Santa Clara High Technology Law Journal

Volume 30 | Issue 1 Article 4

2-25-2014

Facing Real-Time Identification in Mobile Apps & Wearable Computers

Yana Welinder

FACING REAL-TIME IDENTIFICATION IN MOBILE APPS & WEARABLE COMPUTERS

Yana Welinder†

Abstract

The use of face recognition technology in mobile apps and wearable computers challenges individuals' ability to remain anonymous in public places. These apps can also link individuals' offline activities to their online profiles, generating a digital paper trail of their every move. The ability to go off the radar allows for quiet reflection and daring experimentation—processes that are essential to a productive and democratic society. Given what we stand to lose, we ought to be cautious with groundbreaking technological progress. It does not mean that we have to move any slower, but we should think about potential consequences of the steps that we take.

This article maps out the recently launched face recognition apps and some emerging regulatory responses to offer initial policy considerations. With respect to current apps, app developers should consider how the relevant individuals could be put on notice given that the apps will not only be using information about their users, but also about the persons being identified. They should also consider how the apps could minimize their data collection and retention and keep the data secure. Today's face recognition apps mostly use photos from social networks. They therefore call for regulatory responses that consider the context in which users originally shared the photos. Most importantly, the article highlights that the Federal Trade Commission's first policy response to consumer applications that use face recognition did not follow the well-established principle

---

† Legal Counsel, Wikimedia Foundation; Junior Affiliate Scholar, Center for Internet and Society at Stanford Law School. LL.M., Harvard Law School; J.D., University of Southern California; LL.B., London School of Economics and Political Science. Ms. Welinder is incredibly grateful to Thomas Barton, Ryan Calo, Angelica Eriksson, Eric Goldman, Seny Kamara, Nancy Kim, Joanna Sax, Lee Tien, and Peter Welinder for commenting on this Article. She would also like to thank the participants in the Santa Clara High Technology Law Journal Symposium on "The Mobile Revolution: Legal Ramifications of Spontaneity and Flexibility" and the 2013 Internet Law Work-in-Progress event. The views expressed in this Article do not necessarily reflect the views of her employer or any other organization.

of technology neutrality. The article argues that any regulation with respect to identification in real time should be technology neutral and narrowly address harmful uses of computer vision without hampering the development of useful applications.

TABLE OF CONTENTS

INTRODUCTION

In a thrilling scene in the computer-animated film *The Incredibles*, Mr. Incredible stumbles upon a tablet-like device. The device scans his face with a camera, identifies him as Mr. Incredible, and proceeds with telling him a classified message before it self-destructs. Is this technology something you would only see in a fiction cartoon about superheroes? As it happens, it is neither imaginary nor sci-fi. In fact, a mobile application with similar functionality can today be downloaded instantly to your smartphone for $1.99—save the self-destruction.[1]

But while we may observe some mobile applications of face recognition technology crop up in the iTunes store and elsewhere, this technology is still in its infancy. Computer scientists have been working on face recognition technology for decades, but the technology has only recently been implemented in consumer applications. These applications leverage the vast amount of labeled photos aggregated in social networks and the users' oblivious keenness to teach algorithms how to recognize their friends. The ubiquity of mobile phones with built-in cameras presents a new opportunity for this technology. For now, face recognition with mobile phones requires fast Internet connection to communicate with servers that can store all the data about faces and process the information.[2] But this too is now being enabled through rapid progress in mobile Internet speeds and the deployment of 4G mobile broadband.[3]

The use of face recognition technology in mobile apps challenges individuals' ability to remain anonymous in public places. These apps—in their current iteration—encourage users to upload photos with identified faces to social networks, along with embedded metadata revealing where and when they were captured. Consequently, when uploaded, the labeled images generate a digital

---

1. *See FaceLook Face Recognition Lite*, ITUNES, https://itunes.apple.com/us/app/facelook-face-recognition/id512967999?mt=8 (last visited Dec. 8, 2012).

2. Moore's law predicts that the number of components on integrated circuits will double every two years and so eventually phones may have sufficient memory capacity and processing power to perform face recognition of a large number of individuals locally on the phones. *See Excerpts from A Conversation with Gordon Moore: Moore's Law*, INTEL 1 (2005).

3. FED. COMMC'NS COMM'N, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 22 (2010), *available at* http://www.broadband.gov/plan/ (describing the upgrade to 4G mobile networks).

paper trail of the individuals' location in the photo. The apps have this effect without seeking the consent of the identified individuals, who will not have seen the privacy notice displayed when an app was downloaded, and may not even know that they were photographed or identified. In essence, this practice subjects individuals to a possible surveillance by their peers, employers, and companies that have an interest in their everyday choices, and perhaps even the government. The ability to go off the radar allows for quiet reflection and daring experimentation—processes that are essential to a productive and democratic society.[4] In the words of privacy scholar Julie Cohen, "citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests . . . increasingly will lack the capacity to form and pursue meaningful agendas for human flourishing."[5] Given what we stand to lose, we ought to be cautious with groundbreaking technological progress. It does not mean that we have to move any slower, but we should think about potential consequences of the steps that we take.[6]

This article maps out the recently launched real-time identification applications and some emerging regulatory responses to offer initial considerations for regulating this type of app. With respect to current apps, app developers should consider how the relevant individuals could be put on notice given that the apps will not only be using information about their users, but also about the persons being identified. They should also consider how the apps could minimize their data collection and retention and keep the data secure. Today's real-time identification apps mostly use photos from social networks. They therefore call for regulatory responses that consider the context in which users originally shared the photos. Most importantly, I note that the FTC's first policy response to consumer applications that use face recognition did not follow the well-established principle of technology neutrality. I argue that any regulation with respect to real-time identification should be technology neutral and narrowly address harmful uses of computer vision without hampering the development of useful applications.

As such, Part I of this article broadly outlines how face

---

4. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. (forthcoming 2013) (manuscript at 2), *available at* http://www.harvardlawreview.org/symposium/papers2012/cohen.pdf (last visited Apr. 19, 2013).

5. *Id.* at 7.

6. *See* discussion *infra* Part IV.

recognition technology works and presents a few early examples of how it has been implemented in real-time identification apps. Part II explores the privacy implications of these apps. To provide some policy context, this Part also compares the real-time identification apps to mobile apps that use geolocation data, which has been a recent concern for privacy advocates. Part III reviews two broader regulatory responses to face recognition technology in the United States and Europe to identify some principles that may pertain to real-time identification. Finally, Part IV offers five initial principles to consider when regulating these apps in order to protect both fundamental privacy interests and innovation.

I. REAL-TIME FACE RECOGNITION TECHNOLOGY USING PHONES (AND GLASSES)

A. The Process of Automatic Face Recognition in Real Time

Disruptive and highly visible uses of technology sometimes prompt hurried and overbroad policy responses. The recent implementation of face recognition technology in mobile apps and social networks are but two applications of a field that has been developing for decades but may not yet have realized its full potential. As I discuss in Part IV below, it is therefore important to formulate policy that narrowly targets particular uses of face recognition without impacting the development of the technology. To appreciate the limited role of the recent consumer applications of face recognition technology, it is helpful to briefly review the history of the development and application of face recognition techniques.

Computer scientists have long been captivated by the possibility of getting computers to recognize faces. When recognizing a person's face, you need not solicit interaction by asking for a name or taking a fingerprint.[7] Though perhaps less precise, face recognition technology is certainly more convenient than many other types of biometric recognition that require individuals to consciously submit to the recognition process.[8] But more importantly, face recognition is the main process by which humans recognize each other.[9] And so this research problem presents one piece of the puzzle to get computers to simulate—or even excel at—human vision and, more broadly, the

7. Tanzeem Choudhury, *History of Face Recognition*, MIT MEDIA LAB (Jan. 21, 2000), http://vismod.media.mit.edu/tech-reports/TR-516/node7.html.

8. *Id.*

9. *Id.*

quest for artificial intelligence.

In 1973, Takeo Kanade published his PhD thesis at Kyoto University in Japan, outlining one of the earliest face recognition technologies.[10] While Kanade's work was revolutionary, the technology did not really take off until 1991, when Matthew Turk and Alex Pentland presented a method for distinguishing faces from crowded environments.[11] This was the beginning of real-time identification, but the technology has gone a long way since.[12]

Today's face recognition methods generally begin with an analysis of "training images" of already known individuals to measure their facial features.[13] The measurements, also known as "biometric data," are collected into a biometric database.[14] Once a biometric database is compiled, face recognition technology can use it to recognize the listed individuals in new photos.[15] This, of course, means that the person using the technology and the database does not need to know anything about the listed individuals to be able to recognize them. The user only needs to upload a photo to a computer or web application that uses the technology and has access to the database.[16] The technology then tries to detect a face in the new photo.[17] If it finds a face, the technology transforms its size, position, illumination, and color-scale so that it can be compared to biometric data gathered under other conditions.[18] In other words, it *normalizes* the photo.[19] Finally, it measures the facial features in the normalized photo and compares them against the measurements in the biometric database to determine if the face corresponds to one of the listed

10. HANDBOOK OF FACE RECOGNITION 1 (Stan Z. Li & Anil K. Jain eds., 2d ed. 2011) (citing Takeo Kanade, Picture Processing by Computer Complex and Recognition of Human Faces (1973) (unpublished Ph.D. dissertation, Kyoto University)).

11. Choudhury, *supra* note 7.

12. Choudhury, *supra* note 7.

13. *See* HANDBOOK OF FACE RECOGNITION 2-3 (Stan Z. Li & Anil K. Jain eds., 1st ed. 2005).

14. *Id.*

15. *Id.*

16. Article 29 Data Protection Working Party, *Working Party 29 Opinion on Facial Recognition in Online and Mobile Service*, 2012 00727/12 (WP 192) (EN), 2012 O.J. (L 727) 2 (EN) [hereinafter WP29 Opinion], *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf (last visited Nov. 7, 2013).

17. *See* HANDBOOK OF FACE RECOGNITION, *supra* note 13, at 2-3.

18. *See id.*

19. *See id.*

individuals.[20] As researchers perfected this process, face recognition technology began cropping up in consumer applications such as iPhoto, Picasa, Facebook, Google Plus, and Microsoft's Kinect gaming device.[21]

The availability of ubiquitous camera phones with fast Internet connection means that this process can also be performed directly via a mobile app. This eliminates the delay of having to upload a photo to a computer or web application. A camera phone user can simply snap a picture of an anonymous face and instantly get information about that individual on the phone screen in real-time. The photographed individual would likely not even realize that she was being automatically identified.[22] Today, it has become so common to take photos of food and other mundane things that it is virtually impossible to figure out when a stranger is trying to take a photo of your face.[23] Secret photographing will further be facilitated by wearable computers, which will incorporate the functionalities of smartphones into head mounted displays. [24]

B. Early Applications of Real-Time Identification

In 2011, a research team at Carnegie Mellon University showed that publicly available face recognition technology (which was subsequently acquired by Google) could be applied to Facebook photos to identify college students on a campus with a 31.18 percent success rate in only a few seconds.[25] Various mobile apps have similarly tapped into Facebook's vast photo database to recognize

---

20. *See id.*

21. *See, e.g.*, Alessandro Acquisti et al., *Faces of Facebook: Privacy in the Age of Augmented Reality*, BLACK HAT WEBCAST 1 (Jan. 9, 2012), http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf; Larry Magid, *Google+ Adds Find My Face Feature*, FORBES (Dec. 8, 2011, 1:59 PM), http://www.forbes.com/sites/larrymagid/2011/12/08/google-adds-find-my-face-feature/. *See also* Douglas Gantenbein, *Helping Kinect Recognize Faces*, MICROSOFT RESEARCH (Oct. 31, 2011), http://research.microsoft.com/en-us/news/features/kinectfacereco-103111.aspx.

22. *See* WP29 Opinion, *supra* note 16, at 1 ("images of an individual may be captured (with or without the individual being aware)").

23. College humor has an excellent parody about this new trend to photograph everything. *See Look at this Instagram*, COLLEGE HUMOR (Dec. 3, 2012), http://www.collegehumor.com/video/6853117/look-at-this-instagram-nickelback-parody.

24. *See, e.g.*, Paul Miller, *Project Glass and the Epic History of Wearable Computers*, THE VERGE (June 26, 2012, 2:42 PM), http://www.theverge.com/2012/6/26/2986317/google-project-glass-wearable-computers-disappoint-me. *See also infra* Part I.C.

25. Alessandro Acquisti et al., *Faces of Facebook: Privacy in the Age of Augmented Reality*, BLACK HAT WEBCAST 1 (Jan. 9, 2012), http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf.

individuals in real-time. In 2012, Face.com was offering an iPhone app called KLIK, which identified users' Facebook friends in a photo while it was being taken.[26] KLIK had serious security vulnerabilities and was discontinued as soon as Facebook acquired Face.com that same year.[27] FaceLook is another app that uses Facebook photos to recognize faces with an iPhone in real time.[28] Android users can do the same with Viewdle SocialCamera, which was acquired by Google's Motorola Mobility in late 2012.[29] Given the recent boom in face recognition technology, it should be no surprise that start-ups using the technology are hot acquisition targets for today's tech giants.[30]

Most of these apps allow users to upload photos to social networks after they automatically identify the photographed individuals. Uploaded photos may include metadata about where the photo was taken.[31] And even if the metadata could be scraped before it is shown to other social network users, the location of the photo may still be obvious from landmarks in the background.[32] For

---

26. *See* David Goldman, *Real-time Face Recognition Comes to Your iPhone Camera*, CNN MONEY, Mar. 12, 2012, http://money.cnn.com/2012/03/12/technology/iPhone-face-recognition/index.htm (last visited Mar. 16, 2012).

27. *See* Ashkan Soltani, *Facepalm*, ASHKANSOLTANI (June 18, 2012), http://ashkansoltani.org/2012/06/18/facepalm/ (last visited Jul. 21, 2013) ("Face.com essentially allowed *anyone* to hijack a KLIK user's Facebook and Twitter accounts to get access to photos and social graph (which enables 'face prints'), even if that information isn't public." (emphasis in the original)); Steven Musil, *Facebook Shuts Down Face.com APIs, Klik App*, CNET NEWS (July 8, 2012, 11:00 AM), http://news.cnet.com/8301-1023_3-57468247-93/facebook-shuts-down-face.com-apis-klik-app/.

28. *FaceLook Face Recognition Lite*, ITUNES, https://itunes.apple.com/us/app/facelook-face-recognition/id512967999?mt=8.

29. *See, e.g.*, Emily Steel, *A Face Launches 1,000 Apps*, WALL ST. J. (Aug. 5, 2011), http://online.wsj.com/article/SB10001424053111903885604576488273434534638.html?mod=WSJ_Tech_LEFTTopNews; *Viewdle*, CRUNCHBASE, http://www.crunchbase.com/company/viewdle.

30. In addition to PittPatt and Viewdle, Google has also acquired Neven Vision, Riya, and Picasa. Apple has acquired the Swedish face recognition company, Polar Rose. *See* Alessandro Acquisti et al., *Faces of Facebook: Privacy in the Age of Augmented Reality*, BLACK HAT WEBCAST 1 (Jan. 9, 2012), http://www.blackhat.com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf.

31. *See, e.g.*, *Facebook Data Use Policy: Information We Receive and How It is Used*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#inforeceived (last visited Feb. 8, 2012) (Facebook may get this information as a geotag uploaded with the photo, containing its exact latitude and longitude). *See also* Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES, Aug. 12, 2010, at B6.

32. *See Vice.com Publishes Exclusive with John McAfee Reveals Location in iPhone Metadata (EXIF)*, MOBILE PRIVACY (Dec. 3, 2012), http://www.mobileprivacy.org/2012/12/vice-com-publishes-exclusive-with-john-mcafee-reveals-location-in-iphone-metadata-exif/; *see also* Hanni Fakhoury, *A Picture is Worth a*

example, other users can easily recognize that a person is in San Francisco if the Golden Gate Bridge is visible in the background.[33] Real-time identification apps thus create a record of location data both for the app users, who presumably were there to take the photo, and the photographed individuals.

It should be noted that most of this process could of course be carried out without face recognition technology. Users can manually tag photos and upload them to social networks, and there are apps that provide this very capability.[34] But this would require users to actually know and be able to recognize the individual in question. And users are more likely to exercise good judgment and be restrained by social norms when they upload photos of their friends.[35] They are also more likely to know about their friends' personal circumstances and have a sense for when uploading photos of them may be inappropriate. Finally, they are able to ask their friends for permission to post photos of them and more agreeable if a friend asks them to take down a photo.

C. Cyborgs, Wearable Computers, and Augmented Reality

While real-time identification apps in mobile phones can identify individuals without their knowledge, this concern will be exacerbated with the next wave of smart devices. The development of wearable computers promises to augment human vision to make humans into cyborgs. A *cyborg* or *cybernetic organism*—a concept thought up by Manfred Clynes and Nathan Kline in 1960—refers to a human that

---

Thousand Words, Including Your Location, ELECTRONIC FRONTIER FOUNDATION (Apr. 20, 2012), https://www.eff.org/deeplinks/2012/04/picture-worth-thousand-words-including-your-location.

33. Fakhoury, *supra* note 32.

34. *See, e.g.*, *Facebook Camera*, ITUNES, https://itunes.apple.com/us/app/facebook-camera/id525898024?mt=8; *see also* Ingrid Lunden, *Security Loophole in Facebook's Camera App Allowed Hackers to Hijack Accounts Over WiFi [Confirmed]*, TECHCRUNCH (Dec. 24, 2012), http://techcrunch.com/2012/12/24/security-loophole-in-facebooks-camera-app-allowed-hackers-to-hijack-accounts-over-wifi/#comment-box.

35. *But see* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1008 (2012) (pointedly observing that "'Facebook friends,' are often not friends in the traditional sense. As Danah Boyd explains, '[t]he term "friend" in the context of social network sites is not the same as in everyday vernacular. And people know this . . . The term is terrible but it means something different on these sites; it's not to anyone's advantage to assume that the rules of friendship apply to Friendship.' A tongue-in-cheek illustration of this point is offered by the 'Whopper Sacrifice' campaign that Burger King ran as a Facebook Platform application. The campaign offered Facebook users who purged ten Facebook friends deemed unworthy of their weight in beef a coupon for a free Whopper. Burger King dispersed many coupons.").

has been modified with technology to enhance her capabilities.[36] For example, blind people can wear glasses that record their surrounding and represent it to them as noises through headphones.[37] Another example is EyeTap, computer glasses famously worn by Steven Mann, which could be used to improve his night vision or to remove annoying advertising from his visual spectrum.[38] Similarly, one could imagine glasses with face recognition technology and a connection to a biometric database, which could augment an individual. She could, for example, automatically recall important details upon meeting an acquaintance, such as the name of his spouse or children, where he works, or whether he has some particular sensibilities that she may want to avoid in a conversation. The general perception is that people who naturally possess the skill of paying attention to and remembering these details are generally well-liked and tend to fare better in personal and professional life. It is easy to see how others would like to mimic that skill with technology. Indeed, Steve Mann explained the value of his device as providing "an on-demand photographic memory [that] can help all of us by offloading, to a wearable computer, the task of memorizing now-mundane details that might only later become important."[39] Yet, his motive with wearing his EyeTap and logging his experiences in a video "lifeglog" seemed to be more a political statement in response increased surveillance by government and corporate entities.[40] In his view, a personal "lifeglog" can counteract surveillance from the top with "sousveillance" from the bottom—from the perspective of individuals who are normally under surveillance by various authorities.[41]

In addition to keeping track of acquaintances, a wearable computer with face recognition technology could also allow users to identify people that they do not yet know. The person standing next

---

36. Manfred E. Clynes & Nathan S. Kline, *Cyborgs and space*, ASTRONAUTICS, Sept. 1960 at 26, *available at* http://cyberneticzoo.com/wp-content/uploads/2012/01/cyborgs-Astronautics-sep1960.pdf (last visited Nov. 7, 2013).

37. *See Augmented Reality for the Totally Blind*, SEEING WITH SOUND, http://www.seeingwithsound.com/.

38. Jane Bailey & Ian Kerr, *Seizing Control?: The Experience Capture Experiments of Ringley & Mann*, 9 ETHICS & INFO. TECH., no. 2, 2007 at 129, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1303204 (last visited Feb. 11, 2013); *see also Steve Mann: My "Augmediated" Life*, IEEE SPECTRUM (Mar. 1, 2013, 2:17 PM), http://spectrum.ieee.org/geek-life/profiles/steve-mann-my-augmediated-life.

39. Bailey & Kerr, *supra* note 38, at 129.

40. *Id.*

41. Ian Kerr & Steve Mann, *Exploring Equiveillance*, ON THE IDENTITY TRAIL (Jan. 3, 2006, 11:07 PM), http://www.anonequity.org/weblog/archives/2006/01/exploring_equiv_1.php.

to you in line at the grocery store or a coffee shop may have the exact same interests as you and you may have incredibly compatible personalities. Wouldn't it be great if a pair of computer glasses could tell you this so that you could seize the day and make a new friend? This may now be closer to reality as consumer applications of wearable computing are being developed. The most notable consumer product is Google's Project Glass.[42] The computer display manufacturer Vizux is developing a competitor with its Smart Glasses M100.[43] While Google Glass and M100 have a futuristic design that is bound to attract a lot of attention if worn in public, the British Company TTP is developing a device that looks very much like ordinary black-framed glasses from the front.[44] Less sleek than Google Glass, M100, and the TTP glasses, is the head-borne device HC1, developed by Motorola Solutions.[45] Microsoft has also recently filed a patent application for "a head mounted display with supplemental information when viewing a live event."[46] While these

---

42. *Glass*, GOOGLE, http://www.google.com/glass/start/; *see also Details of Google's Project Glass Revealed in FCC Report*, BBC NEWS (Feb. 1, 2013), http://www.bbc.co.uk/news/technology-21290934.

43. *Intelligent Hands-Free Display for Smartphones*, VUZIX, http://www.vuzix.com/consumer/products_m100.html#overview (last visited Nov. 7, 2013); *see also Best Smart Glasses 2013*, SQUIDOO, http://www.squidoo.com/best-smart-glasses (last visited Nov. 7, 2013).

44. *UK Company's 'Augmented Reality' Glasses Could be Better than Google's*, THE SYDNEY MORNING HERALD (Sept. 11, 2012), http://www.smh.com.au/digital-life/digital-life-news/uk-companys-augmented-reality-glasses-could-be-better-than-googles-20120911-25pdn.html; *see What Happens When You Walk into a Bar Wearing Google Glasses*, ZOWCHOW (Feb. 1, 2013), http://zowchow.com/2013/02/01/what-happens-when-you-walk-into-a-bar-wearing-google-glasses/ (describing how people are reacting to early adopters of Google Glass); *see also Get Ready For Even More Google Glasshole Sightings*, TECHCRUNCH (Jan. 28, 2013), http://techcrunch.com/2013/01/28/glassholes/.

45. Mark Gregory, *Motorola Unveils a Computer That Straps onto Your Head*, BBC NEWS (Nov. 13, 2012, 7:01 PM), http://www.bbc.co.uk/news/technology-20316589 (While this helmet-like device with an external snap-on camera will not easily melt into crowds, it is mainly intended for maintenance and construction work in locations that are difficult to reach with other computer equipment); *see also HC1 Headset Computer*, MOTOROLA SOLUTIONS, http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Mobile+Computers/Wearable+Computers/HC1 (last visited Nov. 7, 2013).

46. U.S. Patent Application No. 13/112,919, Publication No. 20120293548 (filed May 20, 2011), *available at* http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220120293548%22.PGNR.&OS=DN/20120293548&RS=DN/20120293548; *see also* Alex Wilhelm, *Microsoft's Augmented-Reality Patent Could Square it Off Against Google's 'Glass' Project*, THE NEXT WEB (Nov. 24, 2012, 1:06 AM), http://thenextweb.com/insider/2012/11/24/microsofts-agumented-reality-patent-could-square-it-off-against-googles-glass-project/.

products take photos and can connect to the Internet, none of them are known to include face recognition technology at this point.[47] As this article went to press, Google Glass face recognition and face classification applications were already being developed.[48] In response to growing privacy concerns, Google issued a statement that it would not approve face recognition apps for Glass.[49]

While face recognition technology in computer glasses can have many useful applications, it does raise the potential that individuals can be recognized instantly against their will and in situations when they prefer to remain anonymous. In the case of Mann's experiment with EyeTap, which displayed video recordings of people online and did not run face recognition technology on them, he relied on people's ability to object to the recording.[50] Ian Kerr has noted that even if Mann discussed the experiment with his subject before streaming it online, it would be difficult for them to comprehend the consequences of their consent.[51] Moreover, the EyeTap transformed Mann's appearance into a bionic man such that it would be difficult for a subject not to realize that she is being captured by a piece of technology while talking to him.[52] By contrast, some of the technologies being developed today can be far more discrete. If equipped with face recognition technology, these devices could record and automatically recognize individuals in public without as much as a sound or flash.[53] The following discussion regarding real-time identification apps in mobile phones applies equally to the

47. *See, e.g.*, *Intelligent Hands-Free Display for Smartphones*, VUZIX, http://www.vuzix.com/consumer/products_m100.html#specifications (last visited Nov. 7, 2013).

48. David Talbot, *Google Irks Developers with Ruling on Facial-Recognition Apps*, MIT TECHNOLOGY REVIEW, http://www.technologyreview.com/news/515756/google-irks-developers-with-ruling-on-facial-recognition-apps/ (last visited June 16, 2013); *see also ReKognition APIs for Google Glass*, ORBEUS, http://glass.rekognition.com/sdk/index.php (last visited Nov. 7, 2013).

49. Jon Brodkin, *Google Forbids Facial Recognition Apps on Glass in the Name of Privacy*, ARS TECHNICA (June 3, 2013, 7:43 AM), http://arstechnica.com/information-technology/2013/06/google-forbids-facial-recognition-apps-on-glass-in-the-name-of-privacy/ (last visited June 16, 2013); *see also Glass and Facial Recognition*, *Project Glass*, GOOGLE PLUS (May 31, 2013), https://plus.google.com/u/0/+projectglass/posts/fAe5vo4ZEcE.

50. Bailey & Kerr, *supra* note 38, at 129.

51. *Id.*

52. Andy Greenberg, *Cyborg Discrimination? Scientist Says McDonald's Staff Tried To Pull Off His Google-Glass-Like Eyepiece, Then Threw Him Out*, FORBES (July 17, 2012, 8:00 AM), http://www.forbes.com/sites/andygreenberg/2012/07/17/cyborg-discrimination-scientist-says-mcdonalds-staff-tried-to-pull-off-his-google-glass-like-eyepiece-then-threw-him-out/.

53. *See* M. Ryan Calo, *Against Notice Skepticism In Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1037, n.54 (2012) (noting that Congress tried to recreate the shutter sound of analog cameras in camera phones with the Camera Phone Predator Alert Act of 2009).

potential use of computer glasses with face recognition technology.

II. CONCEPTUAL SIMILARITIES (AND DIFFERENCES) BETWEEN REAL-TIME IDENTIFICATION AND GEOLOCATION APPLICATIONS

Real-time identification apps will challenge our fundamental privacy law framework of notice and consent in unprecedented ways. To show some of the issues they will raise, I compare them here to geolocation data in mobile apps. Both are capable of determining a person's location in real time. But geolocation apps are also very different in that the person to whom the location data pertains could potentially have notice of the collection—albeit not a very effective notice—when downloading the app to her phone and later seeing the location symbol on the mobile screen when the app uses location data.[54] By comparison, an individual whose face is recognized at a distance with a real-time identification app on another's phone does not even have that luxury. This makes it very difficult for real-time identification apps to seek meaningful consent of the affected individual. Their data collection and processing is invisible by design. In that sense, face recognition is also different from some other forms of biometric identification where you need to press your fingerprint or palm against a scanner, putting you on notice of the identification process.

A. Location, Location, Location

In 1996, the Federal Communication Commission issued an order requiring mobile service providers to design their services such that 911 emergency responders would be able to establish a caller's location within a 125-meter radius.[55] This was accomplished through determining the caller's proximity to nearby cell towers.[56] Today, the distance to cell towers can reveal a person's location with 100 meters

54. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 17-18 (2013) [hereinafter FTC MOBILE PRIVACY DISCLOSURES], *available at* http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (discussing how "Apple and Google utilize icons to signal to consumers when an app is accessing their geolocation information").

55. FED. COMMC'NS COMM'N, REVISION OF THE COMMISSION'S RULES TO ENSURE COMPATIBILITY WITH ENHANCED 911 EMERGENCY CALLING SYSTEM (1996), *available at* http://transition.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt; *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 24 (2009) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT].

56. *See* Daniel Ionescu, *Geolocation 101: How it Works, the Apps, and Your Privacy*, TECHHIVE (Mar. 29, 2010, 7:45 PM), http://www.techhive.com/article/192803/geolo.html.

accuracy, but the location data is becoming more accurate as providers build new cell towers.[57] Most mobile phones also contain GPS chips that calculate their coordinates based on information obtained from satellites.[58] This method generally provides more accurate location data than the distance to cell towers and can now determine a person's location with ten meters accuracy.[59] Although often less accurate, the proximity to cell towers is still used to determine location when the GPS chip has bad satellite reception, which often is the case indoors.[60]

Mobile apps use location data to, for example, help users navigating to a destination, to recommend nearby services, or to allow users to link up with friends that are nearby.[61] Users often also self-report their location online by manually "checking-in" at restaurants, airports, museums, and other establishments and posting their location to social networks.[62] They do so to tell their friends about what they are up to or to unlock a virtual reward for having frequented a particular location.[63]

While fun and often useful, geolocation data can also be collected and shared in undesirable ways.[64] Unlike a desktop, or even

---

57. Nicole Ozer et al., *Location-Based Services: Time for a Privacy Check-In* 4 (ACLU of N. Cal., 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1732269.

58. Ionescu, *supra* note 56.

59. *See Geolocation Privacy and Surveillance: Hearing on ECPA, Part 2 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 113th Cong. (2012) (testimony of Prof. Matt Blaze, Assoc. Prof. of Computer and Info. Sci., Univ. of Pa.), *available at* http://judiciary.house.gov/hearings/113th/04252013/Blaze%2004252013.pdf (last visited June 22, 2012) (noting that "assumptions that might have been true several years ago, such as that GPS satellites always provide higher precision location information than the cellular network does, are no longer universally true today").

60. Ionescu, *supra* note 56; *The Collection and Use of Location Information for Commercial Purposes: Hearing Before the H. Comm. on Energy and Commerce, the Subcomm. on Communications, Technology and the Internet, and the Subcomm. on Commerce, Trade, and Consumer Protection*, 112th Cong. (2010) (testimony of Lorrie Faith Cranor, Assoc. Prof. of Computer Sci. & Eng'g & Pub. Policy, Carnegie Mellon Univ.), *available at* http://democrats.energycommerce.house.gov/Press_111/20100224/Cranor.Testimony.2010.02.24.pdf.

61. Ionescu, *supra* note 56. *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 33 (2012) [hereinafter FTC CONSUMER PRIVACY REPORT], *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf.

62. Ozer et al., *supra* note 57, at 4; *see also* Janne Lindqvist et al., *I'm the Mayor of My House: Examining Why People Use foursquare - a Social-Driven Location Sharing Application*, 29 ASS'N FOR COMPUTING MACHINERY CONF. ON HUM. FACTORS IN COMPUTING 1 (2011), *available at* http://www.winlab.rutgers.edu/~janne/chi2011web.pdf.

63. Lindqvist et al., *supra* note 62.

64. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 33.

a laptop, a mobile phone follows its user, tucked into a back pocket or a purse.[65] The mobile phone is powered at most times, collecting vast amounts of data about its user everywhere.[66] In 2011, two security researchers reported that iPhones store an unencrypted file of location data history and automatically send it to Apple—though without identifying each particular user.[67] Apple acknowledged that the magnitude of the location history was a bug, but continued to maintain seven days worth of data.[68] Upon closer inspection, it turned out that Android phones similarly collect and store data.[69] Unbeknownst to users, location data can also be collected by the numerous apps that can be downloaded to a smartphone. Certain apps automatically transmit the phone's location data to external sites with regular intervals.[70] Apps can also share the information with advertising networks with data flows so complicated that users would be perplexed even if they were put on notice.[71] And even users who knowingly self-disclose their location online can sometimes unintentionally tip-off a burglar or a stalker.[72] Users may simply not anticipate how pieces of their data can be compiled and analyzed further to provide very detailed predictions of their future locations and actions.[73] This "dataveillance" is merely a side effect of the many

65. *See* FTC MOBILE PRIVACY DISCLOSURES, *supra* note 54, at 2.

66. *See* Parker Higgins, *Mobile User Privacy Bill of Rights*, ELECTRONIC FRONTIER FOUND. (Mar. 2, 2012), https://www.eff.org/deeplinks/2012/03/best-practices-respect-mobile-user-bill-rights.

67. *See* Brian X. Chen, *iPhone Tracks Your Every Move, and There's a Map for That*, WIRED (Apr. 20, 2011, 1:30 PM), http://www.wired.com/gadgetlab/2011/04/iphone-tracks/; Brian X. Chen, *Why and How Apple Is Collecting Your iPhone Location Data*, WIRED (Apr. 21, 2011, 5:44 PM), http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/.

68. *Apple Q&A on Location Data*, APPLE (Apr. 27, 2011), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html.

69. Matthew Panzarino, *It's Not Just the iPhone, Android Stores Your Location Data Too*, THE NEXT WEB (Apr. 21, 2011, 9:31 PM), http://thenextweb.com/google/2011/04/21/its-not-just-the-iphone-android-stores-your-location-data-too/.

70. *See* Blaze, *supra* note 59.

71. FTC MOBILE PRIVACY DISCLOSURES, *supra* note 54, at 8 (discussing a "survey [that] showed that many apps . . . shared information with third parties, including advertising networks, without disclosing this fact").

72. *See, e.g.*, PLEASE ROB ME, http://pleaserobme.com/ (last visited Nov. 7, 2013); *The Location Privacy Protection Act of 2011 (S. 1223)*, AL FRANKEN 1, http://www.franken.senate.gov/files/documents/121011_LocationPrivacyProtection.pdf (last visited Nov. 7, 2013) (reporting that in 2006 "approximately 26,000 persons are victims of GPS stalking").

73. Robert Lee Hotz, *The Real Smart Phone*, WALL. ST. J. (Apr. 22, 2011, 7 :34 PM), http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html; FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 33 (citing Comment of Electronic Frontier Foundation, cmt. #00400, at 3); ANN CAVOUKIAN & JEFF JONAS, PRIVACY BY DESIGN IN THE

useful functions that mobile apps serve.[74] It potentially enables both greater surveillance by the government and monitoring by our peers.[75]

As the various risks posed by geolocation data are being unveiled to smartphone users, they become increasingly worried about services that rely on such data.[76] Empirical studies suggest that the concern for privacy prevents some users from taking advantage of location sharing apps.[77] Those users that do use them, try to avoid disclosing their home and work locations, as well as the locations of their friends' homes.[78] The cautious use of technology observed from studies could be explained by a desire for basic liberties. As Jeffrey Reiman observed almost a decade ago, when technology enables perfect surveillance, individuals stand to lose their freedom, their sense of individuality, and the desire to be different and experimental.[79] They lose their freedom to engage in private activities for fear of embarrassment or potential damage to their careers.[80] And if individuals constantly think about how their actions may be perceived by others, they stop acting spontaneously and restrain themselves to a few well-rehearsed moves.[81] With this, they also lose their symbolic notion of "self-ownership."[82] But most importantly, they lose their "inner personal core that is the source of

---

AGE OF BIG DATA 4 (2012), *available at* http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf.

74. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 55, at 23-24 (citing Roger Clarke).

75. *Id.* at 24.

76. Jennifer Urban et al., *Mobile Phones & Privacy* (UC Berkeley Pub. Law Res., Paper No. 2103405, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405; *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NIELSEN (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/.

77. *See* JAN LAUREN BOYLES ET AL., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf (finding that "57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reasons"); *see also* Lindqvist et al., *supra* note 62 (noting that research "has found that privacy is a barrier to adoption of location sharing services").

78. *See* Lindqvist et al., *supra* note 62.

79. Jeffrey Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future*, 1 SANTA CLARA COMPUTER & HIGH TECH. L.J. 11, 27 (1995).

80. *Id.*

81. *Id.* at 38.

82. *Id.*

criticism of convention, of creativity, rebellion and renewal."[83] This is not only a loss for individuals, but affects innovation and societal progress more generally.[84] Mobile users may not be thinking about the big picture. But the short-term fear of losing freedom to make individual choices may explain why users are anxious that the increased use of location data in mobile apps could lead to greater monitoring of their movements.

Real-time identification apps raise similar concerns. By identifying a face with a mobile phone camera, the app generates a record of that individual's location.[85] The record can be stored in the phone or be uploaded to a social network, where it may be connected to the photographed individual's profile.[86] The uploaded photo can contain embedded metadata such as when and where the photo was taken.[87] This means that real-time identification apps can generate location data for a particular individual, which may be far more precise than the geolocation data based on GPS or distance to cell towers. It may also be more sensitive because the photo shows what the person is doing and whom she is with, while her facial expression may reveal her mood.[88] The decision of how that location data is shared is ultimately with the app user rather than the photographed individual. It could therefore result in unwanted collection and sharing of location data.

Both location data and real-time identification are difficult to protect because they often involve the contradictory notion of "privacy in public."[89] The black and white polarity between private

---

83. *Id.* at 42.

84. PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 213, 225 (1995).

85. *See* Soltani, *supra* note 27; Steven Musil, *Facebook Shuts Down Face.com APIs, Klik App*, CNET NEWS (July 8, 2012, 11:00 AM), http://news.cnet.com/8301-1023_3-57468247-93/facebook-shuts-down-face.com-apis-klik-app/.

86. *See id.*

87. *See e.g.*, Hanni Fakhoury, *A Picture is Worth a Thousand Words, Including Your Location*, ELECTRONIC FRONTIER FOUND. (Apr. 20, 2012), https://www.eff.org/deeplinks/2012/04/picture-worth-thousand-words-including-your-location (location data embedded in photos).

88. Bianca Bosker, *Affectiva's Emotion Recognition Tech: When Machines Know What You're Feeling*, The HUFFINGTON POST (Dec. 24, 2012, 3:22 PM), http://www.huffingtonpost.com/2012/12/24/affectiva-emotion-recognition-technology_n_2360136.html.

89. *See* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998), *available at* http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf (last visited June 23, 2013). Both location data and real-time recognition can of course also be used to track individuals when they

and public spheres has largely been rejected as scholars have developed more elaborate conceptualizations of privacy. Yet current privacy law and theory still recognize that privacy interests are not absolute and must be balanced against competing interests.[90] Asserting a privacy interest in public space is often seen to have implications for other interests—such as a photographer's desire to capture her surroundings or a government's interest in conducting surveillance to ensure public safety.[91] It is easy to dismiss a privacy interest in public with an understanding that a person has voluntarily chosen to give up her privacy by appearing in public.[92] The lack of privacy is seen as the price people pay to avoid a life in isolation. They are rewarded with social interaction, financial opportunities, cultured life, and other benefits. But until now, this transaction has not in practice led to complete loss of privacy. People have been free to move about in public and rely on their anonymity as against strangers. The ability to track their movements with location data and real-time identification changes the terms of the social contract.

B. No Notice or Consent

While real-time identification and geolocation apps are both capable of collecting sensitive location data, they have one stark difference: the real-time identification app can collect, use, and share location data pertaining to a passer-by, who has neither brought the phone to the location in question, nor downloaded the relevant app. And while commentators question the effectiveness of notice in geolocation apps,[93] it is clear that there is no such notice at all in real-time identification apps.

Not all apps that collect or use geolocation data provide a privacy notice to the users.[94] Some of these apps have recently come under scrutiny for failing to provide a notice before collecting private

---

are in private places.

90. *Id.* at 571.

91. *See id.*

92. *Id.*

93. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 70 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

94. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 33. *See also* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY, INFORMATION, & TECHNOLOGY (2012) (noting that in 2011 "22 out of 30 [mobile apps] did not have a privacy policy"); Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, CYLAB USABLE PRIVACY AND SECURITY LAB. 8 (February 2010), http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf (finding that only 66% of location based apps provided a privacy policy).

information about children and Californians—two groups that have been afforded greater legal protection than the average person in the U.S.[95] Pending legislation would further require all companies that collect location data to get users' permission before collecting or sharing it.[96] But even when apps do ask users to agree to privacy notices on a phone, the value of that exercise is questionable. Long privacy policies in small print, split up over multiple pages on a small mobile screen are not likely to put consumers on notice.[97] For that reason, the Federal Trade Commission (FTC) has recommended that app developers work out alternatives to privacy policies, such as data use icons, privacy dashboards, and just-in-time privacy disclosures.[98] These tools are meant to communicate data practices in a streamlined manner that take up less physical space on a mobile screen and provides better overview.[99]

Effective privacy disclosures and meaningful consent primarily protect a notion of privacy known as "control over information."[100] This is the idea that when individuals try to protect the privacy of their information, they are not seeking to prevent everyone from knowing it.[101] Rather they want to control what particular individuals know about them.[102] They disclose more details about their personal lives to their inner circle of friends, family, or others whom they trust.[103] Indeed, limited disclosure of information is considered

95. *See* United States v. W3 Innovations, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) ("First COPPA case against a mobile application developer"); Brandon Bailey, *California Attorney General Sues Delta Air Lines Over Smartphone App Privacy Policy*, MERCURY NEWS (Dec. 7, 2012, 9:25 AM), http://www.mercurynews.com/business/ci_22141459/california-sues-delta-airlines-over-smartphone-app-privacy; *see also* FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

96. *The Location Privacy Protection Act of 2011 (S. 1223)*, AL FRANKEN 1, http://www.franken.senate.gov/files/documents/121011_LocationPrivacyProtection.pdf; Brendan Sasso, *Senate Panel Approves Franken's Location Privacy Bill*, THE HILL (Dec. 13, 2012, 6:29 PM), http://thehill.com/blogs/hillicon-valley/technology/272889-senate-panel-approves-frankens-location-privacy-bill; Devin Henry, *Franken Pushes Last Minute Action On Location Privacy Bill*, MINNPOST (Dec. 12, 2012), http://www.minnpost.com/dc-dispatches/2012/12/franken-pushes-last-minute-action-location-privacy-bill.

97. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 70 (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

98. FTC MOBILE PRIVACY DISCLOSURES, *supra* note 54.

99. *See id. at* 15-18.

100. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968).

101. *Id.*

102. *Id.*

103. *Id.*

necessary to foster those types of relationships.[104] But at the same time, people do not want their personal information to become public or shared with individuals who have no business knowing it.[105] At a more functional level, control over information guards people against prejudice. Unlike computers that make predictable determinations based on specified parameters, humans are prone to making subjective decisions based on gut feeling and without filtering out certain irrelevant factors. It is therefore helpful to be able to shield personal information like political affiliation or sexual orientation from everyday decision makers, such as prospective employers or teachers. In the digital age, privacy notices are meant to help mobile users to manage the flow of their information by specifying what particular information they reveal while using an app and how that information will be used. The users may then select to share their location data with friends over an online social network to provide recommendations, or to meet up with friends that happen to be around, or simply to let their friends know what they are up to. Sometimes, they can control the information flow by restricting their privacy settings such that their information is not publicly available to others.

While notice and consent is currently the cornerstone of American privacy law, it is notably absent from the process of recognizing individuals with real-time identification apps. The person whose face is automatically recognized may never even know that she is being photographed or that the picture is used to identify her in real-time. If the real-time identification app provides a privacy notice upon installation, the notice is shown only to the user and does not reach other people whose data is collected and used. Some apps appear to rely on the notice that Facebook provides to its users when they upload photos to the social network.[106] But that notice cannot reasonably warn a Facebook user that a particular real-time identification app could use the photos years later to automatically recognize the users' face in public. It also cannot effectively inform users that this information can be used to determine their location at any point in time—even if they purposefully do not use geolocation data on their own phones. In short, when a real-time identification

104. *Id.*

105. *Id.*

106. *See FaceLook Face Recognition Lite*, ITUNES, https://itunes.apple.com/us/app/facelook-face-recognition/id512967999?mt=8 ("FaceLook doesn't recognize friends who blocked 3rd party apps from accessing their [Facebook] photo").

app identifies an individual in public, the app fails to provide the person with an opportunity to control her information because the app simply has no interaction with her.

C. The Ability to De-Anonymize a Face

Perhaps the most vocal concern with respect to real-time identification apps is that they could be used to recognize anonymous faces in the street.[107] Face biometrics is particularly sensitive because people expose their faces publicly at most times and the appearance of a face cannot easily be altered.[108] Today, people rely on the fact that there are only a limited number of individuals that can recognize them. They can seek to avoid those people when they do not wish to be noted. As Alan Westin eloquently articulated:

> [One] state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behavior and role that would operate if he were known to those observing him. In this state the individual is able to merge into the "situational landscape." Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men [and women] seek in open spaces and public arenas . . . .[109]

The ability to remain anonymous in public allows individuals to expose their unique faces while doing things they would not want others to know about. This could be a "minor non-compliance" with rules that we do not anticipate will be upheld at all times.[110] As Westin pointed out, society will sometimes let people off the hook for minor traffic violations or for "smoking in the restrooms" to allow them to release some of the pressure that society imposes upon them

---

107. *See* FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES i-ii (2012) [hereinafter FACING FACTS], *available at* http://www.ftc.gov/reports/facialrecognition/p115406commissionfacialrecognitiontechnologiesrpt.pdf.

108. Yana Welinder, *A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165 (2012); *see also* FACING FACTS, *supra* note 107, at 19 (discussing that "[a] consumer's face is a persistent identifier that cannot be changed in the way that a consumer could get a new credit card number or delete a tracking cookie").

109. ALAN WESTIN, PRIVACY AND FREEDOM 31 (1967).

110. *Id.*

at other times.[111] But sometimes the secret act is not going to be a violation at all.[112] Culturally, most people would not want to be seen purchasing contraceptives by their parents, children, or even siblings. They may not want their employer to see them going to a therapist or an AA meeting. They may not want to have all their friends witnessing how they desperately try to charm someone on a first date. Real-time identification apps could be used to recognize individuals in these potentially embarrassing moments. And they can be used to spread information about what they were doing beyond the few strangers that actually witnessed the situation in real-time.

D. Government Access to Data

While the discussion in this article focuses primarily on companies' collection and use of biometric data, it is entirely possible for privately collected data to end up in the hands of government agencies.[113] Currently, an agency only needs a subpoena or a court order issued pursuant to a lower standard than a warrant to obtain biometric data or photos of identified individuals with time and location meta data from a provider that stores the information remotely (as opposed to on the users' home computer).[114] The agency must first notify the user, but can postpone the notice if it believes that the user will delete the information or there is another special reason for not notifying the user in advance.[115] There is now some movement to introduce a warrant requirement when agencies try to obtain location data.[116] A pending bill would likely also apply to

111. *Id.*

112. *Id.*

113. *See, e.g.*, Laura K. Donohue, *NSA Surveillance May Be Legal — But It's Unconstitutional*, WASH. POST (June 21, 2013), http://www.washingtonpost.com/opinions/nsa-surveillance-may-be-legal--but-its-unconstitutional/2013/06/21/b9ddec20-d44d-11e2-a73e-826d299ff459_story.html (last visited June 22, 2013).

114. Stored Communications Act, 18 U.S.C. § 2703(b) (West 2013). Unlike the probable cause showing that is normally required for a search warrant, a court order can be issued under this provision "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). It should be noted that this provision only regulates data held by providers of electronic communication and remote computing services. As such, an agency seeking this type of data from another source, such as a shopping mall security camera, may not even need to satisfy this lower standard.

115. *Id.* § 2705. If there is no special reason for postponing notice and the agency does not wish to provide prior notice, it needs to get a warrant to obtain the information. *Id.* § 2703(a).

116. Geolocational Privacy and Surveillance Act, S. 639, 113th Congress (2013), *available at* http://www.govtrack.us/congress/bills/113/s639.

photo metadata because it is "derived from the operation of [a phone and can] be used to determine or infer information regarding [a person's] location."[117] But the biometric data itself would still be obtainable pursuant to a lower standard court order or a subpoena. Moreover, there is even less data protection when an agency is investigating something related to foreign intelligence.[118] As a result of the USA PATRIOT Act, the foreign intelligence issue does not have to be the primary purpose of an investigation to suspend the ordinary electronic surveillance protections; it need only be a "significant purpose."[119] Privacy issues surrounding privately collected biometric data are inextricable from issues of government surveillance. If companies do not want to become conduits for surveillance of their users,[120] they also need to design their services to avoid collecting or retaining unnecessary data.[121]

While it may be practical for government agencies to tap into readily developed private databases with information, it is not the only way that government agencies can get hold of biometric data. The FBI is developing its own face recognition system, which is to use a mug shot database of 12 million arrested individuals.[122] It has also partnered with state Departments of Motor Vehicles (DMVs) to get access to databases of driver's license photos.[123] Coupled with extensive anti-masking laws, expanding networks of closed-circuit television (CCTV) cameras, and video surveillance by drones, it could put an end to anonymity in public as we know it today.[124] For

---

117. *Id.*

118. *See* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1804(a)(7)(B), 1823 (a)(7)(B), and 1881(a).

119. *Id.*; *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) ("FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is not criminal prosecution.").

120. *See ECPA Reform: Why Now?* DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (last visited Nov. 7, 2013).

121. *See infra* Part IV.D.

122. *Next Generation Identification*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Nov. 7, 2013); *FBI Criminal Justice Information Services Division Staff Paper – Update on Next Generation Identification*, ELECTRONIC FRONTIER FOUND. (June 2012), https://www.eff.org/document/fbi-cjis-staff-paper-next-generation-identification.

123. *FBI Performs Massive Virtual Line-up by Searching DMV Photos*, ELECTRONIC PRIVACY INFO. CENTER (June 17, 2013), http://epic.org/2013/06/fbi-performs-massive-virtual-l.html (last visited June 23, 2013).

124. *See* MINN. STAT. ANN. § 609.735 (West 2012) ("A person whose identity is concealed by the person in a public place by means of a robe, mask, or other disguise, unless

now, this system may not be very effective because photos of criminal suspects, particularly images from security cameras, are not likely to be the high quality frontal images that can easily be matched to mug shots and driver's license photos.[125] This system will further not have the benefit of contextual information that allows consumer apps to make better guesses based on that users are more likely to appear in photos with particular friends. That is unless the program mines social network data, which it possibly does.[126] Consumer apps also rely on their users to confirm or deny automatic identification of their friends, training the identification algorithm every time. Conversely, it would be very difficult to continuously train a government identification system as to all the individuals in its database, which could include everyone with a drivers' license.[127] Given the likely limited effectiveness of a government identification system, there is also a potential for misidentification with severe civil liberties implications for those who are unjustly accused. Although beyond the scope of this article, we also need to think about appropriate accountability for using face recognition in law enforcement.[128] And

---

based on religious beliefs, or incidental to amusement, entertainment, protection from weather, or medical treatment, is guilty of a misdemeanor."); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 277 (2002); Webcast: *Hearing on Oversight of the Federal Bureau of Investigation before the S. Comm. on the Judiciary*, 113th Cong. (2012) (testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=36ffa9c8160f81a25730563dc7e8c551 (last visited June 23, 2013) (responding that the FBI currently uses "drones for surveillance on U.S. soil"); *FAA List of Certificates of Authorizations (COAs)*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/document/faa-list-certificates-authorizations-coas/ (last visited Nov. 7, 2013) (listing FBI as one of the agencies with drones certified by the Federal Aviation Administration); *see also* Tim Maly, *Anti-Drone Camouflage: What to Wear in Total Surveillance*, WIRED (Jan. 17, 2013, 3:14 PM), http://www.wired.com/design/2013/01/anti-drone-camouflage-apparel/.

125. Sara Reardon, *FBI Launches $1 Billion Face Recognition Project*, NEWSCIENTIST (Sept. 7, 2012), http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html; Erika Eichelberger, *Why Facial Recognition Technology Didn't Help ID the Tsarnaevs*, MOTHER JONES (Apr. 23, 2013, 7:01 AM), http://www.motherjones.com/mojo/2013/04/facial-recognition-technology-boston-bombing.

126. *See* Richard Lardner, *Your New Facebook 'Friend' May be the FBI*, MBC NEWS (Mar. 16, 2010, 10:54:25 AM), http://www.nbcnews.com/id/35890739/ns/technology_and_science-security/t/your-new-facebook-friend-may-be-fbi/.

127. *See* Erika Eichelberger, *Why Facial Recognition Technology Didn't Help ID the Tsarnaevs*, MOTHER JONES (Apr. 23, 2013, 7:01 AM), http://www.motherjones.com/mojo/2013/04/facial-recognition-technology-boston-bombing.

128. *See* Christopher Rutledge Jones, *'EyePhones': A Fourth Amendment Inquiry into Mobile Iris Scanning*, 63 S.C. L. REV. 925, 946 (2012); *see also* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, 48

until government agencies develop their own effective identification techniques, there will be a lot of temptation to use private sector databases and identification methods, which are not adequately protected by our outdated electronic surveillance laws.

III. EMERGING REGULATORY RESPONSES TO FACE RECOGNITION TECHNOLOGY

As the discussion above suggests, real-time identification is in its infancy. Even though implementations are relatively few, regulators have yet to catch up to its development. A couple of states have specific statutes regulating the collection and use of biometric data.[129] In the rest of the U.S., the best hope of redress is the tort of intrusion upon seclusion, which is problematic because a person's facial features will mostly not be secluded from the public and courts generally do not consider data collection to be sufficiently offensive for the tort.[130] Over the past couple of years, however, a few general regulatory responses to face recognition technology have provided some initial guidance in this new field.

The debate over the privacy of face recognition technology heated up in 2011 as Facebook introduced the "Photo Tag Suggest" feature in Europe.[131] Its earlier introduction in the U.S. was rather uneventful.[132] But the European launch triggered almost immediate investigation by several European data protection agencies.[133] After

---

B.C. L. REV. 609 (2007) (discussing the various procedural and substantive protections of law enforcement use of data mining that have developed in Europe).

129. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/5 (West 2012); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2012).

130. RESTATEMENT (SECOND) OF TORTS § 652B (1977) (providing that "[o]ne who intentionally intrudes, physically or other-wise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person"); *see* DANIEL J. SOLOVE, THE DIGITAL PERSON 59 (2004) (noting that courts have dismissed "actions based on obtaining a person's unlisted phone number, selling the names of magazine subscribers to direct mail companies, and collecting and disclosing an individual's past insurance history").

131. *See* Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (Dec. 15, 2010), https://www.facebook.com/blog.php?post=467145887130 (last updated June 30, 2011).

132. *See id.*

133. *See Gesichtserkennungsfunktion von Facebook Verstößt Gegen Europäisches und Deutsches Datenschutzrecht [Facebook's facial recognition feature violates European and German data protection law]*, HMBBFDI (Aug. 2, 2011), http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html?tx_ttnews%5BbackPid%5D=170&cHash=b9607e92ef91d779f308acd01b7dd639 (last visited Apr. 27, 2012); *see also* BUNDESDATENSCHUTZGESETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Dec. 20, 1990, BUNDESGESETZBLATT [BGBL. I] at 2954, §§ 38(3)-

the Hamburg Data Protection Agency concluded that the feature violated European law, Facebook voluntarily discontinued its use in Europe, apparently going beyond recommendations of the Irish Data Protection Commissioner.[134] But in the meantime, the European Article 29 Working Party (WP29) issued an advisory opinion about how face recognition technology can be implemented in online and mobile technologies in compliance with European law.[135] In the U.S., the Electronic Privacy Information Center asked the FTC to also investigate Facebook's Photo Tag Suggest, alleging that the feature amounted to an unfair and deceptive trade practice under Section 5 of the FTC Act.[136] The FTC responded with a workshop in December 2011 to solicit comprehensive information about different uses of face recognition technology.[137] Based on that workshop, it recommended best practices for the industry in October 2012. Ironically, in Facebook's spirit of "mov[ing] fast and break[ing] things," Photo Tag Suggest triggered rapid regulatory responses to many different implementations of face recognition technology, which had previously been developing in a near regulatory vacuum since the 1960s.[138] While these responses are not primarily focused on real-time identification, they offer some insight into how the law will address this technology.

A. Federal Trade Commission Guidelines on Face Recognition

38(4), as amended Sept. 14, 1994, *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile.

134. *See PRESS RELEASE: Facebook's Biometric Database Continues to Be Unlawful*, HMBBFDI 1 (Nov. 10, 2011), http://www.datenschutz-hamburg.de/uploads/media/PressRelease-2011-11-10-Facebook_BiometricDatebase.pdf; Somini Sengupta & Kevin J. O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky*, N.Y. TIMES, Sept. 21, 2012, at A1, *available at* http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html; *Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook Turns off Tag Suggest in the EU*, IRELAND OFF. OF THE DATA PROTECTION COMMISSIONER (Sept. 21, 2012), http://www.dataprotection.ie/docs/21-09-12-Press-Release--Facebook-Ireland-Audit-Review-Report/1233.htm.

135. WP29 Opinion, *supra* note 16.

136. *See* Complaint, *In re* Facebook, Inc. and the Facial Identification of Users, No. C-4365 (F.T.C. 2011) [hereinafter Complaint, Facebook], *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf; 15 U.S.C. § 45(a)(1) (2006).

137. FACING FACTS, *supra* note 107, at ii.

138. *See Registration Statement (Form S-1)*, Facebook, 69 (Feb. 1, 2012), http://battellemedia.com/wp-content/uploads/2012/02/Facebook-S-1.pdf. I have previously surveyed different laws that potentially apply to face recognition technology. Welinder, *supra* note 107.

Technology

The FTC's recommended best practices for the use of face recognition technology were based on its revised framework for consumer privacy issued earlier in 2012.[139] The framework would require companies that collect significant amount of data to implement three baseline principles into its use of consumer data: "[1] privacy by design, [2] simplified choice, and [3] greater transparency."[140] The best practices primarily apply these principles to three case studies: the established fields of face detection in photos and classification of faces by demographics in digital signs,[141] and the more groundbreaking use of the technology in social networks.[142] The FTC did not discuss mobile technologies and real-time identification in any greater detail. It mentioned them as "possible future uses of facial recognition technologies."[143] Significantly, the FTC noted that a real-time identification app capable of "identify[ing] anonymous individuals on the street or in a bar could cause serious privacy and physical safety concerns, although such an app might have benefits for some consumers."[144] The FTC therefore suggested that "affirmative express consent" may be necessary before a stranger may recognize a previously unknown individual.[145] "Opt-out consent" would not be sufficient in that situation because there is no going back once a stranger discovers a person's identify.[146] To explain this concept, the FTC provided the following example:

> Consider the example of a mobile app that allows users to identify strangers in public places, such as on the street or in a bar. If such an app were to exist, a stranger could surreptitiously use the camera on his mobile phone to take a photo of an individual who is walking to work or meeting a friend for a drink and learn that individual's identity—and possibly more information, such as her address—without the individual even being aware that her photo

139. FACING FACTS, *supra* note 107, at 1.

140. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at iii.

141. A digital sign is an advertising board with a built-in camera and software that can determine the demographics of individuals that are looking at it. FACING FACTS, *supra* note 107, at i.

142. *Id.* at 2.

143. *Id.*

144. *Id.* at 8.

145. *Id.* at iii.

146. *Id.* at 19; *see also* DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY, TECHNOLOGY, & LAW 433 (2012) (describing "opt-out" consent as providing "a default rule that the company can use or disclose personal information in the ways it desires so long as the consumer does not indicate otherwise").

> was taken. Given the significant privacy and safety risks that such an app would raise, only consumers who have affirmatively chosen to participate in such a system should be identified.[147]

The question remains how an individual can affirmatively submit to such an identification system in practice. Is it sufficient for an individual to provide consent to extraction of biometric data when submitting a photo? Or does the individual need to allow each particular app to use the photo? As this excerpt suggests, the FTC does not believe this scenario to be an issue yet; the commissioners were merely hypothesizing about possible requirements "[i]f such an app were to exist."[148] This explains the lack of specificity in its recommendation with respect to mobile apps. Indeed, the apps that I have described above do not currently appear to be designed to allow identification by strangers because they are limited to recognizing its users' Facebook friends.[149] It is, however, entirely possible that such an app may develop in the near future, leveraging Facebook's vast image database or other online photos that are even more easily available.[150] Therefore, the FTC has recommended that social networks and other similar online services protect their photos against scraping by third parties.[151]

Even when *strangers* do not perform the identification, users may still need to "affirmative[ly and] express[ly] consent" to the use of their biometric data if it "materially differ[s]" from the representations pursuant to which they originally submitted their photos.[152] How would this recommendation apply to apps like KLIK, FaceLook, and SocialCamera that use photos collected by Facebook? It seems that if Facebook's privacy policy does not specify that real-time identification apps can use Facebook photos to identify users offline, the apps need to enter into separate clickwrap agreements with Facebook users.[153] And regardless of what the original privacy

147. *Id.* at iii.

148. FACING FACTS, *supra* note 107, at 6-7.

149. Limiting the identification to a user's social network friends allows the current applications to do more accurate recognition because one person's social circle is less likely to contain look-alikes. Matching faces to databases of several million individuals is still difficult unless you have very high quality data. *See* Erika Eichelberger, *Why Facial Recognition Technology Didn't Help ID the Tsarnaevs*, MOTHER JONES (Apr. 23, 2013, 7:01 AM), http://www.motherjones.com/mojo/2013/04/facial-recognition-technology-boston-bombing.

150. *Id.*

151. FACING FACTS, *supra* note 107, at ii.

152. *Id.* at iii.

153. Clickwraps are terms that are agreed to by clicking "I agree terms and conditions." Nancy Kim, *Clicking and Cringing*, 86 OR. L. REV. 797, 810 (2007).

policy provides, the apps would need to enter into new clickwraps with any other individuals in photos—i.e. those who did not submit the photo to Facebook in the first place. As of December 2012, Facebook's privacy policy does not specifically inform users that their photos can be used by real-time identification apps.[154] It does provide that "[o]nce you share information with your friends and others, they may be able to sync it with or access it via their mobile phones and other devices." It further provides that "[i]f you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications." However, extraction of biometric data and real-time identification are uses that arguably are materially different from Facebook's broad representations that photos will be shared with apps or synced to friends' mobile phones. If so, the real-time identification apps that tap into Facebook's photo album also need to get an "affirmative express consent" from the individuals they identify. This is particularly important because Facebook's privacy policy notifies users that they are able to opt out of Facebook's face recognition feature when uploading photos. Given this more specific provision suggesting control with respect to automatic face recognition, users may reasonably conclude that the broader provision regarding mobile apps does not pertain to face recognition technology:[155]

> We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from the other photos you've been tagged in. This allows us to make these suggestions. You can control whether we suggest that another user tag you in a photo using the "How Tags work" settings.[156]

The broader problem with online consent is that users seldom know what they consent to even if they are prompted to agree to a

---

154. *See Data Use Policy*, FACEBOOK.COM (Dec. 11, 2012), https://www.facebook.com/about/privacy/#infoaboutyou (last visited Nov. 7, 2013).

155. Provided that Facebook's privacy policy is to be interpreted as a contract, a provision that more directly applies to the matter at issue prevails over a more general provision when the two are in conflict. RESTATEMENT (SECOND) OF CONTRACTS § 203(c) (1981) ("specific terms and exact terms are given greater weight than general language"). However, sometimes privacy policies are considered to be "general statements of policy" and not enforceable under contact law. *In re* Northwest Airlines Privacy Litigation, No. Civ. 04-126, 2004 WL 1278459 (D. Minn. June 4, 2004); *see also Dyer v. Northwest Airlines Corp*., 334 F. Supp. 2d 1196 (D.N.D. 2004).

156. *See Data Use Policy*, FACEBOOK.COM (Dec. 11, 2012), https://www.facebook.com/about/privacy/#infoaboutyou (last visited Nov. 7, 2013).

clickwrap.[157]

It also appears that the FTC generally approves of opt-out choice when the face recognition technology is part of the social network, provided it is "easy to find" and "meaningful."[158] In that case, users should get a conspicuous notice (not within the site's privacy policy) describing the new data collection and use.[159] So if Facebook were to reinstate its newly acquired app KLIK, it may not need to obtain users' affirmative consent to use their photos in this manner, provided users get a separate notice on Facebook and are able to easily opt out.

The FTC also noted that particular applications of face recognition technology can provide certain privacy or security functions.[160] This is the case with apps that look for a phone owner's facial features to unlock the phone.[161] While these apps are not intended to share biometric data, they still need to implement some privacy measures, like storing the data securely.[162]

Other apps may not be privacy or security protective and yet may raise less of a privacy concern because they do not "identify" an individual. The FTC indicated that even apps that do not process biometric data to determine the identity of individuals will have to implement privacy protections that are appropriate for that particular situation.[163] It gave the example of SceneTap, which analyzes photos from bars and informs consumers about the resulting demographics to consumers through a mobile app.[164] When an app does not link biometric data to individual, it still needs to protect its photo database from misuse and delete photos after a reasonable time.[165]

The few guiding principles in the FTC's report with respect to real-time identification do not create any hard legal obligations. They are only intended as recommendations and the FTC expressly stated that it will not base its enforcement actions on anything in the report

---

157. *See* Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 466 (2006) (noting that "Clickwraps put some pressure on the classical notion of assent derived from bargained agreements, because they substitute a blanket, take-it-or-leave-it assent for the classical notion that the parties actually thought about and agreed to the terms of the deal.").

158. FACING FACTS, *supra* note 107, at 19.

159. *Id.* at 18-19.

160. *Id.* at 7.

161. *Id.* at 6.

162. *Id.* at 5-6.

163. *Id.* at 11-12.

164. FACING FACTS, *supra* note 107, at 5-6.

165. *Id.*

that exceeds already established legal requirements.[166] The report is nevertheless helpful because it gives companies an initial idea as to how future laws in this field could develop, and allow them to design their services accordingly.

B. European Union Article 29 Working Party Opinion on Facial Recognition in Online and Mobile Services

By the time the FTC issued its recommendations on the use of face recognition technology in late 2012, some of its European counterparts had already opined on the issue. First, the Hamburg data protection agency deemed Facebook's use of the technology to violate European laws.[167] Facebook tacitly agreed by disabling its face recognition feature in Europe.[168] Second, the WP29, charged with providing independent advice on the implementation of national laws adopted pursuant to the European Data Protection Directive,[169] issued an opinion regarding the uses of face recognition technology in online and mobile services.[170] Given that the WP29 opinion specifically focuses on mobile services, unlike the FTC, it provides somewhat more concrete guidance with respect to real-time identification apps.[171] It should be noted that the WP29 opinion is of limited legal authority because WP29 serves only an advisory role with respect to the Directive, whereas the European Court of Justice reserves "a monopoly of final interpretation" of EU law.[172] But the opinion is still a persuasive authority, given that it is the only EU opinion on this specific matter.

---

166. *Id.* at iii.

167. *See Facebook's Biometric Database Continues to Be Unlawful*, *supra* note 134.

168. Loek Essers, *Facebook Deleted All EU Facial Recognition Data, Regulators Confirm*, CFO WORLD (Feb. 07, 2013, 9:50 AM), http://www.cfoworld.com/technology/57103/facebook-deleted-all-eu-facial-recognition-data-regulators-confirm.

169. Council Directive 95/46, arts. 29-30 of the European Parliament and of the Council of 24 October 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 (EC) [hereinafter Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF (last visited Nov. 26, 2012).

170. WP29 Opinion, *supra* note 16.

171. *See id.* at 3 (stating that the photo in its example of uses of face recognition technology "may be captured direct from a smartphone camera.").

172. Nial Fennelly, *Legal Interpretation at the European Court of Justice*, 20 FORDHAM INT'L L.J. 656, 673 (1996), *available at* http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1526&context=ilj (last visited Apr. 19, 2013).

The EU Data Protection Directive—first adopted in 1995 and now in the process of being updated—requires the EU member states to adopt national legislation regulating the automatic processing of personal data.[173] Broadly, those laws are to ensure that a "controller"[174] of data processing protects the data and informs the individuals to whom the data pertains about the controller's data practices.[175] Subject to a few exceptions, personal data may only be processed if the person to whom it pertains has freely consented or when the processing is necessary to carry out a contract with that person or a legal obligation.[176]

The WP29 opined that photos and personally identifiable biometrics are personal data within the scope of the Directive.[177] This means that a real-time identification app that automatically processes photos or personally identifiable biometrics must first get the individuals' informed consent before using their data, unless it has some other legal basis for the processing.[178] The app may not transfer extracted biometrics to other systems.[179] If it uses face recognition technology to provide users with sensitive information about the individual being identified, such as ethnicity, religious beliefs, or health records, the app may further need to obtain special consent that refers to that particular information.[180] In any event, the app developer must try to minimize the amount of data that the app collects to what is absolutely necessary to deliver the service.[181] The data that is collected must also be carefully protected. The app developer must determine whether the data should be stored on the app or in the cloud and encrypted if necessary for its security.[182] At the same time, the individuals in the photos must have some way to access the photos and biometric data.[183] These requirements may not apply to apps that only extract enough information to detect or categorize a face because they are not processing "personal data."[184]

---

173. Directive, *supra* note 169, art. 5.
174. *Id.* art. 2(d).
175. *See id.* arts. 7, 17.
176. *Id.* art. 7.
177. WP29 Opinion, *supra* note 16, at 4.
178. *Id.* at 5; Directive, *supra* note 169, art. 7.
179. WP29 Opinion, *supra* note 16, at 5.
180. *Id.* at 4.
181. *Id.* at 8.
182. *Id.*
183. *Id.* at 9.
184. *Id.* at 4.

If the main purpose of an app is automatic face recognition, it appears that the app developer can provide sufficient notice by describing the face recognition process in its terms of use.[185] The terms would of course need to be read and accepted by the individual being identified and not only by the person using the app.[186] But an app developer cannot rely on provisions about face recognition technology in the general terms of use of a social network from which it takes photos because face recognition is not the main purpose of that network.[187] Opt-out privacy settings in an app or a social network will likewise not suffice as informed consent, though they are important for allowing users to take back their consent if they have second thoughts.[188] Most importantly, the opinion specified that the current practice of opting individuals into a biometric database simply because they upload photos to an online app does not comply with the EU requirements.[189] When sharing photos with friends online, individuals likely do not anticipate that their photos will be used for automatic face recognition and they may not even have the authority to consent if there are other people in those photos.[190]

If an app developer cannot rely on the consent provided by the phone user, how can it set up the service to obtain consent from the person being identified? First, it would need to collect opt-in consent from individuals when it enrolls them in a biometric database, whether it does so through a social network or through the app itself.[191] But the EU requirements seemingly present a Catch-22 for real-time identification apps because the app would need to process a person's biometric data to determine her identity, whereupon it can determine whether she consented to the processing.[192] If it turns out that the individual is not listed in the app's biometric database, the initial processing of her data to determine her identity would be in violation of the EU requirements.[193] The WP29 opinion resolves this issue by stating that apps may process photos or biometric data for the limited purpose of determining whether the person in question

185. *See* WP29 Opinion, *supra* note 16, at 7.
186. *See id.* at 6.
187. *See id.* at 7.
188. *See id.* at 6-7.
189. *See id.* at 6.
190. *See id.* at 6-7.
191. *See* WP29 Opinion, *supra* note 16, at 6.
192. *See id.* at 5.
193. *See id.*

consented to being identified.[194] But if the match against the app's biometric database shows that the individual is either not listed or did not consent, the app would need to delete all data it collected in the process.[195] In a real-time identification app, this would probably mean that the app would not even show the individual's name to the person running the app if it turned out that the individual did not consent to being identified. This limited processing, the WP29 reasoned, is necessary to allow app developers to comply with their legal obligation to determine whether individuals in photos have consented to their services.[196]

Beyond that, the opinion suggests that app developers may want to allow users to blur out the faces of individuals that do not match against their biometric database.[197] That may help users to avoid liability under other European laws that sometimes prohibit photographing of faces in public places without first getting a person's consent.[198]

IV. INITIAL POLICY RECOMMENDATIONS FOR REAL-TIME IDENTIFICATION

If the existing regulatory responses leave something to be desired when it comes to real-time identification, how should this problem be tackled? In a seminal 1890s piece articulating the foundation of our current privacy law, Samuel Warren and Louis Brandeis observed:

> [Back when] the state of the photographic art was such that one's picture could seldom be taken without his consciously "sitting" for the purpose, the law of contract or of trust might afford the prudent man sufficient safeguards against the improper circulation of his portrait; but since the latest advances in photographic art have rendered it possible to take pictures surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection, and the law of tort must be resorted to.[199]

---

194. *Id.* at 5.

195. *Id.*

196. *Id.*

197. WP29 Opinion, *supra* note 16, at 6.

198. *See* Elisabeth Logeais & Jean-Baptiste Schroeder, *The French Right of Image: An Ambiguous Concept Protecting the Human Persona*, 18 LOY. L.A. ENT. L. REV. 511, 526 (1998) (explaining that consent is required unless the photo does not focus on any particular person, and the individuals who happen to be in the photo are performing "public, rather than private, activities").

199. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193,

As this excerpt suggests, instantaneous photography challenged the law some hundred years ago just like instantaneous face recognition poses difficult questions today.[200] In the years that followed, it came upon courts, legislators, and the public at large to determine the laws and norms regulating photography. The result was not a complete prohibition of portable cameras or their use. To the contrary, we have seen continuous innovation in analog and, subsequently, digital cameras. But we have, for example, come to prohibit photographing and videotaping private body parts without a person's consent.[201] Thanks to Warren and Brandeis, we have also developed torts that articulate specific situations when photographing or publishing a photo may invade a person's privacy.[202] Other jurisdictions have struck differently the balance between a person's privacy and the photographer's right to capture images. For example in France, a photo focusing on a particular person requires that person's consent—even if the photo is taken in public.[203] Just like photographs, face recognition will not go away. But it will require us to figure out how and when it can be used.

In a recent article, I analyzed the privacy implications of the use of face recognition technology in social networks.[204] I concluded that the use of photos submitted to an online application for the purpose of socializing cannot be used to automatically identify individuals without violating what Helen Nissenbaum calls "contextual integrity" and I proposed a multifaceted solution to this problem.[205] It is much too early to provide that level of analysis with respect to real-time identification apps. The handful of existing apps do not adequately suggest how different uses of face recognition will develop. They do, however, indicate some of the privacy concerns considered in Part II(A) above. Based on these conceptual observations, and drawing upon the existing regulatory responses to face recognition technology, this Part provides some early recommendations for how real-time identification should be addressed. This analysis is by no means intended as a complete policy response to this application of face

---

211 (1890).

200. *See id.*

201. Video Voyeurism Prevention Act, 18 U.S.C. § 1801 (2004).

202. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977) ("The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.").

203. Logeais & Schroeder, *supra* note 198, at 526.

204. Welinder, *supra* note 108.

205. *Id.*

recognition technology. Rather, it is meant to start the dialogue while this application evolves to a point where its impact can better be analyzed.

A. Focus on Use Rather than Technology

When comparing FTC's Facing Facts report and the WP29 opinion broadly, it is clear that the latter offers far more concrete guidance with the respect to real-time identification. There are several reasons for this. First, the FTC did not intend to specifically address mobile technologies in its report, as is obvious from the case studies that it focused on and its suggestion that real-time identification apps may not yet exist. Second, the WP29 opinion applied concrete data protection legislation to this particular use. Given that there is no baseline privacy legislation in the U.S., the law is far less predictable and it is difficult for the FTC to provide concrete guidelines for how companies may use biometric data. Finally, and most importantly in my view, the FTC's focus was too broad. It sought to cover all kinds of face recognition technologies from software "ensuring that the frame for a video chat feed actually includes a face," to "virtual makeover tools that allow consumers to "try on" a pair of glasses or a new hairstyle online," and to "technologies that identify moods or emotions from facial expressions," just to name a few.[206] The WP29 opinion, on the other hand, focused only on a handful of online and mobile applications of the technology and provided a number of specific recommendations with respect to those applications. The specificity of its recommendations not only better protects consumers, but also makes it easier for app developers to determine the bounds of the law when they work on new services.

In my earlier recommendations on face recognition technology in social networks, I argued against a blanket prohibition on face recognition technology because the technology also presents useful applications, many of which we are still to discover.[207] Digital cameras, for example, use face detection to focus the lens on a face.[208] Face recognition technology built into photo management apps like Picasa can help users who exhaust the seemingly limitless flash cards in their digital cameras to automatically categorize all the photos on

206. FACING FACTS, *supra* note 107, at i, 5.

207. *Id.*

208. *See Face Detection*, SONY, http://www.sony.co.uk/hub/learnandenjoy/2/1 (last visited Apr. 26, 2012).

their computers.[209] The gaming device Kinect uses face recognition to keep track of different players so that friends can challenge each other in dance or sports in their living rooms rather than just exercising their thumbs with the more traditional forms of video games.[210]

Particular uses of the technology, however, may be more harmful. Though it is too early to tell, real-time identification apps may arguably fall in the more harmful category, at least when used by strangers. As such, they could invite more stringent regulation, making their implementation very difficult, if not impossible. Any regulation that could overly burden or eliminate uses of technology needs to be preceded by very careful analysis. But more importantly, any such regulation should narrowly target a *use*, rather than the *technology*. With respect to real-time identification, this means regulation should focus on real-time identification apps rather than regulation covering all uses of face recognition technology. Technology neutrality is a well-established regulatory principle that is particularly beneficial for rapidly developing technologies.[211] I would argue that tech-neutrality is incorporated into the EU Data Protection Directive, which regulates automatic processing of data—a *use*. Though the WP29 opinion appears to focus on a *technology*, it merely applies the tech-neutral Directive to particular uses of face recognition. In that sense, the WP29 opinion is fundamentally different from the FTC's Facing Facts report, which seeks to provide guidance for developing various applications that use face recognition technology.[212] Going forward, as regulators develop a response to real-time identification with more teeth than the Facing Facts report, they do well in considering the tech-neutrality principle. A tech-neutral solution does not mean that regulation has to be particularly broad. It could, for example, specifically address the instantaneous

209. *See* Mitchell, *supra* note 132.

210. Douglas Gantenbein, *Helping Kinect Recognize Faces*, MICROSOFT RESEARCH (Oct. 31, 2011, 9:30 AM), http://research.microsoft.com/en-us/news/features/kinectfacereco-103111.aspx.

211. *See* Bert-Jaap Koops, *Should ICT Regulation Be Technology-Neutral?*, *in* 9 IT & LAW SERIES, STARTING POINTS FOR ICT REGULATION, DECONSTRUCTING PREVALENT POLICY ONE-LINERS 77 (Bert-Jaap Koops et al. eds., 2006) (arguing that "[l]egislation should abstract away from concrete technologies to the extent that it is sufficiently sustainable and at the same provides sufficient legal certainty"), *available at* http://ssrn.com/abstract=918746.

212. Unlike the WP29 Opinion, which specifically applies the tech-neutral Directive, the FACING FACTS report only "draw[s] upon the three core [tech-neutral] principles outlined in the FTC's March 2012 report" and is primarily based upon a workshop on face recognition technologies. FACING FACTS, *supra* note 107, at 1.

processing of biometric data, which would apply to real-time identification as well as other similar processes.

It may seem that broad regulation of face recognition technology will be more effective because it will cover new face recognition technology implementations as they evolve, and does not as easily become outdated. But that reasoning has two major flaws. First, while broad regulation of automatic face recognition could provide regulation of new implementations as they crop up, that regulation may not be suitable for them because those uses would not have been anticipated when the regulation was developed. The regulation will likely unduly burden a new implementation and may not address any of its problems (if there are any such problems to be addressed). Second, regulation of particular uses may actually outlast seemingly broader regulation of a technology.[213] Consider, for example, a law that would regulate collection of data indicating a person's real-time location. If well-drafted, such a law would apply to sensitive location data in geolocation apps and real-time identification apps alike. And it would apply to new technologies that would expose individuals in the same manner.[214] It would be more targeted at the relevant harm and address all new technologies that have similar uses. Using Lawrence Lessig's vocabulary, the law would not need to be *translated* into the language of the future—it will be timeless.[215] Likewise, protection against identification of anonymous individuals in public could regulate future technologies that would identify individuals from a distance based on their smell or the rhythm of their heartbeat.[216] Conversely, the regulation of face recognition

213. *See* Koops, *supra* note 211; *but see* Christian Laux, *Must RFID-Legislation Be Technology Neutral?*, THE CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL (Apr. 12, 2007, 1:02 PM), http://cyberlaw.stanford.edu/blog/2007/04/must-rfid-legislation-be-technology-neutral (arguing that tech-specific regulation may be appropriate for radio frequency identification given that it allows the tracking of goods at a time of convergence of the physical space and cyberspace through the "Internet of Things").

214. *See* Koops, *supra* note 211 (noting that "particular attention must be given to the sustainability of laws that target technology, because there is a greater risk than usual that changes in the subject matter may soon make the law obsolete").

215. *See* LAWRENCE LESSIG, CODE 157-169 (2d ed. 2006).

216. *See* Jacob Aron, *Your Heartbeat Could Keep Your Data Safe*, NEWSCIENTIST (Feb. 11, 2012), http://www.newscientist.com/article/mg21328516.500-your-heartbeat-could-keep-your-data-safe.html; JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 215 (2007) (implying that odor recognition technology may one day recognize individuals, provided that they have unique bodily odors); *see also* Paul Marks, *Google Glass App Identifies You by Your Fashion Sense*, NEWSCIENTIST (Mar. 7, 2013), http://www.newscientist.com/article/mg21729075.600-google-glass-app-identifies-you-by-your-fashion-sense.html.

technology would be useless with respect to these new technologies even though they raise very similar concerns. Indeed, one day, regulation of face recognition technology could sound just as outdated as the regulation of gramophones or video cassette tapes sounds today.[217]

B. Security by Design

Security is always important when a company holds personal data. It is particularly important for biometric data given that, unlike a compromised password or a stolen credit card, a person's biometric data cannot simply be replaced.[218] If the photos or biometric data are transferred between a mobile app and a website, there are additional security risks because the data has to pass through multiple servers, each of which could possibly be compromised. The WP29 therefore recommended that apps be designed to locally process and store the data.[219] If that is not possible, the app developer should consider using encrypted communication channels or making use of cryptographic protocols for processing data.[220] An individual's biometric data could also be split up over several servers to make recognition difficult if one of them is compromised.[221]

Given that the app will already have a person's biometric data, it may be practical to use biometric encryption when accessing it.[222] This would require the app to turn the biometric data into a random string that can be used as a key to encrypt and decrypt information.[223]

---

217. For example, the regulation of "video cassette tapes" in the Video Privacy Protection Act (VPPA) has caused the legislation to quickly seem antiquated. However, the VPPA also regulates "similar audio-visual technology," which essentially means that this is regulation of a *use* rather than a *technology*. Therefore, it has been applied to various subsequent technologies like DVDs and online video. Yana Welinder, *Dodging the Thought Police: Privacy of Online Video and Other Content Under the "Bork Bill,"* HARV. J. L. & TECH. DIG. (Aug. 14, 2012, 6:11 PM), http://jolt.law.harvard.edu/digest/legislation/dodging-the-thought-police-privacy-of-online-video-and-other-content-under-the-bork-bill.

218. *See Face Facts: A Forum on Facial Recognition Technology*, FED. TRADE COMM'N 1 (Dec. 8, 2011), http://www.ftc.gov/video-library/transcripts/120811_FTC_sess3.pdf (Alessandro Acquisti testifying that "[i]t's much easier to change your name and declare 'reputational bankruptcy' than to change your face.").

219. WP29 Opinion, *supra* note 16, at 8.

220. Margarita Osadchy et al., *SCiFI – A System for Secure Face Identification*, BENNY PINKAS, 1 (May 2010), http://pinkas.net/PAPERS/scifi.pdf; *see also* WP29 Opinion, *supra* note 16, at 8.

221. Osadchy et al., *supra* note 220, at 1.

222. *Id.*

223. Ann Cavoukian & Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy*, INFORMATION AND PRIVACY

Biometric encryption is sometimes considered more secure because it uses a person's face instead of a password that the person can remember.[224] Because the user does not have to memorize the data derived from her facial features, biometric identifiers can use longer and more complicated numbers that are more difficult to guess or steal.[225] However, it may be less effective when the identity of the user is known and the data could be decrypted with a photo of the user downloaded from a social network or found in an online image search.[226] For added security, the encryption could be based on biometric data combined with a password that is selected by the user.[227]

Some may argue that there is a technical hurdle if someone tries to steal biometric data that has been derived using proprietary face recognition software. The argument goes something like this: a biometric database compiled with proprietary software can only be used to identify the individuals using the same version of that particular software. Consequently, a security breach only as to the database may not affect the individuals unless there is also a security breach as to the particular proprietary software. This argument is based on "security by obscurity," which in security research is not considered to be a solid security strategy.[228] In essence, keeping the algorithm secret will not help because attackers will eventually find vulnerabilities in the system.[229] Indeed, it may be more effective to open source the security development because, "given enough eyeballs, all bugs are shallow."[230] Some may of course choose to keep proprietary software secret for business reasons, but it is certainly no substitute for encrypting their data.[231]

COMMISSIONER OF ONTARIO, CANADA, 1 (Mar. 2007), http://www.ipc.on.ca/images/resources/bio-encryp.pdf.

224. *Id*. at 12, 18.

225. *Id.*

226. See *id*. at 12 (discussing how biometric identification can be spoofed with images instead of the actual face).

227. Lucas Ballard et al., *Towards Practical Biometric Key Generation with Randomized Biometric Templates*, MICROSOFT RESEARCH, 1 (Oct. 2008), http://research.microsoft.com/pubs/121269/rbts.pdf.

228. *See* Peter Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Agencies*, 42 HOUS. L. REV. 101, 105 (2006).

229. *Id.*

230. ERIC S. RAYMOND, THE CATHEDRAL AND THE BAZAAR 30 (1999) (describing Linus's Law of open source development).

231. *See* Steve Bellovin, *Security Through Obscurity*, RISKS DIGEST (June 6, 2009, 10:21 PM), http://catless.ncl.ac.uk/Risks/25.71.html#subj19 (citing "Kerckhoffs' second principle, translated as "[t]he system must not require secrecy and can be stolen by the enemy without

Even if biometric databases are kept secure, individuals are still not safe from automatic face recognition by strangers. Around one seventh of the earth's population could have a labeled photo of them available on Facebook.[232] Others provide their headshots online through LinkedIn or Google+, or on their company website. Those images are connected to their name and often some other identifying information that allows for instant recognition. And so, it is not difficult to compile a biometric database using images available online.[233] The FTC has therefore recommended that companies that store labeled photos should maintain their security and protect them from being scanned for unauthorized uses.[234] Even applications that only process images without storing them—like digital signs—need to consider the security to prevent outsiders from accessing the images while they are being processed.[235] Thus, if a real-time identification app only allows users to identify their Facebook friends while pointing their camera phone at them without taking or storing any photos, it would still need to ensure that third parties cannot compromise this process.[236]

C. Ask (the Right Person) for Permission

While disagreeing about the type of consent that should be required, the FTC report and the WP29 opinion are consistent about whom companies should ask for permission: the person to be identified.[237] The FTC report primarily recommends that companies seek "affirmative express consent" before either allowing strangers to recognize an individual or using the individual's photo in a materially new way.[238] The WP29 opinion states that consent should be required more broadly whenever a company collects photos or personally

causing trouble").

232. *See* Alex Wilhelm, *Facebook: Our 1 Billion Users Have Uploaded 240 Billion Photos, Made 1 Trillion Connections*, THE NEXT WEB (Jan, 15, 2013, 7:18 PM), http://thenextweb.com/facebook/2013/01/15/facebook-our-1-billion-users-have-uploaded-240-billion-photos-made-1-trillion-connections/.

233. Alessandro Acquisti et al., *Face Recognition Study — FAQ*, HEINZ COLLEGE, CARNEGIE MELLON UNIVERSITY, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ (last visited Nov. 20, 2012).

234. FACING FACTS, *supra* note 107, at ii, 11.

235. *Id.* at 13.

236. *See* Ashkan Soltani, *FacePalm*, ASHKANSOLTANI.ORG, http://ashkansoltani.org/docs/face_palm.html (last visited Oct. 2, 2012).

237. FACING FACTS, *supra* note 107, at iii; *see* WP29 Opinion, *supra* note 16, at 5.

238. FACING FACTS, *supra* note 107, at iii.

identifiable biometrics for automatic processing.[239] Both agencies, however, are in agreement that consent must be provided by the individual whose face is identified rather than the person that uses the face recognition technology or provides the photo.[240] This will be essential for regulation of real-time identification apps because they will mostly identify individuals other than the user who downloads the app to her phone.

The regulatory agenda with mobile apps right now is to ensure that they provide notice and obtain consent from the phone user before using their sensitive data such as geolocation, contacts, or surfing habits.[241] App developers are instructed to develop short and sweet privacy notices that users can review when they download the app.[242] They are encouraged to develop privacy icons and communicate their data practices to app users via privacy dashboards and just-in-time notices.[243] This approach, however, will not be sufficient for real-time identification apps, which use sensitive data that pertains to a third party who will not have access to those notices on the phone.

Consent is meaningless unless the person knows to what she is consenting. A clause hidden in a social network's term of use should not be legally sufficient to put an individual on notice that apps can tap into that network to gather identifying data. Given that users generally do not read the terms, the WP29's focus on the main purpose of the app is helpful.[244] If the main purpose of an app is to recognize faces, the users who provide their photos will anticipate that they will be used in this manner. If the main purpose is different, however, a separate notice and consent is needed to put the users on notice.[245] The FTC has articulated a similar idea in its recent consumer privacy guidelines, which provide that separate consent may not be required when a data "practice is consistent with the context of [a] transaction or the consumer's existing relationship with

239. WP29 Opinion, *supra* note 16, at 5.

240. FACING FACTS, *supra* note 107, at iii; *see* WP29 Opinion, *supra* note 16, at 5.

241. *See* FTC MOBILE PRIVACY DISCLOSURES, *supra* note 54; FTC CONSUMER PRIVACY REPORT, *supra* note 61*;* Kamala D. Harris, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, STATE OF CAL. DEP'T OF JUSTICE, OFFICE OF THE ATTORNEY GEN., 1 (Jan. 2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

242. FTC CONSUMER PRIVACY REPORT, *supra* note 61.

243. FTC MOBILE PRIVACY DISCLOSURES, *supra* note 54.

244. WP29 Opinion, *supra* note 16, at 7.

245. *See id.*

the business."[246]

Limited non-consensual collection and processing may be acceptable in narrow situations to allow apps to determine whether a person has consented.[247] It may also be necessary to find missing persons or to identify an injured individual who is unable to consent.[248] Such exceptions can be complemented by technology that allows individuals to object to even this preliminary collection and processing—perhaps by registering their general objections beforehand. To avoid generating a database of objecting individuals similar to the Do-Not-Call register, there may be ways to communicate an objection directly to a real-time identification app.[249] Regardless of how it is achieved, an individual should have the ability to avoid collection altogether, particularly as apps do have a tendency to collect more data than necessary and to not take adequate precautions that the information is permanently deleted afterward. This brings us to the next recommendation: limited collection and regular deletion.

D. Collect Less; Delete More

Even when biometric data is collected for a particular purpose and pursuant to informed consent, there is the potential for subsequent *function creep*—i.e. that the data could later be misused for a different purpose.[250] When the FTC held a hearing in 2012 to consider how companies should protect consumer privacy going forward, several groups representing the consumers expressed concern that companies are allowed to collect more data than necessary to provide their

246. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 39.

247. *See* WP29 Opinion, *supra* note 16, at 5.

248. *See* Directive, *supra* note 169, art. 8(c) (providing an exception to the consent requirement when "processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent").

249. For example, a camera phone could pick up a message via infrared light emitted by a device on a person indicating that she does not wish to be recognized. *See* Welinder, *supra* note 108, at 225 (discussing patented technology that would enable a camera phone "to receive messages via infrared light [that] . . . could for example read: 'Please do not collect my biometric data.'"); Jack Purcher, *Apple Working on a Sophisticated Infrared System for iOS Cameras*, PATENTLY APPLE (June 2, 2011, 7:19 AM), http://www.patentlyapple.com/patently-apple/2011/06/apple-working-on-a-sophisticated-infrared-system-for-ios-cameras.html. Alternatively, regulators could establish certain free-zones from face recognition, similar to prohibitions on photographing commonly found in public restrooms and gym changing rooms.

250. Article 29 Data Protection Working Party, *Opinion on 'Developments in Biometric Technologies*,' 2012 00720/12 (WP 193) (EN) 2012 O.J. (L 720) 17 (EN), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (describing "function creep").

services.[251] Companies also often lack clear data retention policies that would determine when data should be deleted. Excessive collection of data and its retention for an indefinite time exposes consumers to risks that the data can be misused later. This is particularly problematic for companies that use location data, which can be used to predict a person's future movement. It is likewise a problem for biometrics that can be misused to de-anonymize faces in the street. Mobile apps that collect and store this kind of data therefore need to limit their collection and regularly delete data that is not needed for their services. Problematically, mobile app developers often lack the organizational infrastructure to maintain a good data retention policy.[252]

The FTC and WP29 are mostly in agreement on this point. The FTC has incorporated data collection and retention into its "privacy by design" principle.[253] It recommended that companies only collect as much data as consumers expect based on their services.[254] Any additional collection should be accompanied by a separate, timely, and conspicuous disclosure (in addition to the regular privacy policy).[255] The FTC further recommended that companies delete or anonymize data after it has served its initial purpose.[256] The FTC invited industry groups to come up with reasonable retention periods for different businesses.[257] It noted specifically that companies collecting location data—like real-time identification or geolocation apps—should delete that data early.[258] The FTC also encouraged the development of "eraser button[s]" to allow consumers to directly delete the data that they upload.[259] To be effective, the buttons need to actually delete data from companies' databases and not only from

---

251. *See* FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 26-28.

252. Mathew J. Schwartz, *Data Retention Policies Absent Or Partially Implemented*, INFORMATION WEEK (Aug. 5, 2010, 8:00 AM), http://www.informationweek.com/storage/data-protection/data-retention-policies-absent-or-partia/226600018 (reporting an Applied Research study, which showed that "87% of IT and legal professionals believe that having a formal data retention plan is important for knowing which information to retain or delete[, while] only 46% of their organizations actually have such a plan").

253. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 44.

254. *Id.* at 27.

255. *Id.*

256. *Id.* at 28.

257. *Id.* at 29.

258. *Id.*

259. *Id.* at 29, 70 (giving Facebook as an example of companies that have already implemented these kind of buttons).

the consumer-facing side of the product.[260] Today, deleting a photo in Facebook does not necessarily protect a user from being identified with real-time identification apps because the photo is only removed from the user's profile and it may not be deleted from Facebook's database until 90 days after the user completely deletes her profile.[261]

Consistent with its general privacy framework, the FTC's report on face recognition recommended that companies develop retention policies for photo and biometric data.[262] Photos and biometric data should only be retained while needed to provide the relevant service.[263] So, if a user deletes her account or turns off the face recognition function, the data is obviously no longer needed.[264] As an example, the FTC cited the face recognition feature in the Google+ social network, which deletes all biometric data once a user withdraws her opt-in consent to use the feature.[265]

The WP29 opinion, for its part, applied the minimal collection principle found in the EU Data Protection Directive to automatic face recognition.[266] It stated that apps should collect the minimal amount of biometrics necessary to carry out the service.[267] It also noted that data must be deleted once it is not necessary for the purpose for which it was collected, such as when the only purpose of the face recognition was to identify the individual to determine if she previously consented to the use of her data.[268]

---

260. *See, e.g.*, Lance Ulanoff, *Snapchat CEO: Delete Is the Default*, MASHABLE (Apr. 16, 2013), http://mashable.com/2013/04/16/snapchat-ceo-delete-default/ (describing a chatting service that deletes pictures from service, as well as the recipient computer, within seconds of delivery).

261. *See, e.g.*, Ryan Budish, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1884-85 (2007) (suggesting that deletion of names from a biometric database would allow "citizens [to] secure their privacy without hiring attorneys or clogging the judicial system"); *see also Facebook Data Use Policy*, *supra* note 31 (stating that "some information may remain in backup copies and logs for up to 90 days" after an account is deleted); *but see* FACING FACTS, *supra* note 107, at 18 n.70 (referring to Facebook's testimony that "Facebook deleted any previously collected biometric data" "if a user opted out of Facebook's 'Tag Suggest' feature").

262. FACING FACTS, *supra* note 107, at ii.

263. *Id.* at 11.

264. *Id.* at 11, 18.

265. *Id.* at 18.

266. WP29 Opinion, *supra* note 16, at 5, 8; Directive, *supra* note 169, art. 6.

267. WP29 Opinion, *supra* note 16, at 5 ("[P]rocessing must first be compliant with data quality requirements (Article 6). In this case the digital images of individuals and the respective templates must be "relevant" and "not excessive" for the purposes of the facial recognition processing.").

268. WP29 Opinion, *supra* note 16, at 5*d*.

It is clear that American and European regulators alike are thinking about data minimization with respect to automatic face recognition. Companies would do best to adopt data retention policies early before they become overwhelmed by data that they collect. Avoiding unnecessary collection and retention will not only protect consumers from misuse within companies, but will also prevent misuse by third parties if there is a security breach and make it easier for companies to respond to law enforcement requests.

E. Think About the Context and User Experience Design

Real-time identification based on photos uploaded to a social network or otherwise available online presents a conceptual problem for our traditional understanding of privacy. Even though many would consider real-time identification of people in photographs posted online to be a privacy violation, traditionally, those photos would not qualify as secret information or information found in a completely private space.[269] One privacy theory that can address this issue is Helen Nissenbaum's theory of contextual integrity.[270] I have previously applied this theory to explain the controversy surrounding the use of face recognition in social networks.[271] Essentially, that scenario violates contextual integrity by transforming information that users share through photos, to personally identifying biometric data and sharing the information with new recipients beyond users' control.[272] Real-time identification exacerbates this problem by using information shared in an online context to identify individuals in an offline context. It can link various online actions to an otherwise anonymous face. Offline, it can also use biometric data to determine the location of an individual. There are thus two transformations of information: from photos to biometric data and, ultimately, to location data. The transformations evidence "a prima facie violation of contextual integrity," which can only be overcome if the practice advances an important social concern.[273] This contextual analysis should be taken into account when designing a service to avoid abusing users' trust.

The FTC has also adopted something resembling Nissenbaum's

269. Welinder, *supra* note 108, at 180-81.

270. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 55, at 2.

271. Welinder, *supra* note 108, at 186-88.

272. *Id.*

273. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 55, at 150, 182 (describing "a prima facie violation of contextual integrity").

contextual analysis in its new recommended business practices for consumer privacy:

> Companies should limit data collection to that which is consistent with *the context* of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law. For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document.[274]

Similarly, the FTC has emphasized the scope of a transaction's context when discussing notice and consent for face recognition processes. It noted, for example, that automatic face recognition is inconsistent with the context of a social network.[275] A social network should therefore separately notify its users if it decides to start using photos to automatically identify faces.[276] When it cannot provide notice to individuals—perhaps because they do not use the social network—it should not use labeled photos of them to create a biometric database.[277] The separate notice must be accompanied by a conspicuous ability to opt-out and a mechanism that deletes all photos and biometric data once a user opts-out.[278] I would argue that opt-out choice—however conspicuous—is not sufficient to protect against extra-contextual face recognition. Opt-out settings are notoriously underutilized, particularly by children.[279] Given that users upload photos to social networks with the particular purpose of socializing with their friends, specific opt-in consent should be required before using them in this vastly different manner.

The FTC's attention to the context of transactions is similar to the WP29's consideration of the main purpose of an application when determining whether separate user consent is necessary.[280] Both are

---

274. FTC CONSUMER PRIVACY REPORT, *supra* note 61, at 19.

275. FACING FACTS, *supra* note 107, at 18.

276. *Id.* at 18-19.

277. *Id.* at 19.

278. *Id.*

279. *See* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, 2006 PRIVACY ENHANCING TECH. WORKSHOP 16, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.8177&rep=rep1&type=pdf ("[A]mong current members, 30% claim not to know whether [Facebook] grants any way to manage who can search for and find their profile, or think that they are given no such control."); *See also* Michelle Madejski et al., *The Failure of Online Social Network Privacy Settings*, FUTURE OF PRIVACY FORUM (July 2011), http://bit.ly/MlkhFT.

280. WP29 Opinion, *supra* note 16, at 7; *see supra* Part III.C.

examples of a general trend towards focusing on users' experience of transactions, rather than written privacy policies.[281] Developers can influence the user experience through product design—effectively creating a desired context. User experience design instinctively makes a user aware of data collection without the need to read or understand a privacy policy. It can also provide notice to individuals beyond the primary user of a product. For example, a camera can produce a shutter sound or a flash that tells a person that she is being photographed.[282] Similarly, security cameras are sometimes equipped with a screen showing customers that they are being recorded in real time instead of posting a "smile, you're on camera" notice next to the camera.[283] One could imagine a real-time identification app in a phone or a pair of computer glasses that loudly announces the name of a recognized subject, putting her on notice that she is identified and perhaps allowing her to prevent an embarrassing photo from being posted to her social network profile. While the exact implementation of such a feature might vary, the general idea of notifying subjects when recognized is a palpable example of privacy protective user experience design.[284] An alternative design would be an app that allows each user to compile a biometric database specific to an individual device. Each user would then only be able to recognize individuals that appear in her own user-generated database.[285] The

281. Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1653 (2011) ("A growing body of literature in the field of human-computer interaction has focused on what are known as 'privacy indicators'—designs such as logos, icons, settings, and seals used to intuitively convey a website's policy regarding collection and use of personal information."); *See* Calo, *supra* note 53, at 1033-34, 1041 (2012) (suggesting that privacy notices be designed based on users' "familiarity" with older technologies and their "psychological responses" to certain elements, as well as by "demonstrating the result of company [data] practices"); *See* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1018-19, 1021 (2012) (stating that "over the past two decades, a growing body of privacy-focused [human-computer interaction] research has emerged to address the development of ubiquitous computing technologies" and noting that a user-centric form of privacy by design "demands attentiveness to context and human experience, the very attributes that companies, through privacy notices, attempt to disavow and make irrelevant."). At a more general level, user experience design is based on the more established research fields of cognitive psychology and human factors. *Id*. at 1020.

282. *See* Calo, *supra* note 53, at 1036-37 ("Analog cameras make a click and, often, emit a flash when taking a picture."). *Id*.

283. *See Photo of Self-Checkout at Home Depot*, FLICKR (Apr. 19, 2011), http://www.flickr.com/photos/ginger-jengibre/5635513442/in/photostream/.

284. The feature could, for example, also generate a digital record of the recognition and transmit it to the identified individual via email or a text message, including the time and place of the recognition and the identity of the device that performed it.

285. The user-generated database could also contain individuals that have never met the

design would play on people's expectations that a person they interact with may remember them next time, no matter how brief the initial interaction. To maximize innovation in privacy design, regulation should not try to mandate any particular design like a camera shutter sound,[286] but should instead leave it to developers to come up with effective solutions to the third-party notice problem.[287]

CONCLUSION

Although face recognition technology has been evolving for decades, its policy ramifications remained largely unexplored. The recent implementation of the technology into consumer applications provoked rapid policy responses. These responses, however, did not comprehensively address real-time identification. The FTC report on face recognition technology, in particular, implied that real-time identification apps were yet to hit the market and provided some preliminary recommendations of what such apps should avoid.[288]

In reality, however, real-time identification apps are already on sale and call for us to begin thinking about when and how their use may be inappropriate. While these apps resemble mobile apps that use geolocation data, real-time identification apps raise additional issues because they collect location information about third parties and are capable of identifying anonymous faces in the street. The regulatory solutions that are being developed for geolocation apps—such as shorter privacy notices for mobile screens and just-in-time disclosures to users—will therefore not work for real-time identification.

As the FTC will inevitably have to review real-time identification apps, it would do well to focus on this particular use rather than seeking to address it along with other face recognition applications. That will ensure technology neutral regulation that addresses the specific issues raised by real-time identification and that will apply to similar uses in the future without affecting vastly

---

user but opt in to being recognizable by her—making blind dating and other such first meetings much less awkward.

286. *Contra* Camera Phone Predator Alert Act, H.R. 414, 111th Cong. (2009), *available at* http://www.govtrack.us/congress/bills/111/hr414 (seeking to require camera phones to make a sound while photographing).

287. *See* Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1019 (2012) (noting "that Facebook, Google, Apple, Microsoft, Twitter, and other companies employ significant numbers of [human-computer interaction] researchers" that look into the issue of user experience design).

288. FACING FACTS, *supra* note 107.

different uses of face recognition technology. With respect to the apps available today, the policy response should consider how relevant individuals could be put on notice, given that these apps affect other individuals in addition to the app user. The policy response will also need to consider how these apps can minimize their data collection and retention and keep the data secure. Importantly, the policy will also need to consider the initial context in which the data is collected—particularly given that today's apps take advantage of photos that people share with their friends in social networks. Future real-time identification apps may raise additional issues because of their design, which will need to be addressed at that time. This should not stop us from getting the ball rolling.