epic.org

February 5, 2014

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

John Verdi, Director of Privacy Initiatives
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave N.W., Rm 4725
Washington, D.C. 20230

Re: Facial Recognition Technology

Dear Director Verdi:

Regarding the current NTIA review, the Electronic Privacy Information Center ("EPIC") would like to bring to your attention comments EPIC submitted to the Federal Trade Commission ("FTC") regarding commercial facial recognition technology.

EPIC explained that increased commercial use of facial recognition threatens a fundamental understanding of the right to privacy—the ability of individuals to decide when to disclose their actual identity to others. Ubiquitous and near-effortless identification eliminates our ability to control our identities. It also degrades an essential aspect of personal security by undermining our ability to know under what circumstances others are seeking access to our identity and to make a determination as to whether to reveal our actual identity. Additionally, there are privacy and security concerns associated with the collection, use, and storage of facial geometry measurements used for identification.

The lack of a facial recognition framework to protect privacy and the security of the data is already creating a backlash against the technology's use. Europe banned Facebook's use of facial recognition technology and required the company to delete the data used for facial recognition.[1] Google banned apps and services that perform facial recognition from its Google Glass product.[2] A proper framework that protects users' privacy and data is needed.

We also note that federal agencies are moving forward with the adoption of facial recognition techniques with low levels of reliability. A FOIA request pursued by EPIC determined that the FBI is prepared to deploy facial recognition techniques for the Next Generation Identification system that allow for a 20% error rate.[3]

---

[1] Data Protection Commissioner, *Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU* (Sept. 21, 2012), http://www.dataprotection.ie/docs/21-09-12-Press-Release--Facebook-Ireland-Audit-Review-Report/1233.htm.
[2] Google Glass Platform Developer Policies: What you can't do in your Glassware, https://developers.google.com/glass/policies#c_what_you_cant_do_in_your_glassware (last visited Feb. 5, 2014).
[3] NGI System Requirements, 244 (Oct. 1, 2010), *available at* http://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.

EPIC recommends a facial recognition framework that requires companies collecting, handling, storing, and transmitting such data to adhere to the Fair Information Practices. Moreover, there should be no surreptitious collection of identity or collection of identity that occurs without meaningful consent. EPIC recommends the suspension of facial recognition technology deployment until adequate safeguards and privacy standards are established.

Sincerely,

Marc Rotenberg
Executive Director, EPIC

Jeramie D. Scott
EPIC National Security Counsel

Attachments

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

To

THE FEDERAL TRADE COMMISSION

Face Facts: A Forum on Facial Recognition

Project Number P115406

January 31, 2012

By notice published on December 23, 2011, the Federal Trade Commission ("FTC") has requested public comments on the issues raised at the workshop "Face Facts: A Forum on Facial Recognition Technology," [hereinafter "Face Facts Workshop" or "FTC Workshop"]. Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the Commission's treatment of facial recognition technology by businesses sufficiently protects the ability of consumers to control the disclosure of their identity. At a minimum, EPIC recommends that the Commission enforce Fair Information Practices ("FIP") against commercial actors when collecting, using, or storing facial recognition data. We further believe that businesses should never use facial recognitions techniques to obtain the actual identity of consumers without the consumer's actual knowledge and informed consent. Consumers today enjoy enormous freedom and personal safety because they are able to interact with so many merchants, who are essentially strangers, without concern that they will be secretly tracked and profiled. It is critical that the Federal Trade Commission take affirmative steps to ensure the protection of the consumers' right to safeguard their identity. In the absence of guidelines and legal standards, EPIC recommends a moratorium on the commercial deployment of facial recognition techniques.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[1] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and subsequent settlement concerning the social networking service.[2] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[3] The Commission's recent settlement with Facebook was based on complaints filed by EPIC and other privacy and civil liberties organizations.[4] The Commission found that Facebook had "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[5] EPIC has also worked to bring the Commission's attention to the issues raised by facial recognition technology. In 2011, EPIC Senior Counsel John Verdi

[1] *See, e.g.*, Letter from EPIC Executive Director Marc Rotenberg to FTC Commissioner Christine Varney, EPIC (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[2] Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").

[3] *Id*.

[4] Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm ("Facebook's privacy practices were the subject of complaints filed with the FTC by the Electronic Privacy Information Center and a coalition of consumer groups.").

[5] *Id*.

spoke at the Face Facts Workshop,[6] and EPIC filed a complaint with the Commission regarding Facebook's use of facial recognition technology.[7]

At a minimum, EPIC recommends that the FTC enforce Fair Information Practices ("FIP") for all commercial actors that collect, use, or store sensitive personal information like facial recognition data.[8] Described in more detail in Section V of this Comment, this would impose a set of legal obligations on these actors: limitations on collection, use, and retention of facial recognition data, informed consent, security, accessibility, and accountability. In the absence of guidelines and legal standards, EPIC recommends a moratorium on the commercial deployment of facial recognition techniques.

Section I details the FTC's Face Facts Workshop. Section II describes EPIC's involvement and expertise in facial recognition technology. Section III explains the privacy and security risks raised by the implementation of different facial recognition technologies. Section IV discusses the legal framework surrounding facial recognition technology. Section V offers a general framework for protecting consumers who use facial recognition technology based on Fair Information Practices. Section V also shows how these FIPs would apply to Facebook and Google, both of which are subject to consent agreements reached with the Commission.

I. Face Facts: A Forum on Facial Recognition Technology

On December 8, 2011, the Commission held a public workshop exploring "exploring facial recognition technology and the privacy and security implications raised by its increasing

[6] Face Facts: Forum on Facial Recognition Technology, Fed. Trade Comm'n (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/ [hereinafter Face Facts].
[7] Facebook, Inc., (2011) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf [hereinafter EPIC 2011 Facebook Facial Recognition Complaint].
[8] The OECD Guidelines provide a good overview of fair information practices. Org. for Econ. Cooperation & Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

use."[9] After introductory remarks by FTC Chairman Jon Leibowitz, the workshop featured panel discussions on the operation of facial detection and recognition technology; the uses and ramifications of facial detection; the current and future possibilities of facial recognition; and the policy implications of facial detection and recognition.[10] Panelists discussed the differences in accuracy and performance between facial detection and facial recognition, the approaches to facial recognition taken by Google and Facebook, and the inability of the current U.S. legal regime to address the issues raised by facial recognition.[11]

II. EPIC's Involvement and Expertise in Facial Recognition

EPIC has pursued the privacy and security risks raised by facial recognition in many forums, including letters to federal agencies, congressional testimony, complaints before the Commission, and public workshops hosted by the Commission. In 2002, EPIC Executive Director Marc Rotenberg testified about facial recognition before Congress.[12] He explained there are several ways to compromise the effectiveness of a biometric system: by false identification at enrollment, physical alteration of a personal biometric, skewing the sample collection by not cooperating, and hacking into or falsifying data.[13] Facial recognition system errors would lead to innocent people being falsely matched to watchlists or databases, while suspects would pass through the system unrecognized.

---

[9] *See* Face Facts, *supra* note 6.
[10] Agenda, Face Facts: Forum on Facial Recognition Technology, Fed. Trade Comm'n (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/facefacts-agenda.pdf.
[11] Twitter Transcript, Face Facts: Forum on Facial Recognition Technology, Fed. Trade Comm'n (Dec. 8, 2011), http://www.ftc.gov/os/2011/12/111214FaceRecTwitterTranscriptRecords.pdf.
[12] *Identity Theft Involving Elderly Victims: Joint Hearing Before the Special Comm. on Aging*, 107th Cong. (2002) (statement of Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr.), *available at* http://www.epic.org/privacy/biometrics/testimony_071802.html.
[13] *Id*.

In 2007, EPIC wrote to Secretary of Defense Robert Gates about the military's collection of biometric information from Iraqi citizens.[14] EPIC explained that because the identifying information of many Iraqis is tied to their religious and ethnic affiliation, the creation of a large biometric database presented a dangerous potential for misuse in a region with deep religious and ethnic strife.[15] Thus, EPIC urged the Secretary to "develop and adopt clear guidelines that incorporate strong privacy safeguards to ensure that Iraqis are afforded basic human rights in their personal information."[16]

Facial recognition in the commercial sector provided the basis for EPIC's 2011 complaint before the Commission on Facebook. On June 10, 2011, EPIC filed a complaint with the Commission regarding Facebook's compilation and subsequent use of facial images for automated online identification.[17] EPIC's complaint alleged that Facebook did not obtain the consent of users before "collecting 'Photo Comparison Data,' generating unique biometric identifiers, and linking biometric identifiers with individual users."[18] Nor did Facebook obtain users' consent before implementing "Tag Suggestions," which uses the unique biometric identifiers generated by the photo comparison data to identify users when a photograph containing their image is uploaded to Facebook.[19] Facebook also misled users' regarding the process for deleting photo comparison information, did not allow users to disable Facebook's collection of biometric data, and did not establish that application developers, the government, and other third parties would not have access to such data.[20]

---

[14] Letter from Marc Rotenberg et al., Exec. Dir., Elec. Privacy Info. Ctr., to Robert Gates, U.S. Dep't of Def. (July 27, 2007), *available at* https://epic.org/privacy/biometrics/epic_iraq_dtbs.pdf.
[15] *Id*.
[16] *Id*. at 1.
[17] *See* EPIC 2011 Facebook Facial Recognition Complaint, *supra* note 7.
[18] *Id*. at 10.
[19] *Id*. at 11.
[20] *Id*. at 16-19.

EPIC's complaint requested that the Commission "investigate Facebook, enjoin its unfair and deceptive business practices, and require Facebook to protect the privacy of Facebook users."[21] Specifically, EPIC requested that the Commission require Facebook to (1) suspend any form of Facebook-initiated "tagging"; (2) avoid misrepresenting the extent to which Facebook maintains and protects the privacy of consumer information; (3) prohibit sharing of identified information with any third party without clearly disclosing the practice and obtaining the affirmative consent of users; and (4) establish a comprehensive privacy program.[22]

Most recently, EPIC Senior Counsel John Verdi spoke at the Commission's Face Facts workshop in December 2011.[23] He explained the risk that facial recognition poses to an individuals' ability to control the disclosure of their identity, and drew important conceptual distinctions, such as that between face detection and facial recognition.

III. Privacy and Security Concerns Raised by the Implementation of Different Facial Recognition Technologies

A. Facial Recognition Technology

Facial recognition technology allows commercial and government entities to use software that automates the detection and recognition of human faces and to identify people in circumstances in which they may not choose to reveal their actual identity. To detect human faces, the software searches images for identifiers including the position, size, and shape of facial features. Three-dimensional facial recognition systems, which use multiple photographs to create 3-D feature maps, are beginning to emerge and promise even greater accuracy.[24]

---

[21] *Id*. at 33.
[22] *Id*.
[23] *See* Face Facts, *supra* note 6.
[24] *See* Timothy C. Faltemier, Kevin W. Bowyer, & Patrick J. Flynn, *A Region Ensemble for 3-D Face Recognition*, 3 IEEE TRANSACTIONS ON INFO. FORENSICS AND SEC. 62 (2008).

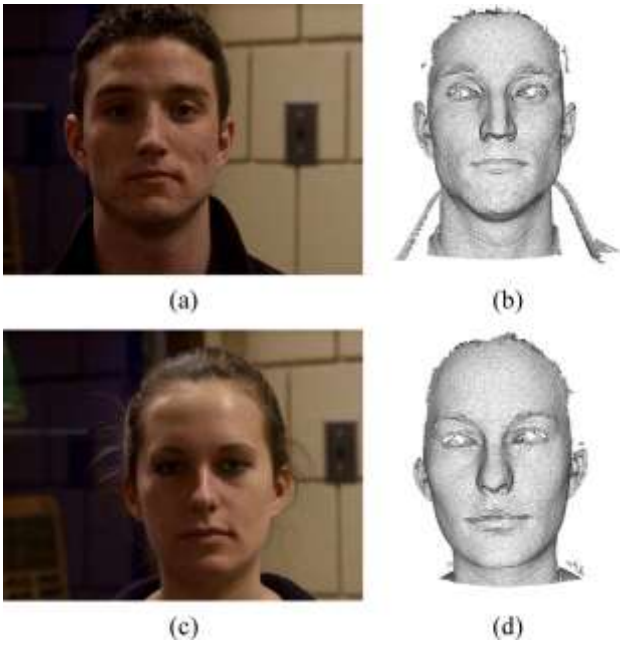

FIGURE 1: Example of 3D facial mapping. From Faltemier (note 24).

Recognition occurs when these identifiers are compared against biometric databases, and the pictures matched with identities. In the past decade, the accuracy of both facial detection and facial recognition techniques has grown significantly, though both false positives and false negatives routinely occur depending on environmental factors, the quality of the matching algorithm, the scope of the database, as well as image quality.[25]

Commercial actors have already implemented this technology in a number of ways. Digital signs can target advertising based on the detected gender and age of viewers.[26] In Japan, stores can train and monitor employees with "smile-scan" facial detection software to ensure employees' facial expressions are sufficiently enthusiastic.[27] Companies like Google, Facebook, and Apple that offer photo album software increasingly use facial recognition technology to efficiently identify the people in photographs, though significant differences in the deployment

[25] David Goldman, *Can You Remain Anonymous?*, CNN (Jan. 13, 2012), *available at* http://money.cnn.com/2012/01/13/technology/face_recognition/.
[26] *Id*.
[27] *Japan Steps Up Use of Facial Recognition Technology*, REUTERS (Jan. 25, 2010), *available at* http://www.3news.co.nz/Japan-steps-up-use-of-face-recognition-technology/tabid/412/articleID/138665/Default.aspx.

of these techniques suggests that companies can adopt standards that are either more or less privacy respectful.[28] For example, deployment of facial recognition in Apple's iPhoto9 leaves the user in control of the image database, while use of facial recognition by Facebook for autotagging photos and by Google for photo identification in Picasa leaves the companies in control of the photo database.[29] In the future, there are predictions that we will be able to take pictures of people on the street and, in real time, scan the internet for matches.[30]

There are four primary risks associated with the increased commercial use of facial recognition technology. First, ubiquitous and near-effortless identification eliminates our ability to control our identities.[31] It will no longer be possible to remain anonymous in public – a legal right that the Supreme Court has recognized carries free speech and liberty implications.[32] Second, there are privacy and security concerns associated with the collection, use, and storage of the facial geometry measurements used for identification. The International Biometrics and Identification Association stated that these measurements, called faceprints, are personally identifiable information.[33] The storage and control of this data must remain secure. Third, a fundamental understanding of the right of privacy is the ability of individuals to decide for themselves when to disclose their actual identity to others.[34] Fourth, an essential aspect of personal security, commonly described as "Basic Access Control," is the ability of the individual

[28] *See* Justin Mitchell, *Making Photo Tagging Easier*, FACEBOOK BLOG (June 30, 2011), http://www.facebook.com/blog.php?post=467145887130; Simpson Garfinkel, *Face Recognition: Clever or Just Plain Creepy?*, TECH. REVIEW (Feb. 27, 2009), *available at* https://www.technologyreview.com/computing/22234/.
[29] *Id*.
[30] *See* Goldman, *supra* note 25.
[31] *See* Ian Kerr & Jennifer Barrigar, *Privacy, Identity and Anonymity*, *in* INTERNATIONAL HANDBOOK OF SURVEILLANCE STUDIES (Kristie Ball et al. eds., forthcoming 2012), *available* at http://iankerr.ca/wp-content/uploads/2011/08/PrivacyIdentityAnonymityScannedfromLibrary.pdf.
[32] See *infra* Part III.B.
[33] INT'L BIOMETRIC & IDENTIFICATION ASS'N, FACE DETECTION & FACE RECOGNITION CONSUMER APPLICATIONS: RECOMMENDATIONS FOR RESPONSIBLE USE (Dec. 2011), *available at* http://www.ibia.org/download/datasets/956/IBIA_recommendations_final.pdf ("[A] faceprint… is a biometric and should be considered as Personally Identifiable Information (PII) when stored in association with other identity meta data. A faceprint should enjoy all the security and privacy protections bestowed upon other PIIs.").
[34] *See generally* ALAN WESTIN, PRIVACY AND FREEDOM (1967).

to know under what circumstances others are seeking access to his or her identity and to make a determination as to whether to reveal actual identity. In the proposed e-Passport, for example, it became clear that to allow a remote read of Passport by a person unknown to the passport holder would raise significant security risks for Americans travelling abroad.[35] The use of facial recognition techniques raises similar threats to personal safety.

The storage of personally identifiable information and the unmasking of a person's identity are especially at risk with facial *recognition* technology. When there is no storage of faceprints and no identification, facial *detection* technology has far fewer security and privacy risks.[36] This report focuses largely on facial recognition technology.

B. Risk of Facial Recognition Technology: Loss of Anonymity

The right to control one's identity is of fundamental importance in the United States. The Supreme Court made this clear in a case recently cited by the Court of Appeals for the D.C. Circuit that declares "both the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person."[37] Controlling one's identity requires the choice to remain anonymous.[38] Courts have vigorously upheld constitutional protections of the right of anonymity in a long line of cases. In *NAACP v. Alabama*, the Court held that requiring identification interfered with "the right of the members to pursue their lawful

[35] Erik Larkin, *Electronic Passports May Make Traveling Americans Targets, Critics Say*, PC World (Apr. 11, 2005 4:00 AM), https://www.pcworld.com/article/120292/electronic_passports_may_make_traveling_americans_targets_critics_say.html.

[36] For a discussion on the differences between detecting faces and storing biometric information for identification, see *id*. at 1-3; DIGITAL SIGNAGE FEDERATION, DIGITAL SIGNAGE PRIVACY STANDARDS 2-3 (Feb. 2011), *available at* http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf.

[37] *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989), cited in *Nat'l Cable & Tele. Assn. v. Fed. Commc'ns. Comm'n*, 559 U.S. 996, 1001 (D.C. Cir. 2009).

[38] *See* Kerr & Barrigan, *supra* note 31.

private interests privately and to associate freely with others."[39] Similarly, in *Talley v. California*, the Court recognized that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[40] The Court recognized how closely tied anonymity and identity are in *Buckley v. American Constitutional Law Foundation*, where they unanimously overturned the portion of a Colorado statute that required people handing out petitions wear nametags.[41] As the Court explained:

> [T]he name badge requirement 'forces circulators to reveal their identities at the same time they deliver their political message,' it operates when reaction to the circulator's message is immediate and 'may be the most intense, emotional, and unreasoned.' … The injury to speech is heightened for the petition circulator because the badge requirement compels personal name identification at the precise moment when the circulator's interest in anonymity is the greatest.[42]

And in *Hiibel v. Sixth Judicial District,* the Supreme Court narrowly upheld by 5-4 a state identification law so long as the individual was only required to say his name and not to actually produce an identity document.[43]

The practical importance of controlling one's identity and retaining the right of anonymity grows more important as technology advances. A name is "no longer a simple identifier," but the key to increasingly interwoven law enforcement databases.[44] Facial recognition technology transfers control over the disclosure of identity and makes it more difficult for subjects to control their identity and protect their anonymity. Law enforcement can use the facial recognition technology to identify protesters in public spaces, threatening First Amendment freedoms and chilling protected political speech.[45]

---

[39] 357 U.S. 449, 466 (1958).
[40] 362 U.S. 60, 65 (1960)
[41] 525 U.S. 182 (1999).
[42] Id at 182 (citations omitted).
[43] Hiibel v. Sixth Judicial Dist., 542 U.S. 177, 185 (2004).
[44] *See id*. at 196 (Stevens, J., dissenting)
[45] *See* Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. TIMES, Sept. 12, 2011.

These threats to our identity and liberty are not mere possibilities. For example one researcher, using a combination of facial recognition technology, an online database of public photographs, and publicly available information on the Internet, obtained identifying information from random passersby, including some subjects' social security numbers.[46] Nothing more than a photograph and the Internet are needed to find the name and private information of a stranger on the street using this technique.[47] One company's website offers to place mobile facial recognition technology "directly in the hands of law enforcement, private security . . . or any other company that needs to be able to identify a person of interest."[48] News reports suggest that at least forty law enforcement units across the U.S. have purchased similar technologies.[49] In Canada, police used facial recognition software to match Vancouver hockey rioters with the provincial driver's license photograph database.[50]Additionally, under the FBI Secure Communities initiative, local police are currently sharing arrestees' and witnesses' fingerprints and other biometric information with DHS to aid immigration enforcement. Immigration and Customs Enforcement advertises Secure Communities as "prioritizing the removal of individuals who present the most significant threats to public safety";[51] in practice, the program fails at this goal. Three states have withdrawn from the Secure Communities program because many deportees did not pose a threat to public safety.[52]

Today, the growing use of facial recognition technology threatens to extinguish our right

[46] Alessandro Acquisti, *Face Recognition Study – FAQ*, CARNEGIE MELLON UNIVERSITY http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/ (last visited Jan. 12, 2012).
[47] *Id*.
[48] *FACER MobileID*, ANIMETRICS (last updated 2012), http://www.animetrics.com/products/MobileID.php.
[49] Zach Howard, *Police to Begin iPhone Iris Scans Amid Privacy Concerns*, REUTERS, July 20, 2011, *available at* http://www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720.
[50] *Insurance Corporation Offers to Help ID Rioters*, CBC NEWS, June 18, 2011.
[51] *Secure Communities*, IMMIGRATION AND CUSTOMS ENFORCEMENT, http://www.ice.gov/secure_communities/.
[52] For example, in Massachusetts more than half of those deported were identified as "non-criminal." Massachusetts Letter Withdrawing from Secure Communities Program (June 3, 2011), *available at* http://epic.org/privacy/secure_communities/sc_ma.pdf. *See also* Illinois Letter (May 4, 2011), *available at* http://epic.org/privacy/secure_communities/sc_ill.pdf; New York Letter (June 1, 2011), *available at* http://www.governor.ny.gov/assets/Secure%20Communities.pdf.

to anonymity. Under *Hiibel*, government use of this technology may be unconstitutional in certain circumstances. As we explained, police may have the right to ask a person their name, but there is currently no basis to seize their actual identity. However, these constitutional protections do not apply when non-state actors threaten our right to anonymity. The use of facial recognition technology by commercial actors and individuals should be limited so that fundamental freedoms, including the right of anonymity are protected.

C. Risk of Facial Recognition Technology: Storage and Use of Sensitive Data

The core security issues raised by facial recognition technology are database security, mistaken identification, identity theft, and data sharing.

1. Identity Theft

Theft or misuse of faceprints or facial geometry data is a serious concern. The FTC has estimated that up to 9 million people are victims of identity theft each year.[53] Companies that use facial recognition technology create large databases of personally identifiable faceprints.[54] There were several well-publicized cases in 2011 where hackers broke into databases and accessed personal records, including credit card information.[55] After all, unlike a credit card or social security number, it's not possible to go out and get a new faceprint if your biometric data is hacked. Thus, all necessary precautions must be taken when facial recognition data is stored.

2. Mistaken Identity

Mistakes in identification are another potential risk of facial recognition technology. The effectiveness of facial recognition technology has grown dramatically in the past decade, due in large part to the improved algorithms of facial recognition systems and improvements in digital

[53] *About Identity Theft*, FED. TRADE COMM'N (last visited Jan. 27, 2011), http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.
[54] See *supra* note 33.
[55] Chris Hinkley, *2011 Hack Retrospective: Learning from Three Significant Attacks*, SECURITYWEEK.COM (Oct. 27, 2011), http://www.securityweek.com/2011-hack-retrospective-learning-three-significant-attacks.

cameras.[56] However, effectiveness can vary widely depending on circumstances.[57]

Facial recognition technology can be used for photograph identification, as on Facebook.[58] With growing numbers of employers, college admissions officers, and others using Facebook and other online services to investigate potential employees and students, an incorrect identification can have real-life consequences on employment or admission opportunities.[59]

Facial recognition mistakes may also have security implications. Some smartphones now use this technology in lieu of passwords.[60] In theory, as faceprints are personally identifiable, this should make a smartphone very secure. However, facial recognition software can often be fooled.[61]

3. Secondary Use

Secondary use of facial recognition data is another risk that must be mitigated. Secondary use is "the use of information collected for one purpose for a different purpose without the data subject's consent."[62] Commercial data-sharing is increasingly common on the Internet. Companies that collection facial recognition data may be tempted to sell it to third parties. However, sharing faceprints and other facial recognition data is problematic. Data-collectors, data-holders, and third-party users of facial recognition data must all have security measures in place to ensure the data is protected. Additionally, because of the personal nature of facial

---

[56] *See* Goldman, *supra* note 25.
[57] *See* LUCAS D. INTRONA & HELEN NISSENBAUM, CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, N.Y.U., FACIAL RECOGNITION TECHNOLOGY: A SURVEY OF POLICY AND IMPLEMENTATION ISSUES 3 (2009), *available at* http://www.nyu.edu/projects/nissenbaum/papers/facial_recognition_report.pdf (listing environment, image age, and camera characteristics as variables influencing the accuracy of facial recognition software).
[58] *See* Mitchell, *supra* note 28.
[59] Jeanette Borzo, *Can Employers Fire over Facebook Gaffes?*, WSJ.COM (Jan. 21, 2011), http://online.wsj.com/article/SB10001424052748703954004576089850685724570.html.
[60] Nathan Olivarez-Giles, *Galaxy Nexus, on Android Ice Cream Sandwich Review*, L.A. TIMES (Dec. 31, 2011), http://latimesblogs.latimes.com/technology/2011/12/samsung-galaxy-nexus-review-android-ice-cream-sandwich-verizon.html ("Ice Cream Sandwich offers users the option of a "Face Unlock" feature that uses facial recognition technology to open the phone from its lock screen.").
[61] *Id*. ("With Face Unlock turned on, I was able to unlock the Galaxy Nexus with an iPhone displaying a photo of myself -- not exactly the most secure option.").
[62] Daniel Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 490 (2006).

recognition data, users should know with whom and why their information shared. Transparency and security are vital.

Transparency is especially necessary when data is shared with the government. Facebook's biometric database may be one of the largest in the world, and a state (not necessarily the United States) may want "pipeline" access to the database.[63] Facebook is already screening every posted photograph to check for illegal photos (for example, of child pornography.)[64] Companies must be transparent about how much government access they allow, especially if it is above and beyond legal requirements.

3. Control

Controlling how, when, and why others seek access to your identity and determining when to reveal it is an essential aspect of personal security, commonly described as "Basic Access Control." In the proposed e-Passport, for example, it became clear that allowing remote reading of passports by a person unknown to the passport holder would raise significant security risks for Americans travelling abroad.[65] Similarly, widespread use of facial recognition technology could allow criminals or threatening individuals to stalk others more easily. This raises a very real threat to personal safety.

IV. The Legal Framework Surrounding Facial Recognition Technology

While the use of facial recognition technology has increased over the past several years, few legal safeguards currently protect consumer privacy and security. The Supreme Court has found that a constitutional right to anonymity exists in many circumstances, but this protection

[63] *See* Bill Snyder, *Facebook Facial Recognition: Why It's a Threat to Your Privacy*, CIO (June 20, 2011), http://www.cio.com/article/684711/Facebook_Facial_Recognition_Why_It_s_a_Threat_to_Your_Privacy; *see also* Summer Said, *Saudi RIM Pact Lifts Hope of Ending U.A.E. Impasse*, WALL ST. JOURNAL (Aug. 7, 2010), *available at* http://online.wsj.com/article/SB10001424052748704182304575414814113575300.html (describing deal that allows Saudi Arabia access to BlackBerry maker RIM's servers to surveil text messages).
[64] Riva Richmond, *Facebook's New Way to Combat Child Pornography*, N.Y. TIMES (May 19, 2011), http://gadgetwise.blogs.nytimes.com/2011/05/19/facebook-to-combat-child-porn-using-microsofts-technology/.
[65] Larkin, *supra* note 35.

extends only to government conduct. We require additional safeguards to protect against the misuse of this technology by commercial entities or other non-governmental actors.

Two states have already implemented protections for sensitive biometric information. The FTC should build on these frameworks to protect consumer privacy and security.

A. Constitutional Protection

In the United States, the Constitution only protects individuals from privacy intrusions by the State, not private companies or other individuals. Thus, while it offers some protection for state misuse of facial recognition technology, no constitutional safeguards exist for commercial actions. Instead, we must look to federal or state statutes for protection.

B. State Biometric Information Protection Statutes

Two states have enacted statutes that specifically protect biometric information. In Illinois, the Biometric Information Privacy Act of 2008 ("BIPA") regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[66] BIPA's definition of biometric information includes "face geometry" but excludes photographs.[67] This probably includes facial recognition data based on facial geometry.

The act includes several key requirements that biometric data handlers must meet, including:

- develop a privacy policy and make it available to the public,[68]
- establish a data retention schedule that includes guidelines for destroying data either 1) when it is no longer necessary for the purpose it was collected or 2) within three years of collection, whichever comes first,[69]
- inform subjects in writing of the collection of this type of information and the purposes and length of time it will be stored,[70]

[66] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/ (2011).
[67] *Id*. at § 5.
[68] *Id*. at § 15(a).
[69] *Id*.
[70] *Id*. at. §15(b).

- obtain written consent of the subject before collecting, storing, or using any biometric data,[71]
- store biometric information using security techniques at least as protective as those for other sensitive information,[72] and
- cannot sell biometric information, even with consent.[73]

Finally, BIPA provides a private right of action with penalties up to $5,000 plus attorneys' fees.[74]

Texas law similarly regulates biometric information, although less robustly. Section 503.001 of the Texas Business and Commerce Code prohibits the capture of any "biometric identifiers" without 1) informing the individual of the capture and 2) obtaining consent.[75] The law also regulates the sale, lease, and disclosure of biometric identifiers and requires that the companies storing, transmitting, or protecting biometric identifiers use "reasonable care . . . in a manner that is the same as or more protective" as other confidential data.[76] The law defines biometric identifiers to include a "record of hand or face geometry"[77] and provides a civil penalty of up to $25,000 per violation.[78]

C. Foreign Biometric Information Protection Laws

1. European Union

The 1995 European Union Data Protection Directive sets out privacy requirements for member states to transpose into national law.[79] The E.U's approach to consumer privacy is generalist rather than the sectoral approach of the United States.[80] Thus, E.U. countries impose

[71] *Id*. at § 15(b)(3).
[72] *Id*. at § 15(e).
[73] *Id*. at § 15(c).
[74] *Id*. at § 20.
[75] TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2011).
[76] *Id*. § 503.001(c).
[77] *Id*. § 503.001(a).
[78] *Id*. § 503.001(d).
[79] Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Data Privacy Directive].
[80] *See U.S.-E.U. Safe Harbor Overview*, *supra* note 78.

certain obligations imposed on data controllers handling "personal data."[81] Personal data includes any information that relates to an "identified or identifiable natural person;"[82] this includes biometric data.[83]

EU requirements for processing personal information include:

- Collection and Use Limitations: Personal data must be "processed fairly and lawfully," collected for "specified, explicit and legitimate purposes," and not processed incompatibly with these purposes.[84]
- Accuracy: Personal data must be accurate and, where necessary, up to date.[85]
- Retention: Personal data shall not be kept in an identifiable form for longer than is necessary.[86]
- Consent: Processing of personal data requires the unambiguous consent of the data subject or it must qualify for certain exceptions.[87]
- Duty to Inform: The data subject must know who is collecting the data, why they are collecting it, and to whom it is going.[88]
- Right of Access: The data subject has the right to access the data undergoing processing and, where appropriate, to rectify, erase, or block its processing.[89]

There is no required private right of action in European countries, but consumers can lodge complains with country-specific privacy authorities, who have the capability of monitoring data protection in that country and initiating legal action if the privacy obligations are violated.[90]

On January 25, 2012, the European Commissioner released the draft Regulation on Data Protection – a major reform of the original 1995 directive.[91] This proposed new regulation

[81] Data Protection Directive, art. 1.
[82] *Id*. at art. 2.
[83] *See supra* note 33.
[84] Data Protection Directive, art. 6.
[85] *Id*.
[86] *Id*.
[87] *Id*. at art. 7. These exceptions include that the processing be necessary for a contract to which the data subject agreed, for compliance with legal obligations, to protect the vital interests of the data subject, or for the public interest. *Id*.
[88] *Id*. at art. 10.
[89] *Id*.
[90] *Id*. at art. 28.
[91] *Commission Proposal for a Regulation of the European Parliament and of the Council*, at 51-53, COM (2012) 11 final (Jan. 25, 2012).

defines biometric data as "any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images."[92] Any company processing biometric data must carry out a "data protection impact assessment," in addition to meeting all legal obligations associated with personal data.[93]

In similar fashion, the Council of Europe has recently proposed to add genetic and biometric identification to its listings of special categories of data as well as the definition of personally identifiable information in the Council of Europe Privacy Convention.[94]

2. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The Organization for Economic Cooperation and Development ("OECD") Guidelines contain a set of privacy principles that were adopted in 1980.[95] The privacy principles include:

> Collection Limitation Principle
> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> Data Quality Principle
> Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> Purpose Specification Principle
> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> Use Limitation Principle
> Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

[92] *Id*. at art 4.
[93] *Id*. at art. 33.
[94] Eur. Consult. Ass., *The need for a global consideration of the human rights implications of biometrics*, Doc. No. 12528 (2011).
[95] *OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* (C(80)58/FINAL) (Sept. 23, 1980), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2.

a) with the consent of the data subject; or
b) by the authority of law.

Security Safeguards Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle
An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle
A data controller should be accountable for complying with measures which give effect to the principles stated above.

The Guidelines apply to "personal data" which is broadly defined as "any information relating to an identified or identifiable individual."[96] Because faceprints and other biometric data are related to an "identified or identifiable" individual, they are protected by the OECD guidelines.

V. Recommended Facial Recognition Framework

Because of the special risks involved with biometric data, including facial recognition data and faceprints, the FTC should require companies collecting, handling, storing, and

[96] *Id*.

transmitting this kind of data[97] to adhere to a framework of Fair Information Practices. The adoption of these principles would make the United States a leader in protecting the facial recognition data of consumers. These principles should include:

Limitations on collection and use

Biometric data should be processed fairly and lawfully, collected for specified, explicit and legitimate purposes, and not processed in a manner that is incompatible with these specified purposes. Secondary analysis of biometric information should not be permitted without free and informed consent.

The European Union and Canada have similar limitations on the collection and use of personal data. These limitations protect consumers from unfair or excessive collections of sensitive biometric data for commercial gain.

Informed Consent:

Enrollment must be voluntary and informed. When possible, companies should acquire subjects' affirmative express consent.[98] The data subject must know who is collecting their data, why they are collecting it, and to whom it will be given before enrolling. Data-handlers should create and publicly post comprehensive privacy policies.

Because of the special privacy and security concerns associated with facial recognition data, consumers should be fully informed of its use and grant affirmative consent prior to participation. Illinois and Texas law require this of biometric data holders, as do Europe, Canada, and Australia.[99]

However, for American users, knowledgeable, informative consent to facial recognition technology is currently lacking. For example, the following warning is taken from Facebook's

[97] This does not include companies using facial detection technology, only facial recognition technology. See Section III.A for a discussion of the different risks.
[98] The identifier attached to the biometric profile can be contextual or unique. If a profile is identified by a chosen identifier, such as "Grandma" or "Pete," the privacy risks are lower than if the profile is identified by a unique identifier, such as full name and address. It may not be possible to obtain consent for contextual identification. *See* Garfinkel, *supra* note 28. However, all other Fair Information Principles should still apply.
[99] 740 ILL. COMP. STAT. 14/15(b); TEX. BUS. & COM. CODE ANN. § 503.001(b) (West 2011).

photo uploading system and entirely fails at informing users how their photo data will be used or to provide any meaningful consent for use..

FIGURE 2: Facebook notice for facial recognition tagging technology (January 27, 2012).

The Facebook proposed consent order requires notification and "affirmative express consent." [100] That is clearly lacking in this picture.

Security:

Biometric data should be encrypted and stored separately from other data. Access to this data should be limited to those who need it. Data-handlers should assure the security of this data during transmission to third-parties.

Because of the special risks of identity theft associated with facial recognition data and biometric data, commercial entities must ensure database security is sufficient. The Australian Privacy Code and Illinois and Texas state law include requirements to manage these special risks.[101] The FTC should expand this protection nationwide.

Accessibility:

The data subject has the right to access the data undergoing processing and, where appropriate, to rectify, erase, or block its processing.

[100] Facebook, Inc., FTC File No. 092-3184, at 5 (2011) (Fed. Trade Comm'n. Agreement Containing Consent Order), http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf [hereinafter Facebook Consent Order].
[101] *See, e.g.*, 740 ILL. COMP. STAT. 14/15(e); TEX. BUS. & COM. CODE ANN. § 503.001(c) (West 2011); *Privacy Code*, *supra* note 113, at Principle 12.

Users should have access to and control over their personal information. Companies should create an easy mechanism through which users can determine what personal information the company is storing and, if desired, have the information removed from the company's databases. The proposed Facebook consent order requires that a user's information on Facebook's servers be made inaccessible to a third party "a reasonable period of time, not to exceed thirty (30) days, from the time that the user has deleted such information."[102]

Limited Data Retention:

Data-handlers should establish a data retention schedule that includes guidelines for destroying biometric data either 1) when it is no longer necessary for the purpose it was collected or 2) within three years of collection, whichever comes first.

Because unsecured facial recognition data has special security and privacy risks, it is important to limit the how long the data is retained. Illinois state law[103] and the EU Data Protection Directive[104] include similar requirements.

Accountability:

There must be some consequence for companies that fail to abide by these Principles. This could include a private right of action,[105] regulatory action, or regular audits or privacy assessments.

If a data handler violates either the Fair Information Principles or its privacy policies, there should be clear consequences. Private rights of action provide one means of enforcement. Private rights of action strengthen enforcement and allow individuals to seek remedies, empowering consumers to enforce the law themselves and creating a strong disincentive for irresponsible breaches of consumer privacy. The Commission could also regulate some abuses

[102] Facebook Consent Order, *supra* note 99, at 5.
[103] 740 ILL. COMP. STAT. 14/15(a).
[104] Data Protection Directive, *supra* note 78, at art. 6
[105] *See, e.g.*, 740 ILL. COMP. STAT. 14/20.

of facial recognition in the consumer context under the Federal Trade Commission Act. The FTC Act prohibits unfair and deceptive acts and practices, and empowers the Commission to enforce the Act's prohibitions.[106] A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[107] An act or practice is deceptive if it involves a representation, omission, or practice that is likely to mislead the consumer acting reasonably under the circumstances, to the consumer's detriment."[108]

VII. Conclusion

Because of the risks inherent in facial recognition technology, it is vital for the FTC to create a framework within which companies can work to ensure the security and privacy of consumers. Commercial actors should not deploy facial techniques until adequate safeguards are established. As such safeguards have not yet been established, EPIC would recommend a moratorium on the commercial deployment of these techniques.

As more than 100 hundred privacy organizations and privacy experts stated in the Madrid Declaration.[109] There should be

> A moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate.

---

[106] *See* 15 U.S.C. § 45.
[107] 15 U.S.C. § 45(n); *see, e.g.*, *Fed. Trade Comm'n v. Seismic Entertainment Productions, Inc.*, Civ. No. 1:04-CV-00377 (Nov. 21, 2006) (finding that unauthorized changes to users' computers that affected the functionality of the computers as a result of Seismic's anti-spyware software constituted a "substantial injury without countervailing benefits.").
[108] Fed. Trade Comm'n, FTC Policy Statement on Deception (1983), *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.
[109] The Madrid Privacy Declaration, *available at* http://thepublicvoice.org/madrid-declaration/.

Sincerely,

Marc Rotenberg
EPIC Executive Director

David Jacobs
EPIC Consumer Privacy Fellow

Maria Elena Stiteler
EPIC Legal Intern

Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)