KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

FACIAL RECOGNITION & PRIVACY: AN EU-US PERSPECTIVE

October 8, 2012

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. Facial recognition and other automated systems collecting 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. With such a broad user base and wide variety of applications, facial recognition technology will be abused.

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. 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. Moreover, given the numerous other ways to identify and track consumers using biometric information, it is doubtful that any solution addressing facial recognition alone is even appropriate. Instead, a mix of policy and technical approaches can give consumers a greater measure of control over how facial recognition and detection is used without unduly limiting the benefits of the technology.

I. Background

Facial recognition is increasingly used in a variety of contexts – from photo tagging to targeting advertisements to security and authentication – but it poses complex privacy issues that do not fit squarely with present laws, both in the EU and in the US.

Facial recognition and other systems that collect sensitive information about individuals in public places can significantly alter the ways in which individuals are identified, tracked and marketed to. Privacy issues with facial recognition are compounded by its wide availability. Facial recognition is no longer used only by entities with substantial technical and financial resources; the capability to detect unique facial characteristics is making its way into handheld consumer devices and free software packages.[1] With such a broad user base and wide variety of applications, facial recognition technology will be abused.

[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, (last visited Sep. 11, 2012).

A mix of legislation, industry self-regulation, and privacy enhancing technologies can give consumers a greater measure of control without unduly limiting the benefits of the technology or burdening free expression. The nature of the technology and the variety of contexts in which it can be used precludes any simple solution to privacy concerns. Moreover, given numerous other ways to identify and track consumers using biometric information, a solution addressing facial recognition alone is likely inappropriate.

This paper briefly describes facial recognition technology, some of its commercial applications, and its impact on privacy.[2] This paper explains the inapplicability of current laws in the EU and the US to facial recognition and details important industry self-regulatory efforts. Finally, this paper proposes policy approaches for addressing facial recognition.

II. 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. There are several methods of "facial recognition" – geometric approaches calculate the spatial relationships between certain facial features, photometric approaches interpret a face as a weighted combination of standardized faces, and skin texture analyses map the unique features on an individual's skin.[3] "Face detection" is where the program recognizes a human face but does not retain identifiable information, such as unique geometric data points.

Facial recognition systems have become quite accurate and fast. In 2010, the US 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] 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.[5]

Because so many online images are freely available, a facial recognition program need not purchase access to a 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 has seen explosive growth in recent years. Facebook reportedly possessed an estimated 60 billion photos by late 2010 (up

[2] Although there are clearly critical privacy issues related to the use of facial recognition for law enforcement and security, we largely focus on commercial uses.

[3] 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 te.

[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 (last visited Sep. 11, 2012).

[5] 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), *available at* http://dx.doi.org/10.1109/BTAS.2010.5634523 (last visited Sep. 11, 2012).

from 15 billion as of April 2009), with tens of thousands of photos in an average individual Facebook user's social network – and Facebook now has more than 800 million active users.[6]

III. Facial Recognition Has Broad Commercial Applications

A. Online context

As the above figures suggest, hundreds of millions of individuals – whether they know it or not – are currently participating in commercial facial recognition systems. Facial recognition has business potential in a wide variety of contexts, and the number of participating individuals will increase 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.

Their approaches to obtaining consent however differ. 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 loaded into Picasa,[7] although users may opt out of sharing tags when they upload photos from Picasa to Picasa Web Albums.[8] Google+ tags will not link to a user's Google+ profile without that user's permission.

Facebook takes a slightly different approach, although facial recognition is still on by default. Tags are linked to friends' Facebook profiles and all the other pictures in which the friend is tagged, and other Facebook users can see those pictures if the tagged user's privacy settings permit it. The tagged user receives a notice and can remove the tags after the fact, though they can also approve tags before the photos are linked their profiles.

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. Apple and Google purchased polar Rose and Riya, respectively, in 2010; Facebook purchased face.com in June 2012.[9]

B. Offline Context

A growing number of commercial facial recognition and detection applications are directed at recording faces in public places and business establishments, rather than online.[10] 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 characterized by a dynamic display

---

[6] Natalie Marsan, *Facebook Photo Trends*, Pixable Blog (Feb. 14, 2011), http://blog.pixable.com//2011/02/14/facebook-photo-trends-infographic (last visited Sep. 11, 2012).

[7] Google, Picasa Support: Add Name Tags in Picasa, http://support.google.com/picasa/bin/answer.py?hl=en&answer=156272 (last visited Sep. 11, 2012).

[8] Google, Picasa Support: Uploading Name Tags from Picasa, http://support.google.com/picasa/bin/answer.py?hl=en&answer=161870 (last visited Sep. 11, 2012).

[9] *See* Awesome News – Facebook Acquires Face.com (June 18, 2012) *available at* http://face.com/blog/facebook-acquires-face-com/ (last visited Sep. 11, 2012).

[10] *See, e.g.,* SceneTap, SceneTap: A New Look into Nightlife, http://www.scenetap.com (last visited Sep. 11, 2012).

presenting messages in a public environment.[11] There were an estimated 2 million displays in the United States in 2010, though there are many more screens worldwide – particularly in China.

Most digital signage systems are not yet configured to identify individuals, but instead calculate a passerby's age and gender, how long an individual watches the display and they can react to consumers' emotional states.[12] 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.[13] By using identification and interactivity technologies to deliver advertising targeted to individual interests, the digital signage industry is building an offline version of the behavioral advertising that currently occurs online.

C. Mobile Context

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.[14] This will ultimately enable developers to incorporate facial recognition into a broad range of apps and provide developers with data gathered through facial recognition.

IV. Impact levels of facial recognition on privacy

CDT conceptualizes facial recognition's impact on privacy on three general levels[15]:

- 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.

---

[11] 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 Sep. 11, 2012).

[12] *See, e.g.*, Affective Interfaces, What This Does / How We Do It, http://www.affectiveinterfaces.com/2009/09/what-this-does/ (last visited Sep. 11, 2012). *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 (last visited Sep. 11, 2012).

[13] 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 (last visited Sep. 11, 2012).

[14] Tom, *Face Detection in iOS 5*, b2cloud Blog (Oct. 26, 2011), http://b2cloud.com.au/how-to-guides/face-detection-in-ios-5 (last visited Sep. 11, 2012); *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 (last visited Sep. 11, 2012); *see also* Ryan Paul, *First look: Android 4.0 SDK Opens Up Face Recognition APIs*, Ars Technica (Oct. 21, 2011), http://arstechnica.com/gadgets/2011/10/first-look-android-40-sdk-opens-up-face-recognition-apis/ (last visited Sep. 11, 2012).

[15] The Art 29 WP in its Opinion 02/2012 (*see infra*, note 21) on facial recognition in online and mobile services (adopted on 22 March 2012) considers facial recognition from the perspective of 'identification, authentication/verification or categorization', hence splitting the 'identification' level in two sub-layers (identification and authentication) and not looking at the counting layer.

- 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 affix a name to the face, and fewer still would be able to associate the face with internet behavior, travel patterns, or other profiles.[16] 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.[17] Deployed widely enough, a network of facial recognition cameras can track individuals as they move from place to place.[18] 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.

V. How facial recognition is addressed under EU law

A. Under the Data Protection Directive from 1995 and its interpretation by the Article 29 Working Party

Under the current EU Data Protection Directive[19], it is generally understood that facial recognition falls under the general definition of personal data[20] (and even, in some cases,

[16] *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 Sep. 11, 2012).

[17] *See* Aliya Sternstein, *FBI to Launch Nationwide Facial Recognition Service*, Nextgov (Oct. 7, 2011), http://www.nextgov.com/technology-news/2011/10/fbi-to-launch-nationwide-facial-recognition-service/49908/ (last visited Sep. 11, 2012).

[18] *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 (last visited Sep. 11, 2012).

[19] Directive No. 95/46/EC of the European Parliament and the Council of Oct. 24, 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281/31) [hereinafter *Directive 95/46*], *available* at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (last visited Sep. 11, 2012).

sensitive data). This interpretation has been confirmed in the Article 29 Working Party's recent Opinion 02/2012 on facial recognition in online and mobile services (adopted on 22 March 2012)[21].

The Art 29 WP Opinion focuses on facial technology being used in three main contexts: (1) identifying people in social networks; (2) authenticating and verifying users to control access to services; and (3) categorizing individuals, e.g. to enhance user experience, allow/deny access to age-related content, or to display targeted advertising.[22]

Moreover, the Art 29 WP Opinion considers facial recognition from the perspective of 'identification, authentication/verification or categorization', hence splitting the 'identification' level in two sub-layers (identification and authentication) and not considering our Level I, the counting layer.

The Art 29 WP Opinion also clarifies that both a digital image of an individual and a reference template based on an image of an individual are biometric data and hence personal data, falling under the 'sensitive data' category where the images are used to obtain ethnic origin, religion or health information. It stresses the need to obtain informed consent and specifies that such consent cannot be derived from the user's acceptance of the overall terms and conditions of the service unless the latter's primary aim involves facial recognition. It also recommends that in the case of an authentication system using facial recognition to access an online or mobile service, 'an alternative, and equally secure, access control system must be in place' and that this 'alternative privacy-friendly option should be the default'.

However, as Directive 95/46 merely sets high-level principles for Members States to implement,[23] its codification into national law in practice has led to a patchwork of regulations for image-data processing,[24] as well as an uncertain regulatory environment for facial recognition.[25]

---

[20] Yue Liu, *Identifying Legal Concerns in the Biometric Context*, 3 J. INT'L COM. L. & TECH. 45 (2008) *available at* http://www.jiclt.com/index.php/jiclt/article/viewArticle/41 (last visited Sep. 11, 2012) ("[T]here is no denying that raw biometric data is personal data in the sense of the EU directive."); National Biometric Security Project, *International Data Privacy Laws and Application to the Use of Biometrics in the United States*, NBSP Publication 0205, 26 (March 2006), *available* at http://www.nationalbiometric.org/publications/InternatlonalPrivacyReport0306pdf.pdf ("[A] database of biometric information from which an individual cannot be identified, would not be subject to the Directive, but that once linked to an identifiable individual, it would most certainly be considered personal data.").

[21] Article 29 Data Protection Working Party, *Opinion 02/2012 on facial recognition in online and mobile services* (WP192 – 00727/12/EN), 22 March 2012, [hereinafter *the Art 29 WP Opinion*] *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf (last visited Sep. 11, 2012).

[22] These concepts are to be read as defined in Article 29 Data Protection Working Party, *Opinion 03/2012 on developments in biometric technologies* (WP193 – 00720/12/EN), 27 April 2012, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (last visited Sep. 11, 2012) (see notably Section 2 – Definitions).

[23] For a complete discussion of member state provisions, *see generally* LISA J. SOTTO, BRIDGET TREACY, AND JÖRGÖ HLADJK, EUROPEAN UNION DATA PROTECTION, § 11:9 (2011), Westlaw 2 Data Sec. & Privacy Law; ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A GUIDE TO INTERNATIONAL LAW AND COMPLIANCE § 2:2 (2009), *available at* Westlaw Information Security & Privacy.

[24] Douwe Korff, *Comparative Study of Different Approaches to New Privacy Challenges* (2008) DK/100215, 3 (2008), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_comparative_chart_en.pdf (last visited Sep. 11, 2012).

[25] *See, Data Protection Commissioner, infra* note 33, at 103 (noting a lack of guidance).

This results in differing approaches to required consent, as some member states prohibit any publication and storage of images online without prior authorization,[26] whilst others have created special categories for photos to determine whether sensitive data is involved, and hence consent is required.[27] For example, several member states do not require an express consent to upload situational photos of people in normal activities,[28] but do require express consent for portrait photos containing recognizable people.[29] Approaches also vary as regard the qualification of facial recognition or biometric data as 'sensitive' or even 'risky' data[30].

The controversy surrounding the introduction by Facebook in June 2011 of its facial recognition application without requiring express consent[31] illustrated these divergences in approach, as some data protection authorities (DPA) believed Facebook should have acquired express consent retrospectively from users for Facebook's existing biometric database[32], whilst the Irish DPA that was asked to look specifically at the photo tagging issue recommended that Facebook should adopt additional safeguards going forward,[33] but without addressing the retroactive consent aspect.

B. Under the proposed Data Protection Regulation

This situation is likely to change once the proposed Data Protection Regulation, unveiled by the Commission on 25 January 2012, is adopted following the co-decision procedure between the

---

[26] Implementation, supra note 21, at 23, 64 (citing Italy and France).

[27] Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking* 01189/09/EN, 8 (June 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/w1p63_en.pdf (last visited Sep. 11, 2012); *Data Directive, supra* note 19, Art. 8(1) (defining sensitive data as racial or ethnic origin, or data relating to health or sex life).

[28] Implementation, *supra* note 21, at 64.

[29] DATATILSYNET, *When You Disclose Data* (Aug. 25, 2010), http://www.datatilsynet.dk/english/social-networks/when-you-disclose-data/ (last visited Sep. 11, 2012).

[30] See, e.g., Act No. 101/2000 Coll., of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts, [Czech Personal Data Protection Act], art. 4(b). http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en (last visited Sep. 11, 2012) ("[S]ensitive data shall also mean a biometric data permitting direct identification or authentication of the data subject."). Italy requires prior authorization for law enforcement where the data processing has a higher risk of harming the data subject, such as biometric data in banks. Personal Data Collection Code Legislative Decree no. 196 of 30 June 2003 [Italian Personal Data Collection Code], § 55, *available at* http://www.garanteprivacy.it/garante/document?ID=1219452 (last visited Sep. 11, 2012). France has enacted safeguards for biometric data by requiring prior authorization by France's DPA. Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties [French Data Protection Act], as amended March 27, 2007, art. 11, 25.

[31] Posting of Justin Mitchell to The Facebook Blog, (June 30, 2011, 20:16 WST ("We've been rolling Tag Suggestions out over the last several months and this feature is now available in most countries. We'll continue to post updates here as the roll-out progresses."); Ben Rooney, *Facebook Knows What You Like*, The Wall Street Journal Technology Blog, June 8, 2011, http://blogs.wsj.com/tech-europe/2011/06/08/facebook-knows-what-you-look-like/ (last visited Sep. 11, 2012).

[32] See notably the views expressed by the Hamburg DPA, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Facebook's Biometric Database Continues to be Unlawful (Nov. 10, 2011), *available at* http://www.computerworlduk.com/news/public-sector/3317751/facebook-to-be-sued-by-german-data-protection-authority/ (last visited Sep. 11, 2012).

[33] *Data Protection Commissioner*, *Facebook Ireland Ltd Report of Audit* (Dec. 1, 2011), *available at* http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf, at 103 (last visited Sep. 11, 2012).

three EU institutions.[34] Indeed, as the proposal takes the form of a Regulation rather than a Directive, it is directly applicable in all EU Member States and reduces the margin of interpretation by each of them considerably.

Looking at our identified uses of facial recognition, namely individual counting, targeting and identification, the DPR rules as currently set out in the proposal apply to facial recognition in various ways. The DPR specifically refers to facial recognition Art. 4 (11) that defines biometric data as 'any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images'. This clarifies that facial recognition data does indeed constitute personal data when it allows for 'unique identification'.[35] Moreover, three major exemptions set out under Art. 2 still apply to the application of the DPR, namely (1) the fact that the DPR rules do not apply when an activity falls outside the scope of the Union law (which particularly covers national security), (2) the fact that EU institutions, bodies and agencies do not have to comply with the DPR and (3) the famous 'household' exemption, which does still seem to apply to the situation of an individual uploading pictures on a social network.[36] Finally, specific provisions apply to measures based on profiling (Art. 20 and Recitals 58-59) and the principle of privacy by design has been reinforced by an additional requirement to implement 'privacy by default' (Art. 23).

VI. The US State of Play: Current Federal and State Privacy Laws Do Not Adequately Protect Consumers

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.[37] 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.[38] 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

---

[34] European Comission, *Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century,* (January 2012) *available at:* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf (last visited Sep. 11, 2012).

[35] This implies that facial recognition techniques used for counting purposes for example or in a context where the collected data is rendered anonymous do not fall under the definition of personal data, as clarified under Recitals 23 and 24 of the DPR.

[36] Though it must be noted that the DPR also introduces under Art. 24 the concept of 'joint controller', which seems to be interpreted by some as implying that platforms such as social networks could be considered as 'controllers' in this context and would hence not benefit, as their registered user does, of the household exemption.

[37] *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 (last visited Sep. 11, 2012), and Dow Chemical Co. v. United States, 476 U.S. 227 (1986), *available at* http://supreme.justia.com/us/476/227/case.html (last visited Sep. 11, 2012).

[38] 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 (last visited Sep. 11, 2012).

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

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,[39] and both the Privacy Act and Office of Management and Budget memoranda cover biometric information held by government agencies.[40] 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.[41]

State laws have very little to say on commercial use of facial recognition, and nothing on facial detection. One exception is Illinois' Biometric Information Privacy Act of 2008. The Biometric Information Privacy 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.[42] 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 and how it will be used, and the individual must consent through a written release.[43] 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.[44] 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.[45] Similarly, Texas prohibits persons from capturing

---

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

[40] 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 (May 22, 2007).

[41] 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 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/first-amendment-handbook/introduction-recording-state-hidden-camera-statutes (last visited Sep. 11, 2012).

[42] 740 Ill. Comp. Stat. § 14/10 (2010).

[43] *Id.* § 14/15(b).

[44] *Id.* § 14/15(a).

[45] *Id.* § 14/15(c), (d).

biometric identifiers, including “face geometry” for commercial purposes without notifying the individual and obtaining the individual’s consent to capture the biometric identifier.[46]

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.[47] 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."[48] 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 information to be shared."[49] 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.[50]

VII. Key Recommendations for Policy Approaches to Facial Recognition and Detection

Policy-makers, relevant authorities and companies each have a role in promoting the responsible use of facial recognition while protecting free speech.

Regulators should avoid seeking legislative solutions for facial recognition alone. Rather, we have advocated that Congress should pass a strong baseline consumer privacy law.[51] 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.[52] 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 protections with one comprehensive framework

---

[46] Tex. Bus. & Com. Code Ann. § 503.001(a)-(b).

[47] *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.

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

[49] *Id.* § 3(3)(B).

[50] "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).

[51] 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 (last visited Sep. 11, 2012).

[52] Center for Democracy & Technology, Consumer Privacy: Baseline Privacy Law, https://www.cdt.org/issue/baseline-privacy-legislation (last visited Sep. 11, 2012).

based on the FIPPs.[53] 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.[54]

Moreover, any privacy protection framework should encourage the development of industry specific codes of conduct that apply the necessarily high level FIPPs to the practicalities of narrow industry segments that may utilize facial recognition technologies. Within the past two years, 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.[55] 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).[56] 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.[57] Companies are prohibited from collecting facial recognition information on minors under 13 (or as defined by state law) through digital signage.[58] 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.[59]

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 Viewer Analytics (AVA) uses facial detection software to record the age and gender of passersby and contextualize advertising in real time based on those factors.[60] Intel's AVA is reportedly designed to be incapable of identifying individuals, tracking individuals across systems, linking content associated with individuals' identities, or retaining

---

[53] Center for Democracy & Technology, Recommendations for a Comprehensive Privacy Policy Framework § 1, CDT Policy Posts (Feb. 4, 2011), https://www.cdt.org/policy/recommendations-comprehensive-privacy-protection-framework#1 (last visited Sep. 11, 2012).

[54] *Id.* § 2.

[55] 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 (last visited Sep. 11, 2012); 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 (last visited Sep. 11, 2012).

[56] 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* https://www.cdt.org/report/building-digital-out-home-privacy-infrastructure (last visited Sep. 11, 2012).

[57] *See* POPAI, *supra* note 55, at 6, 9.

[58] *Id.*, at 6.

[59] *Id.*, at 7-8.

[60] Intel, Digital Signage: Overview, http://www.intel.com/p/en_US/embedded/applications/digital-signage (last visited Sep. 11, 2012).

unique data (including photographs) about individuals.[61] In combination with the Digital Signage Privacy Standards, products built with privacy measures incorporated into their design – like Intel's AVA – offer good privacy protections and choices for consumers.[62]

Likewise, some online services that use facial recognition and detection also tailor their practices to protect privacy. For example, 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.[63] In contrast, Facebook does not require user approval for friends' tags based on facial recognition unless the user specifically requests it.[64] It is a positive feature, though, that Facebook will not 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 product development, business models and data management practices – as the best way for companies to reduce privacy risks before problems arise.[65] 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 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. 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.

For this reason, CDT believes that industry codes of conduct work best when backed up by strong legislation. The Data Protection Directive has long provided under Article 27 that Codes of Conduct may be established to demonstrate compliance with the Directive, and similar legislation has been introduced in the United States. Unfortunately, to date, this co-regulatory approach to data governance has not been widely realized in practice.

One of the hardest issues to be addressed both in privacy legislation and in industry guides is how to deal with publicly available information or information a consumer willingly divulges, which may include 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. In the US, important information covered, for example, by the Fair Credit Reporting Act is public or

---

[61] Information & Privacy Commissioner of Ontario, Anonymous Viewer Analytics (AVA) Technology and Privacy 4 (Apr. 2011), *available at* http://edc.intel.com/Link.aspx?id=5043 (last visited Sep. 11, 2012).

[62] 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* https://www.cdt.org/content/role-privacy-design-protecting-consumer-privacy (last visited Sep. 11, 2012).

[63] Nathan Davis, *Announcing: Easier Face Tagging in Albums!*, Google+ (Nov. 22, 2011), https://plus.google.com/u/0/115329226963212625435/posts/atRLstuNRLf (last visited Sep. 11, 2012).

[64] 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 (last visited Sep. 11, 2012).

[65] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 9 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (last visited Sep. 11, 2012).

publicly available, yet the law establishes requirements for its fair use.[66] 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 prior permission from any other person who may be identified.

Federal agencies can play a crucial part in developing and enforcing 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.[67] 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 participation and regulator approval and enforcement of the privacy codes.[68]

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.

In terms of specific policy stipulations, notice and choice alone are not adequate privacy protections.[69] Instead, facial recognition and detection 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

---

[66] 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).

[67] 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.

[68] 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.

[69] "Relying exclusively on notice- and-consent compliance regimes places the entire burden for privacy on the consumer to navigate an increasingly complex data environment. In most instances, little practical privacy protection is achieved by reliance on this narrow set of protections… Notice and consent are crucial, but they are simply not enough to adequately protect consumers today." Comments of Center for Democracy & Technology to the FTC Consumer Privacy Roundtable, Refocusing the FTC's Role in Privacy Protection 5, (Nov. 6, 2009), *available at* https://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf (last visited Sep. 11, 2012).

all situations.[70] CDT believes 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).[71] While a symbol may one day alert consumers to the presence of a facial recognition or detection device or program, a symbol will only be an adequate form of notice if it is adopted on an industry-wide basis and consumers are properly educated on the meaning of the symbol.

Companies using facial recognition or detection should give special considerations for vulnerable populations, especially children. Companies should, obviously, comply with federal and state laws, but many offline uses of facial recognition and detection technology do not clearly fall under current child privacy laws.[72] Where unique facial information is collected, used, or retained for targeting purposes (Level III), CDT believes that companies should obtain informed opt in consent from parents, and then authenticate that consent, prior to retaining any face-based identifier (such as unique facial geometry) from children under 13 years of age. As a matter of best practices, CDT also believes that facial detection systems that are capable of determining age should not target ads to children under 13. Instead, companies could display a generic, non-targeted ad or network announcement (such as a privacy notice) when the system detects children looking at the screen.[73] A better business practice would be to extend these procedures to all minors under 18.

The locations in which companies place facial recognition or detection devices also matter. Beyond the discrete locations and situations regulated by current privacy rules, such as federal and state anti-voyeurism laws referenced above,[74] companies should consider whether it is fair to deploy facial detection systems – and the "opt out via notice" method of consumer choice – in

---

[70] For CDT's FIPPs-based recommendations for facial recognition and detection in the context of digital signage, see Center for Democracy &Technology, Building the Digital-Out-Of-Home Privacy Infrastructure 7-16 (Mar. 1, 2010), *available at* https://www.cdt.org/files/pdfs/Building%20the%20Digital%20Out-Of-Home%20Privacy%20Infrastructure_0.pdf (last visited Sep. 11, 2012).

[71] *Id.*, 13-14. Studies indicate a strong majority of consumers object to "anonymous" tracking for marketing purposes; *See* Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising

and Three Activities that Enable It (Sep. 2009), *available at*

http://www.ftc.gov/bcp/workshops/privacyroundtables/Turow.pdf (last visited Sep. 11, 2012). 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.

[72] For example, the Children's Online Privacy Protection Rule does not clearly apply to offline uses of facial recognition and detection, such as some digital signage advertising. The Rule applies to websites and online services, not services that are wholly offline. 16 C.F.R. 312.2. The Rule's current definition of "personal information" includes images and photographs only when they are combined with "other information such that the combination permits physical or online contacting." *Id.* However, the Federal Trade Commission is currently considering revising this definition to include any image or video of a child, in response to concerns about facial recognition technology. COPPA Proposed Rule, Fed. Reg. vol. 76 no. 187, at 59813, available at http://ftc.gov/os/2011/09/110915coppa.pdf (last visited Sep. 11, 2012).

[73] Companies that choose to display a non-targeted advertisement in the presence of children should screen out content that is inappropriate for children, such as ads for tobacco.

[74] *Supra* note 41.

locations that provide essential or unavoidable services, such as some health care facilities.[75] To do otherwise could create a de facto opt in for consumers who must participate in a facial detection system in order to obtain the services they need. As a matter of best practices, companies should avoid placing facial detection systems in locations that consumers have reduced power to choose whether to travel through. Alternatively, for sensitive areas, companies could restrict the depth of field of the camera lens on the facial detection system so that the system only detects faces directly in front of it, and also provide an indicator (in addition to the layered notices described above) of the system's range, such as colored tape on the floor. CDT does not believe these additional considerations are strictly necessary, however, for facial detection systems in venues that provide nonessential services or services for which there is a robust marketplace and consumer choice is supported by a variety of available locations.

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 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 creative thinking to preserve consumer privacy, choice, and free expression.

For more information contact:

Dr. Joseph Lorenzo Hall
Senior Staff Technologist
Phone: 202-407-8825
Email: joe@cdt.org

[75] The Health Insurance Portability and Accountability Act Privacy Rule likely prohibits many health care facilities from using facial recognition systems for purposes unrelated to treatment, payment, and health care operations without patient authorization. 45 C.F.R. 164.502(a)(1), 164.508. However these restrictions likely do not apply to systems that detect only faces and other information that cannot reasonably be linked to an individual's identity. 45 C.F.R. 160.103.