KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

December 6, 2011

Seeing Is ID'ing: Facial Recognition & Privacy

CDT comments in advance of the Federal Trade Commission's workshop on facial recognition.

Facial recognition is increasingly used in a variety of contexts – from photo tagging on social networking sites to targeting advertisements in stores or public places to security and authentication – but the technology poses complex privacy issues that do not fit squarely with present laws. Facial recognition and other automated systems that collect sensitive information about individuals in public places have the potential to significantly alter the ways in which individuals are identified, tracked and marketed to. The privacy issues associated with facial recognition are compounded by the wide availability of this powerful technology. Facial recognition is no longer used just by entities with substantial technical and financial resources, such as government agencies or corporate actors; the sophisticated capability to detect unique facial characteristics is making its way into handheld consumer devices and free software packages, opening the door to many millions of users.[1] With such a broad user base and wide variety of applications, facial recognition technology will be abused.

A mix of government regulation, industry self-regulation, and privacy enhancing technologies can give consumers a greater measure of control over how facial recognition is used without unduly limiting the benefits of the technology or burdening free expression. However, current laws apply only indirectly to facial recognition and offer consumers no real choices with regard to the technology. To their credit, many businesses are already mindful of privacy issues associated with facial recognition and have taken steps to reduce the impact the technology has on consumers' privacy. While these self-regulatory steps are very important, industry standards today do not encompass the full range of commercial applications for facial recognition in the United States. The nature of the technology and the variety of contexts in which it can be used precludes any simple solution to the privacy issues posed by facial recognition. Moroever, given the numerous other ways to identify and track consumers using biometric information, it is doubtful that a solution addressing facial recognition alone is even appropriate.

This paper briefly describes facial recognition technology, some of its commercial applications, and its impact on privacy. (Although there are clearly critical privacy issues related to the use of facial recognition for law enforcement and security, we largely focus

[1] Phil Leggetter, *Face.com: Free Face Recognition API for Photos*, Programmable Web (Feb. 10, 2011), http://blog.programmableweb.com/2011/02/10/face-com-free-face-recognition-api-for-photos.

on commercial uses.) This paper explains the inapplicability of current laws to facial recognition and details important industry self-regulatory efforts. Finally, this paper proposes policy approaches for addressing facial recognition.

I. Technologies That Enable Facial Recognition Are Growing More Powerful

Facial recognition algorithms generally allow computers to analyze visual input (such as photos or video) to distinguish human faces and identify individual facial characteristics. To avoid defining facial recognition too narrowly, it is worth noting that there are several methods of "facial recognition" – for example, a geometric approach calculates the location of and spatial relationship between certain facial features, a photometric approach interprets a face as a weighted combination of standardized faces, and skin texture analysis maps the unique placement of pores, lines, and spots on an individual's skin.[2] These techniques may be used separately or they may be used in combination with each other to increase accuracy.[3] An important subset of facial recognition is "face detection" – whereby the program merely recognizes a human face and does not retain identifiable information, such as unique geometric data points. From a privacy perspective, face detection is far less troublesome than facial recognition.

Facial recognition systems have become quite accurate and fast. In 2010, the National Institute of Standards and Technology tested various facial recognition systems and found that the best algorithm correctly recognized 92% of unknown individuals from a database of 1.6 million criminal records.[4] In 2003, some facial recognition systems could run comparisons at a rate of 70 million images per minute.[5] The sophistication of computer vision generally is also quickly progressing. In 2010, GE Global Research claimed that its facial recognition system could recognize individuals at a distance of 15-20 meters and track an individual from a distance of 25-50 meters.[6] Visual sensors can estimate an individual's emotional state by measuring minutely shifting facial features.[7]

---

[2] Bir Bhanu & Ju Han, *Human Recognition at a Distance in Video: Advances in Computer Vision and Pattern Recognition* at vii (Springer 2010); *see also* Jean-Sebastien Pierrard & Thomas Vetter, *Skin Detail Analysis for Face Recognition*, 2007 IEEE Conference on Computer Vision and Pattern Recognition 1, 1-8 (2007), http://www.computer.org/portal/web/csdl/doi/10.1109/CVPR.2007.383264.

[3] L-1 Identity Solutions, FaceIt Argus: Scalable Face Screening with Real-time Alarming, http://www.l1id.com/pages/71-facial-screening (last visited Nov. 28, 2011).

[4] Patrick J. Grother et al., Multiple-Biometric Evaluation (MBE) 2010: Report on the Evaluation of 2D Still-Image Face Recognition Algorithms, NIST Interagency Report No. 7709 (Aug. 24, 2011), *available at* http://biometrics.nist.gov/cs_links/NIST_MBE_STILL_first_public_report_v27.pdf.

[5] David McCormack. Note, *Can Corporate America Secure Our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Recognition Technology*. 8 B.U. J. Sci. & Tech. L. 128, 131 (Winter 2003).

[6] Frederick W. Wheeler, *Face Recognition at a Distance for Surveillance Applications*, Proc. Of the IEEE International Conf. on Biometrics: Theory, Applications, and Systems (Sept. 2010).

[7] Kelvin Low, *Smile at Work—Or the Happiness Detector Will Ding You*, CNET Technology News (July 13, 2009), http://news.cnet.com/8301-17938_105-10285578-1.html.

MIT researchers recently announced the development of a system that uses automatic face detection and color analysis to measure heart rate, blood oxygen levels, and blood pressure – potentially exposing medical conditions of individuals within the camera frame.[8]

The wide availability of photos and videos on the Internet enables facial recognition systems to match online photos with the individual before the camera. This enhances the facial recognition system's ability to identify individuals by name (as opposed to just unique geometric data points) and to locate other online information associated with the individual. Because so many online images are freely available, a facial recognition program need not purchase access to a closed, proprietary data set to link unique facial characteristics with a particular identity – the program could merely search through images on one of many open platforms. The quantity of photographs and video featuring individuals' faces on the Internet (both publicly available and in closed sharing systems) has seen explosive growth in recent years. YouTube was uploading 35 hours of video per minute in 2010.[9] Flickr uploaded its 5 billionth photo in September 2010.[10] Facebook reportedly possessed an estimated 60 billion photos by late 2010 (up from 15 billion as of April 2009), with tens of thousands photos in an average individual Facebook user's social network – and Facebook now has more than 800 million active users.[11]

II. Broad Commercial Applications

As the above figures suggest, hundreds of millions of individuals – whether they know it or not – are currently participating in commercial facial recognition systems. That tally could easily surpass a billion individuals if one includes the face detection features installed in most modern compact digital cameras. Facial recognition has business potential in a wide variety of contexts, and the number of participating individuals is only bound to rise as the technology grows cheaper, more effective, and more popular.

Numerous companies – such as Facebook, Apple, and Google – offer automatic facial recognition or detection as part of a more extensive package of services. For example, Google's Picasa photo editing software and Picasa Web Albums utilize face recognition by default. Picasa prompts a user to tag names to clusters of matching faces in photos

---

[8] Ming-Zher Poh et al., *Non-contact, Automated Cardiac Pulse Measurements Using Video Imaging and Blind Source Separation*, 18 Optics Express 10762 (2010), *available at* http://www.opticsinfobase.org/abstract.cfm?uri=oe-18-10-10762; *see also* David L. Chandler, *Your Vital Signs, On Camera*, MIT News (Oct. 4, 2010), http://web.mit.edu/newsoffice/2010/pulse-camera-1004.html.

[9] Pingdom, *Internet 2010 in Numbers*, Royal Pingdom (Jan. 12, 2011), http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers.

[10] *Id.*

[11] Natalie Marsan, *Facebook Photo Trends*, Pixable Blog (Feb. 14, 2011), http://blog.pixable.com//2011/02/14/facebook-photo-trends-infographic.

loaded into Picasa.[12] Users may opt out of sharing tags when they upload photos from Picasa to Picasa Web Albums.[13] Google+ and Picasa Web Albums are integrated – users connected through the Google+ social network may add tags to each other's photos shared through either service. Google+ tags will not link to a user's Google+ profile without that user's permission.

Facebook took a slightly different approach. Facebook's facial recognition feature is also activated by default for the social networking site's users. When a Facebook user with facial recognition functionality activated uploads a photo to Facebook, Facebook will automatically locate faces in the photo that resemble the user's Facebook friends and will suggest the user tag the photo with the friends' names. According to Facebook, facial recognition-based tags will only be suggested for friends that the user has manually tagged at least once. The user is prompted to "save tags" of all the tagged friends, or "skip tagging friends." Upon saving the tags, the tags are subsequently linked to the friends' Facebook profiles and all the other pictures in which the friend is tagged, and other Facebook users can see those pictures if the user's privacy settings permit it. The tagged user receives a notice and can remove the tags after the fact, though users can require that they be given the opportunity to approve tags before the photos are linked their profiles. Facebook allows users to opt out of "tag suggestions" in its privacy settings, but this may not opt Facebook users out of the site's use of facial recognition on the photos users upload to the site.

Other companies – such as Polar Rose, Riya, PhotoTagger, and Face.com – developed face recognition software as a third party program that can be used in conjunction with Facebook, Flickr, and other online image hosting services. Polar Rose and Riya were purchased by Apple and Google, respectively, in 2010. Prior to this, both companies offered services akin to "visual search engines" whereby users could label photos of individuals or objects and then find other photos of the same individual or object – i.e., tagging a photo of an individual taken with a mobile phone and locating more photos of the individual on the open web.[14]

A growing number of commercial facial recognition and detection applications are directed at recording faces in public places and business establishments, rather than online.[15] An important example of this is digital signage advertising. Digital signage, also known as digital out-of-home (DOOH) or "smart signs," is a communications medium

---

[12] Google, Picasa Support: Add Name Tags in Picasa, http://picasa.google.com/support/bin/answer.py?answer=156272 (last accessed Nov. 3, 2011).

[13] Google, Picasa Support: Uploading Name Tags from Picasa, http://picasa.google.com/support/bin/answer.py?hl=en&answer=161870 (last visited Nov. 3, 2011).

[14] Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 Harv. L. Rev. 1870, 1871 (May 2007).

[15] *See, e.g.,* SceneTap, SceneTap: A New Look into Nightlife, http://www.scenetap.com (last visited Nov. 28, 2011).

characterized by a dynamic display presenting messages in a public environment.[16] One of the most common examples of digital signage is a flat screen television displaying a loop of advertisements in a retail store. Other digital signage units take the form of kiosks, projectors or digital billboards. The units appear in a broad range of settings, including in shopping malls, hospitals and doctors' offices, public transportation, gas stations, restaurants, government facilities and public schools. Digital signage has rapidly grown into a multibillion-dollar industry over the past decade. There were an estimated 2 million displays in the United States in 2010, though there are many more screens worldwide – particularly in China.[17] The digital signage industry is exploring several technologies to improve audience measurement and interactivity, especially facial detection.[18]

Most digital signage systems are not yet configured to identify individuals, but instead calculate a passerby's age and gender, and determine how long an individual watches the display. The advertisement on the screen can then change to match the consumer's profile. Other systems note only gender, and still others merely count the number of faces that see the screen (gaze-tracking). Digital signage systems that measure and react to consumers' emotional state have also been developed.[19] Notably, many digital signs using facial recognition or detection are not labeled as such and, when asked, some digital signage companies are reticent to disclose where facial recognition is employed.[20] By using identification and interactivity technologies – such as facial recognition or detection – to log consumers' location and activities in order to deliver advertising targeted to individual interests, the digital signage industry is building an offline version of the behavioral advertising that currently occurs online.

---

[16] Digital Signage Resource, Terms Glossary: Digital Signage, http://www.digitalsignageresource.com/digital-signage-glossary-of-terms.asp?modes=3&col=term&term=digital_signage (last visited Nov. 28, 2011).

[17] Bill Gerba, *7 Million Screens: Making Sense of Digital Signage Growth Rates*, The Digital Signage Insider (June 16, 2011), http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/7_Million_Screens__Making_Sense_of_Digital_Signage_Growth_Rates-802.html.

[18] Other technologies digital signage is incorporating include RFID, Bluetooth, license plate scanners, and mobile marketing. *See* Center for Democracy & Technology, *Safeguarding Privacy in the Digital Signage Industry*, CDT Policy Posts (Mar. 31, 2010), http://www.cdt.org/policy/safeguarding-privacy-digital-signage-industry.

[19] *See, e.g.*, Affective Interfaces, What This Does / How We Do It, http://www.affectiveinterfaces.com/2009/09/what-this-does (last visited Nov. 29, 2011). *See also* Juliane Exeler et al., *eMir: Digital Signs that react to Audience Emotion*, Workshop on Pervasive Advertising 38 (2009), http://pervasiveadvertising.org/wp-content/uploads/2011/03/proceedings.pdf.

[20] James Silver, *When Advertising Gets in Your Face*, Wired UK Magazine (June 15, 2009), *available at* http://www.wired.co.uk/magazine/archive/2009/07/features/ads-can-now-read--you; Aimee Levitt, *The Chesterfield Mall Is Watching You*, Riverfront Times Blog (Feb. 19, 2009), http://blogs.riverfronttimes.com/dailyrft/2009/02/the_chesterfield_mall_is_watching_you.php.

A key development in facial recognition is its integration into mobile phones and other consumer devices. Apple's iOS 5, Windows Mango, and Google's Android 4.0 mobile operating systems include face detection and recognition APIs.[21] This will ultimately enable developers to incorporate facial recognition into a broad range of apps and provide developers with data gathered through facial recognition. Although consumers could already access free facial recognition software for their home computers and Internet services, the technology's inclusion in mobile devices gives many consumers greater ability to quickly take a picture and apply facial recognition to individuals in public spaces.

III. Privacy Protection Is in the Interest of Both Consumers and Businesses

CDT conceptualizes facial recognition's impact on privacy on three general levels:

- Level I: *Individual counting*. Consumers' facial information is gathered on an aggregate basis and not used for tailoring advertisements or messages to the individuals. No retained information, including images, links to individuals or their property. Example: facial detection systems that track gazes or record passerby demographics, but do not store facial images or contextualize ads. This is the least privacy-intrusive form of facial recognition.

- Level II: *Individual targeting*. Consumers' facial information is collected on an aggregate basis and is used for tailoring contextual advertisements or other messages to individuals. No retained information, including images, links to individuals or their property. Example: systems that record passerby demographics and contextualize ads accordingly.

- Level III: *Individual identification*. Consumers' facial information is collected on an individual and aggregate basis and may be used for tailoring advertisements or other messages to the individual. Facial information is linked to individual identity or an individual's property. Example: facial recognition systems that record the unique biometric data points of an individual's face in order to pinpoint images of the individual on the web or log that individual's physical location.

The key privacy interest that commercial facial recognition affects is, obviously, identification of an individual through facial features alone. Without facial recognition technology, a stranger seeking to easily and quickly identify an individual would need more information than mere facial features. Thus, most individuals in public may expect that few businesses and passersby would recognize the individual's face, fewer would

[21] Tom, *Face Detection in iOS 5*, b2cloud Blog (Oct. 26, 2011), http://b2cloud.com.au/how-to-guides/face-detection-in-ios-5; *see also* Brad Molen, *Windows 7.5 Mango In-depth Preview (Video)*, Engadget (June 27, 2011), http://www.engadget.com/2011/06/27/windows-phone-7-5-mango-in-depth-preview-video; *see also* Ryan Paul, *First look: Android 4.0 SDK Opens Up Face Recognition APIs*, Ars Technica (Oct. 21, 2011), http://arstechnica.com/gadgets/news/2011/10/first-look-android-40-sdk-opens-up-face-recognition-apis.ars.

affix a name to the face, and fewer still would be able to associate the face with internet behavior, travel patterns, or other profiles.[22] Facial recognition technology can fundamentally change that dynamic, enabling any marketer, agency, or random stranger to collect – openly or in secret – and share the identities and associated personal information of any individual whose face is captured by the camera. Databases built from commercial use of facial recognition can be accessed or re-purposed for law enforcement surveillance.[23] Deployed widely enough, a network of facial recognition cameras can track individuals as they move from place to place.[24] Unlike other tracking methods, such as GPS or RFID, facial recognition does not require the tracked individual to carry any special device or tag, further reducing consumers' ability to thwart unwanted tracking.

Traditional Constitutional law is often read as holding that Americans have no "expectation of privacy" in information they voluntarily reveal in public places. Courts justified this theory by pointing out that anybody can observe an individual in public, and therefore, the theory goes, using electronic devices such as a camera to augment normal human senses and take pictures in public places is not subject to the Fourth Amendment.[25] On a practical level, this theory is rapidly becoming outdated. CDT and others have urged the Supreme Court, in the pending *U.S. v. Jones* case, to rule that government use of GPS to track a person – even in public places – is a search under the Fourth Amendment, due largely to the stark differences between GPS tracking and human observation.[26] In the context of facial recognition, it would require extraordinary effort to deploy a human being - even a team of human beings - 24 hours a day to capture facial details of all passersby, identify or link associated online content to the individuals, target messages to the individuals, and then retain the data for later use. It is simply no longer reasonable to equate the human eye and sophisticated computer vision connected to vast networks. In any case, the baseline of privacy protection afforded by the Constitution is not the end of the debate; the modern history of privacy law in the US has been dominated by Congress establishing rules that go beyond the Constitutional minimum. And, of course, the federal Constitution does not address the privacy

---

[22] *See* Alessandro Acquisti et al., Draft FAQ for *Faces of Facebook: Privacy in the Age of Augmented Reality* (forthcoming), http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ (last visited Nov. 28, 2011).

[23] *See* Aliya Sternstein, *FBI to Launch Nationwide Facial Recognition Service*, Nextgov (Oct. 7, 2011), http://www.nextgov.com/nextgov/ng_20111007_6100.php?oref=rss.

[24] *See* Naomi Klein, *China's All-seeing Eye*, Rolling Stone, May 29, 2008, *available at* http://www.naomiklein.org/articles/2008/05/chinas-all-seeing-eye.

[25] *See generally* Katz v. United States, 389 U.S. 347 (1967), *available at* http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZC1.html, and Dow Chemical Co. v. United States, 476 U.S. 227 (1986), *available at* http://supreme.justia.com/us/476/227/case.html.

[26] Amicus Brief of CDT, EFF, et al in U.S. v Jones 23 (Oct. 3, 2011) http://www.cdt.org/files/pdfs/Amicus_CDT_EFF_GPS_vehicle_tracking.pdf..

implications of private conduct of businesses and individuals undertaken without government involvement.

In the context of digital signage, consumers and companies are already wary of the privacy implications of facial recognition. The reaction to digital signage parallels the controversy associated with online behavioral advertising. A 2009 study of consumer attitudes towards behavioral advertising found two-thirds of Americans "definitely would not" allow marketers to track them online, even if the tracking is anonymous.[27] The study also found 90% of young adults reject advertising tailored to them based on offline activities. Anecdotally, comments to blog posts and news articles on facial recognition in digital signage indicate many consumers have little faith that digital signage companies will protect consumer data gathered via facial recognition.[28] A New York Times article on billboards with facial recognition prompted a major DOOH company to publicly defend its privacy practices.[29] Nonetheless, it is likely that digital signage media will one day routinely identify individuals for the simple reason that it will be profitable to do so.

Many companies using facial recognition and detection appreciate these risks and incentives and have taken steps to protect consumer privacy. Privacy considerations persuaded Google to withhold a facial recognition enhancement it had created for its Google Goggles mobile app; the company stated that it would not "add face recognition to our apps or product features unless we have strong privacy protections in place."[30] Some digital signage industry figures have said that companies must guarantee consumer privacy, while others have cited unresolved privacy issues as an obstacle to using facial recognition technology for advertising purposes.[31] To their credit, at least two digital signage industry associations have adopted privacy standards, one of which – the

---

[27] Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It 3 (Sep. 2009), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/Turow.pdf.

[28] Nilay Patel, *TruMedia Says Its Facial-recognition Billboards Will Never Record Video, It Won't Share with Cops* – User Comments, Engadget (June 10, 2008), http://engadget.com/2008/06/10/trumedia-says-its-facial-recognition-billboards-will-never-recor/#comments; *see also* Tom Ryan, *From Sci-Fi to Retail: Face-scanning Technology* – User Comments, RetailWire (Jan. 21, 2011), http://www.retailwire.com/news/article.cfm/15015?.

[29] George Murphy, Letter to the Editor, *Billboards and Privacy*, N.Y. Times, June 7, 2008, *available at* http://www.nytimes.com/2008/06/07/opinion/lweb07billboards.html.

[30] Amir Efrati, *Google Acquires Facial Recognition Technology Company*, The Wall Street Journal Blog (July 22, 2011), http://blogs.wsj.com/digits/2011/07/22/google-acquires-facial-recognition-technology-company.

[31] Bill Gerpa, *Digital Signage Networks Must Guarantee Viewer Privacy*, The Digital Signage Insider (Aug. 1, 2008), http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Digital_signage_networks_must_guarantee_viewer_privacy-569.html.

Digital Signage Federation Privacy Standards – is based on Fair Information Practice Principles, discussed in more detail below.[32]

With such high privacy stakes and fierce public sentiment, businesses have a strong interest in promoting transparency and consumer privacy protection for facial recognition use across industries. Secrecy magnifies consumers' sense that their privacy is being invaded – if companies try to hide the fact that they are using facial recognition, it will sensationalize the issue and lead consumers to more deeply distrust the technology. It will be less expensive for companies that use facial recognition to integrate privacy controls now – while the technology is still gaining traction commercially – than it will be to retrofit privacy protections onto existing systems. It will only take a few bad apples that flout consumer privacy expectations to spoil public trust in companies' promises to use facial recognition wisely. How companies handle facial recognition privacy issues today will affect the way the public, regulators, and advertisers perceive the businesses that use the technology, as well as the technology's direction in the future. It is particularly important for companies using facial recognition to take a proactive stance on privacy because of the lack of applicable laws.

IV. Current Federal and State Privacy Laws Do Not Adequately Protect Consumers

Federal laws – and nearly all state laws – do not provide American consumers with basic privacy protections when it comes to biometric information collected for commercial purposes online or offline. Federal law does not explicitly address private sector use of facial recognition technology, although federal law does punish the use of biometric information for identity theft or fraud,[33] and both the Privacy Act and Office of Management and Budget memoranda cover biometric information held by government agencies.[34] Federal and state laws that prohibit the secret photographing or videotaping of individuals are narrowly written and do not apply to the vast majority of public or commercial spaces.[35]

---

[32] These internationally recognized principles are reflected (although often incompletely) in many privacy laws in the U.S. and are also the basis of more comprehensive privacy laws internationally, such as the European Union's Data Protection Directive. See Dep't of Homeland Sec., The Fair Information Practice Principles: Framework for Policy at the Department of Homeland Security, Privacy Policy Guidance Memorandum No. 2008-01 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy privacy_policyguide_2008-01.pdf.

[33] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007, *codified at* 18 U.S.C. § 1028.

[34] Privacy Act of 1974, Public Law No. 93-579, *codified at* 5 U.S.C. § 552A(a)(4). See also, Clay Johnson III, Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, Office of Management and Budget, 1 fn. 1, (May 22, 2007).

[35] For example, the Federal Video Voyeurism Prevention Act of 2004 prohibits knowingly capturing an image of the "private area" of an individual without consent in circumstances in which a reasonable person would believe he or she could disrobe in privacy. The Act only applies to federal land – the special maritime and territorial jurisdictions of the United States – rather than

State laws have very little to say on commercial use of facial recognition. One exception is Illinois' Biometric Information Privacy Act of 2008. The Act regulates the collection, use, and storage of biometric information by private entities, covering "biometric identifiers" – which includes "face geometry" but excludes photographs – regardless of where the information is collected.[36] Under the Illinois law, before collecting biometric information, any private entity – which includes individuals, but not government agencies – must provide the individual with notice that the information is being collected, including the duration of the period in which the information will stored, and used, and the individual must consent through a written release.[37] The biometric information must be destroyed when the initial purpose for collecting the information has been satisfied, or within three years of the individual's last interaction with the private entity."[38] Under the Act, private entities are prohibited from selling, trading, or otherwise profiting from an individual's biometric information, and they may not disclose or disseminate the information without obtaining the individual's consent unless the disclosure is required by law or pursuant to a valid warrant or subpoena.[39]

Some federal legislation proposed in the 112th Congress would address biometric information in limited ways. For example, data security bills would require commercial entities to secure biometric information they maintain and to notify consumers of a breach of that information.[40] Another example is the Commercial Privacy Bill of Rights Act of 2011, which covers personally identifiable information, which includes "[b]iometric data about [an] individual, including fingerprints and retina scans."[41] However, that bill creates an exception for personally identifiable information collected from a publicly-available forum where the "individual voluntarily shared the information or authorized the

---

nationwide. 18 U.S.C. § 1801 (2006). More than a dozen states restrict secret photographing of an individual without consent, but typically only in a private place where one may reasonably expect to be safe from unauthorized surveillance. *See, e.g.,* Del. Code Ann. tit. 11, §§ 1335-1337; *see also* Reporters Committee for Freedom of the Press, *Chapter 3: Surreptitious Recording*, The First Amendment Handbook (7th ed. 2011), *available at* http://www.rcfp.org/handbook/index.php?pg=3-1.

[36] 740 Ill. Comp. Stat. § 14/10 (2010).

[37] *Id.* § 14/15(b).

[38] *Id.* § 14/15(a).

[39] *Id.* § 14/15(c), (d).

[40] *See* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011) (Sen. Patrick J. Leahy); see also Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Cong. (2011) (Sen. Richard Blumenthal). Sen. Blumenthal's bill would also require data brokers maintaining biometric information to provide consumers with notice of adverse actions taken against consumers based on the information the data broker holds about them, and to provide a means for consumers to view and correct that information.

[41] Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 3(5)(A)(viii) (2011).

information to be shared."[42] Because an unmasked individual is, arguably, always voluntarily sharing her facial features, the Act may exempt most scenarios in which one individual takes another's photo and shares the photo with an app or online service that uses facial recognition, such as a social networking site.[43]

V. Voluntary Codes of Conduct and Privacy by Design

The gap in legal privacy protection makes it all the more important for companies and innovators to develop industry-wide codes of conduct and to design facial recognition products with consumer privacy and choice in mind. Several trade associations and institutions have adopted privacy standards for facial recognition, and several major companies have integrated key privacy features into their facial recognition products. Unfortunately, however, there is no overarching set of privacy standards covering all or even most commercial uses of facial recognition, and the overall compliance rate with existing privacy standards related to facial recognition is unknown.

Within the past year and a half, the Digital Signage Federation (DSF) and Point of Purchase Advertising International (POPAI) adopted privacy standards for their member companies that address facial recognition, as well as other information-gathering technologies.[44] Both sets of voluntary standards are detailed and quite strong from a consumer privacy perspective. The DSF Digital Signage Privacy Standards incorporate the full set of Fair Information Practice Principles (FIPPs).[45] Under the privacy standards of both POPAI and DSF, companies are supposed to obtain consumers' opt-in consent before collecting directly identifiable information through digital signage.[46] Companies are prohibited from collecting facial recognition information on minors under 13 (or as

---

[42] *Id.* § 3(3)(B).

[43] "No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world." United States v. Dionisio, 410 U.S. 1 (1973). "[F]ace recognition technology only captures what a person knowingly exposes to the public." David McCormack, Note*, Can Corporate America Secure Our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Recognition Technology*, 8 B.U. J. Sci. & Tech. L. 128, 139 (Winter 2003).

[44] Digital Signage Federation, Digital Signage Privacy Standards (Feb. 2011), *available at* http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf; POPAI Digital Signage Group, Best Practices: Recommended Code of Conduct for Consumer Tracking Research (Feb. 8, 2010), *available at* http://www.popai.com/docs/DS/2010dscc.pdf.

[45] DSF based its Digital Signage Privacy Standards on a report written by the Center for Democracy & Technology (CDT) and worked closely with CDT to develop the standards for its members. Center for Democracy & Technology, Building the Digital Out-Of-Home Privacy Infrastructure (Mar. 1, 2010), *available at* http://www.cdt.org/report/building-digital-out-home-privacy-infrastructure.

[46] *See* POPAI Digital Signage Group, Best Practices: Recommended Code of Conduct for Consumer Tracking Research 6, 9 (Feb. 8, 2010), *available at* http://www.popai.com/docs/DS/2010dscc.pdf.

defined by state law) through digital signage.[47] Companies must also provide notice of any ongoing data collection in the physical location in which digital signage units operate – such as a sign at the entrance of a supermarket – even if the system collects only "anonymous" data, such as through facial detection.[48]

The decision for many digital signage companies to use the less privacy-intrusive facial detection, rather than facial recognition, is itself a choice in favor of consumer privacy. For example, Intel's Anonymous Video Analytics (AVA) uses facial detection software to record the age and gender of passersby and contextualize advertising in real time based on those factors.[49] Intel's AVA is reportedly designed to be incapable of identifying individuals, tracking individuals across systems, linking content associated with individuals' identities, or retaining unique data (including photographs) about individuals.[50] In combination with the Digital Signage Privacy Standards, products built with "Privacy by Design" – like Intel's AVA – offer good privacy protections and choices for consumers.[51]

Likewise, some online services that use facial recognition and detection also tailor their practices to protect privacy. For example, Google+ and Google's Picasa Web Albums, described above, do not automatically suggest friends' names to photos; rather, the services detect clusters of faces, let users add the tags, and then apply the tags to matching faces throughout the user's photos. Google+ takes the extra step of notifying Google+ users whose faces have been tagged in photos and seeking those users' approval for the tag before linking the tag to the Google+ profile.[52] In contrast, Facebook does not require user approval for friends' tags based on facial recognition unless the user specifically requests it.[53] It is a positive feature, though, that Facebook will not

---

[47] *See* POPAI Digital Signage Group, Best Practices: Recommended Code of Conduct for Consumer Tracking Research 6 (2010), *available at* http://www.popai.com/docs/DS/2010dscc.pdf.

[48] *See* POPAI Digital Signage Group, Best Practices: Recommended Code of Conduct for Consumer Tracking Research 7-8 (2010), *available at* http://www.popai.com/docs/DS/2010dscc.pdf.

[49] Intel, Digital Signage: Overview, http://www.intel.com/p/en_US/embedded/applications/digital-signage (last visited Nov. 28, 2011).

[50] Information & Privacy Commissioner of Ontario, Anonymous Video Analytics (AVA) Technology and Privacy 4 (Apr. 2011), *available at* http://edc.intel.com/Link.aspx?id=5043.

[51] For more detailed discussion of the "Privacy By Design" concept, *see* Comments of the Center for Democracy & Technology, FTC Consumer Roundtable (Dec. 21, 2009), *available at* http://www.cdt.org/content/role-privacy-design-protecting-consumer-privacy.

[52] Nathan Davis, *Announcing: Easier Face Tagging in Albums!*, Google+ (Nov. 22, 2011), https://plus.google.com/u/0/115329226963212625435/posts/atRLstuNRLf.

[53] In the Matter of Facebook, Inc., Complaint, Request for Investigation, Injunction, and Other Relief, Before the Federal Trade Commission 8-17 (June 10, 2011), *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

automatically suggest friends' names to photos unless the user has manually tagged the friend at least once.

The FTC has endorsed "Privacy by Design" – incorporating privacy into the fabric of business models and data management practices – as the best way for companies to reduce privacy risks before problems arise.[54] Privacy by Design is clearly needed with respect to facial recognition, and there is some cause for optimism insofar as prominent trade associations and companies proactively adopted privacy standards and features for facial recognition, doing so in the absence of serious public scandal or government pressure. In contrast, the major online behavioral advertising trade associations only issued self-regulatory guidelines under pressure from government regulators and after widespread public controversy over their business practices. However, the digital signage privacy standards cover only a niche in the broad commercial applications for facial recognition; the existing privacy standards are voluntary and – as demonstrated by the online behavioral advertising industry – self-regulation does not have a strong track record without broad adoption and an effective enforcement mechanism.

The lack of adequate protection in current law and the limitations of self-regulation when not backed up by an enforcement mechanism highlights again the point that CDT has been making consistently about consumer privacy: The only effective way to address privacy is with a nuanced mix of baseline consumer privacy legislation, industry self-regulation, and privacy by design.

VI. Policy Approaches to Facial Recognition

Congress, federal agencies, and companies each have a role in promoting the responsible use of facial recognition while protecting free speech.

Congress should avoid seeking legislative solutions for facial recognition alone. Rather, Congress should pass a strong baseline consumer privacy law.[55] U.S. privacy law is currently fragmented, targeting discrete economic sectors with different rules, resulting in a complex patchwork that is a poor fit for businesses and consumers alike.[56] Establishing privacy laws for facial recognition in isolation will perpetuate this fragmentation and will likely be ineffective protection for consumers – if consumer profiling and tracking via facial recognition or other biometrics were curtailed, consumers would still be profiled and tracked through innumerable alternative methods. Instead, as CDT has long advocated, the most sensible solution is setting a floor of privacy

---

[54] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 9 (Dec. 2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[55] Letter from Sen. John D. Rockefeller to the Fed. Trade Comm'n (Oct. 19, 2011), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=f15e7111-f9fb-4eee-b4e7-7cc48c6f003b.

[56] Center for Democracy & Technology, Consumer Privacy: Baseline Privacy Law, http://www.cdt.org/issue/baseline-privacy-legislation (last visited Nov. 28, 2011).

protections with one comprehensive framework based on the FIPPs.[57] This baseline law should cover biometrics (in addition to other categories of personal information), providing consumers with a measure of control over whether they participate in commercial facial recognition systems and requiring companies to be transparent about their use of facial recognition. Baseline consumer privacy legislation should also establish a safe harbor program in which companies that adhere to enforceable industry self-regulatory privacy codes enjoy specified incentives, such as exemption from some forms of liability.[58]

One of the hardest issues to be addressed both in baseline privacy legislation and in industry guides is how to deal with publicly available information or information a consumer willingly divulges, which may includes an unmasked individual's facial features in public areas. The fact that information is publicly available is not the end of the data protection inquiry, of course. Important information covered, for example, by the Fair Credit Reporting Act is public or publicly available, yet the law establishes requirements for its fair use.[59] Regulating facial capture or recognition may also have First Amendment implications. Policymakers will have to determine whether businesses and individuals have a right to take photographs of people in public places, turn the facial features of the people in the photos into a unique mathematical expression, and then search electronic resources for similar mathematical expressions. Likewise, the regulation of individual use of this technology poses special challenges. It would be impractical to require every individual seeking to use a facial recognition camera in public to obtain to obtain prior permission from any other person who may be identified.

Federal agencies can play a crucial part in developing and enforcing voluntary self-regulatory privacy codes that cover facial recognition. In its privacy "Green Paper," the U.S. Dept. of Commerce Internet Policy Task Force proposed convening coalitions of businesses and consumer groups to devise industry-specific privacy codes.[60] CDT supports the Task Force's proposed "multi-stakeholder process," but we caution that any self-regulatory program will not be effective without tangible incentives for business

---

[57] Center for Democracy & Technology, Recommendations for a Comprehensive Privacy Policy Framework § 1, CDT Policy Posts (Feb. 4, 2011), http://www.cdt.org/policy/recommendations-comprehensive-privacy-protection-framework#1.

[58] *Id.* § 2.

[59] Various "privacy" laws regulate publicly available data. See, for example, the Drivers Privacy Protection Act, 18 U.S.C. §§ 2721-2725. In 1989, the Supreme Court rejected "the cramped notion of personal privacy" that "because events summarized in a rap sheet have been previously disclosed to the public, [one's] privacy interest in avoiding disclosure of a federal compilation of these events approaches zero." U.S. Dept. of Justice v. Reporters Committee, 489 U.S. 749, 762-63 (1989).

[60] Dept. of Commerce Internet Policy Task Force, Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 16, 2010), *available at* http://www.commerce.gov/node/12471.

participation and consistent enforcement of the privacy codes.[61] The FTC and state Attorneys General should therefore retain the authority to bring actions against companies falsely claiming compliance with approved privacy standards.

In terms of specific policy stipulations, CDT believes facial recognition should be subject to the full set of privacy protections outlined in the FIPPs, recognizing that not all the FIPPs would be fully applicable in all situations.[62] Companies should generally obtain informed, affirmative consent prior to identifying individuals via facial characteristics in public places or in places open to the public, such as stores (Level III above), and companies should provide consumers with clear, prominent notice of their use of facial detection in such public places (Levels I and II above).[63]

In many ways, businesses have the most important role of all because it is up to individual companies to actually integrate privacy protections into their business practices. As discussed above, some companies and trade groups have already taken steps to protect consumers by adopting strong privacy standards and privacy-enhancing features in their facial recognition products and services. The Digital Signage Privacy Standards, Intel's AVA, and Google's decision to require user approval for photo tags of the user are all good examples. CDT urges companies to use face detection rather than facial recognition to the extent that their business goals can be achieved through this less intrusive method. Likewise, when seeking to identify individual customers, CDT urges stores and other establishments to consider using other techniques based on informed opt in consent. In developing voluntary codes of conduct, companies should base their practices on the FIPPs and agree to a robust accountability mechanism. CDT strongly encourages companies to remain proactive on privacy, transparency, and consumer choice.

Finally, CDT calls on innovators to develop tools and products for consumers that can enhance consumers' privacy in situations where facial recognition is not adequately checked by regulation or company policy. As common mobile devices continue to evolve, millions of individual consumers will come to casually wield facial recognition cameras connected to the Internet. Ensuring transparency and consumer privacy for this application of facial recognition is very challenging without stifling innovation and individual free expression. We should remain open to innovative solutions. Some companies may want to offer a "Do Not Identify" opt out program, in which app developers configure their facial recognition algorithms to ignore registered faces, but

---

[61] Comments of the Center for Democracy & Technology, In the Matter of Information Privacy and Innovation in the Internet Economy 4 (Jan. 28, 2011), *available at* http://www.cdt.org/files/pdfs/CDT-Privacy-Comments.pdf.

[62] Center for Democracy &Technology, Building the Digital-Out-Of-Home Privacy Infrastructure 7-16 (Mar. 1, 2010), *available at* http://www.cdt.org/files/pdfs/Building%20the%20Digital%20Out-Of-Home%20Privacy%20Infrastructure_0.pdf.

[63] *Id.*, 13-14. Studies indicate a strong majority of consumers object to "anonymous" tracking for marketing purposes. Turow et al., supra note 27. Clear notice of facial detection provides consumers with an opportunity to "opt out" of facial detection-based marketing by avoiding the area or service covered by the notice.

that may create more privacy problems than the program is worth if individuals must register their facial characteristics to participate. Perhaps instead companies could voluntarily offer consumers something like as a wearable, physical button bearing a standard machine-readable “Do Not Identify” code to implement consumers’ privacy choices in public places. Publicly available facial recognition is a transformative technology that demands outside-the-box thinking to preserve consumer privacy, choice, and free expression.

We thank the FTC for the opportunity to participate in the facial recognition workshop. Please do not hesitate to contact us if we can be of any assistance.

For further information contact Harley Geiger, CDT Policy Counsel, harley@cdt.org.