***First*,** many technological innovations have been banned after they have been developed. In the military arena, treaties have been reached that ban land mines, poisonous gases, biological weapons, etc., In the medical arena, United States bans (or withdrawals from commercial markets), have been imposed on a long list of drug (e.g., LSD, fentanyl, diethylstilbestrol, lumiracoxib). In the policing arena, we have seen cities and states ban such procedures as chokeholds, no-knock warrants, "stop and frisk," and the link. These were all considered advances in providing security, healing disease, or crime-prevention when initiated, but have come to be seen as too dangerous to be allowed or to continue. Facial recognition technology fits into these categories of banned matters when considered as used by governments.

***Next and importantly*,** facial recognition technology also serves to chill and deter people from exercising the First Amendment rights of peacefully assembling or associating with others and engaging in free speech as people seek to preserve their privacy by disengaging from such activities. Facial recognition technology can and is used to target groups by political persuasion (e.g., as documented with BLM protestors, or by ethnicity, such as in China with the Uighur population). It creates a perpetual and universal line-up for every and any crime that may occur with no "opt out."

***In addition*,** banning the use of facial recognition technology is not a fringe idea.[21] In 2009, San Francisco became the first U.S. city to ban such use by all city agencies, including by the police;

[21] *Id* at 11.

Sommerville, Massachusetts has done the same, as has Oakland, California and Portland, Oregon. There is pending bill in Congress (H.R. 7235), which would prohibit outright facial recognition technology for body-worn cameras.[22] One of the reasons cited for H.R. 7235 is that "[t]he use of facial recognition and other bio-metric surveillance is the functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights. This technology also allows people to be tracked without consent."

The concern with hampering law enforcement, in the civil liberties context, derives from the use of facial recognition technology to identify and arrest perpetrators of crimes caught on video.[23] However, as much as one wants to see accountability for those attempting to block the peaceful transfer of governmental power and related crimes, the majority minimizes the existence of the existing tools at the disposal of law enforcement and the public provision of information to law enforcement that are already used to identify and arrest malefactors. As the Electronic Frontier Foundation has articulated,[24] any good that comes from such intrusive surveillance is invariably buried by the ill that follows:

> *Yet history provides the clear lesson that immediate legislative responses to an unprecedented national crime or a deeply traumatic incident can have profound, unforeseen, and often unconstitutional consequences for decades to come. Innocent people—international travelers, immigrants, asylum seekers, activists, journalists, attorneys, and everyday Internet users—have spent the last two decades contending with the loss of privacy, government harassment, and exaggerated sentencing that came along with the PATRIOT Act and other laws passed in the wake of national tragedies.*

The minority view of the Chicago Council of Lawyers' Civil Liberties Committee strongly supports the majority's insistence on the use of warrants and exclusion of facial recognition technology results from prosecutions, but believes that an all-pervasive, universal system of surveillance that provides no means of opt out, no means to avoid, and indeed makes suspicious any use of such means to preserve one's privacy, requires more: it requires a ban.

[22] Another such bill – H.R. 7235 – takes the moratorium approach favored by the majority and makes in unlawful for a federal agency to use any biometric surveillance system, including facial recognition technology, except as authorized by Congress after standards, uses and auditing are instituted.
[23] *Id* at 12.
[24] *See* "The Government Has All of the Powers It Needs to Find and Prosecute Those Responsible for the Crimes on Capitol Hill This Week" at https://www.eff.org/deeplinks/2021/01/government-has-all-powers-it-needs-find-and-prosecute-those-responsible-crimes.