THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XV STLR.ORG FALL 2013

NOTE

THE RISE OF A NEW TYPE OF SURVEILLANCE FOR WHICH THE LAW WASN'T READY[†]

Kirill Levashov[*]

This article discusses the rising use of facial recognition technology in society and in law enforcement, and its legal implications. Section I describes the technology and how it works. While the potential uses for this technology are too numerous to list, this section goes on to describe the most widespread and troubling current uses, as well as some of the planned uses that illustrate the scope that the technology has the potential to achieve, and why that could be a problem. Section II discusses some of the more prevalent legal concerns that accompany the rise of this technology, such as privacy violations, chilling of free speech, and stalking. Section III analyzes the existing state of the law, and suggests some channels that may offer protection from the concerns raised in section II, while noting that these channels were not designed with facial recognition technology in mind so the protections offered may be weakened or, depending on the leanings of a court of law, nonexistent. The article closes by suggesting additional statutory protections that could be enacted to more completely address the issue, either piecemeal or as part of a larger regulatory scheme.

---

* Kirill Levashov is a 3L at Columbia Law School. He has a B.A. in Psychology and Economics from University of California, Davis. He will begin work at Weil Gotshal and Manges beginning in 2014.

INTRODUCTION

Javier Magana's property spread over twenty-two mostly wooded acres, dotted with "No Trespassing" signs and blocked at the entrance by a locked gate. On July 12, 2012, law enforcement officers entered the property and found marijuana plants growing in a small clearing. Without obtaining a warrant, police installed surveillance cameras around the area. The cameras allegedly captured images of Magana, who was subsequently charged with several crimes, including knowingly and intentionally manufacturing and possessing with intent to distribute marijuana. Magana and a co-defendant filed motions to suppress all images gathered by the cameras, claiming that the installation of surveillance without a warrant violated their Fourth Amendment right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1]

The Eastern District of Wisconsin disagreed and refused to suppress the images. The installation of the cameras was, according

1. U.S. Const. amend. IV.

to the court, "the use of technology as a substitute for ordinary police surveillance."[2] Citing *United States v. Knotts*,[3] the court reiterated that "nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afford[] them."

The ruling highlighted the increasing involvement of surveillance cameras in the legal system. Courts are becoming more tolerant of their use in law enforcement—even when it is warrantless—and police forces are becoming more reliant on them, both in small towns and big cities. In Ypsilanti Township, Michigan, ten cameras survey the most populous public areas. At nearby Eastern Michigan University, over five hundred cameras overlook the campus.[4] On a larger scale, the Lower Manhattan Security Initiative utilizes four thousand cameras south of Canal Street in New York, all of which are monitored constantly by the New York Police Department (NYPD).[5] Police Commissioner Raymond Kelly announced his intent to introduce "smart cameras" into the surveillance system, which would "aggregate data from 911 alerts, arrest records, mapped crime patterns, surveillance cameras, and radiation detectors."[6]

Public cameras could soon form the cornerstone for a new initiative currently being piloted by the Federal Bureau of Investigation (FBI).[7] The Next Generation Identification (NGI) system will use security footage from public cameras to identify suspects and people of interest. The system, which will serve as an upgrade to the current Integrated Automated Fingerprint

---

2. United States v. Mendoza, No. 12-cr-154, 2012 WL 5331216, at *2 (E.D. Wis. Oct. 9, 2012) (order denying motion to suppress).

3. United States v. Knotts, 460 U.S. 276, 282 (1983).

4. John Counts, *Law Enforcement Agencies Continue to Expand the Use of Surveillance Cameras*, ANN ARBOR NEWS (Dec. 26, 2012), http://www.annarbor.com/news/law-enforcement-agencies-continue-to-expand-the-use-of-surveillance-cameras/.

5. Heather Kelly, *After Boston: The Pros and Cons of Surveillance Cameras*, CNN.COM (Apr. 26, 2013), http://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/index.html.

6. *Bloomberg: New Yorkers Will 'Never Know Where Our Cameras Are'*, RT.COM (Apr. 26, 2013), http://rt.com/usa/bloomberg-never-know-where-cameras-477/.

7. Sara Reardon, *FBI Launches $1 Billion Face Recognition Project*, NEWSCIENTIST MAG. (Sept. 7, 2012), http://www.newscientist.com/article/mg21528804.200-fbi-launches-1-billion-face-recognition-project.html.

Identification System (IAFIS), will integrate multiple forms of biometric data, including fingerprint, voice, iris, and facial data.[8] A pilot program of the NGI system is currently deployed in certain locales, but can only identify a person's face if he has a criminal record.[9] Increment 3 of the program was released in May 2013,[10] incorporating powerful new biometric algorithms provided by MorphoTrak, "the world leader in multibiometric technologies for fingerprint, iris and facial recognition, and an acknowledged expert in identification systems."[11] A full-scope program is set to roll out in 2014, with nationwide coverage and the potential addition of non-criminal—or even non-government—databases of photographs.[12]

Despite the fact that facial recognition technology has risen to this level of prominence in law enforcement, the collection of biometric facial data remains largely unregulated. The gathering of this type of data raises many concerns, including threats to privacy, security, and free association.[13] Some existing protections may cover the collection of biometric data, but they are uncertain and relatively weak for data that is so unique and personal to the individual from whom it comes. To understand why further regulation is warranted, one must first understand how the technology works.

I. HOW FACIAL RECOGNITION TECHNOLOGY WORKS

Facial recognition technology uses a photographic camera combined with facial recognition software. This software is able to detect and isolate human faces captured by the camera and analyze them using an algorithm that extracts identifying features.[14]

---

8. *Id.*

9. *Id.*

10. *Lockheed Martin Team Delivers Major New Crime-Solving Capabilities Via FBI's Next Generation Identification System*, LOCKHEED MARTIN (May 15, 2013), http://www.lockheedmartin.com/us/news/press-releases/2013/may/isgs-NGI-inc3-05152013.html.

11. MORPHOTRAK, http://www.morphotrak.com/index.asp (last visited Oct. 24, 2013).

12. Reardon, *supra* note 7.

13. *Swire Presents at FBI/DOD Sponsored Facial Recognition Forum*, FUTURE OF PRIVACY F. (Mar. 21, 2012), http://www.futureofprivacy.org/2012/03/21/fpf-senior-fellow-presents-at-fbidod-sponsored-facial-recognition-forum.

14. Kevin Bonsor and Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm (last visited Mar. 3, 2013).

The algorithm identifies and measures "nodal points" on the face, which are defined by the peaks and valleys that make up human facial features. Using these measurements, the algorithm determines an individual's identifying characteristics, such as distance between the eyes, width of the nose, shape of cheekbones, and the length of the jawline.[15] The combination of a person's nodal points becomes that person's "faceprint," which is as unique and specific to each person as his or her face. The faceprint is then compared to a linked database of faceprints to determine whether the person can be identified. Presently, basic algorithms can gather faceprints from any image in which a person's facial geometry is clearly discernable, such as photographs or still frames from video cameras. Cutting-edge cameras with advanced algorithms are able to capture a three-dimensional image and compare it with a two-dimensional photograph from the database to which the camera is linked; others can store analyses of the unique texture of a person's facial skin.[16] Recently, infrared cameras have also been used, capturing and comparing the unique heat signatures given off by an individual's facial capillaries.[17]

The technology is not infallible, and its usefulness can be limited by several component factors: the location and mobility of the capturing camera, the accuracy and speed of the algorithm, and the size of the database of faceprints from which the algorithm can draw. Public cameras are generally stationary (though some are capable of rotation), so direct capture of images from which faceprints can be drawn is limited because the subject has to appear in the specific area that the camera covers. However, smartphone cameras can be enabled with facial recognition software. The FaceLook application[18] for the iPhone, for example, integrates with the Facebook application for that device, and determines a person's identity by comparing a photograph taken by the device's camera with the database of photographs that can be accessed through the Facebook application. However, even though the technology is mobile, the omnipresent and more discreet nature of a stationary public camera makes it an arguably better tool for some surveillance purposes.

---

15. *Id.*

16. *Id.*

17. Rachel Barclay, *Your 'Face Print' Is the Next Breakthrough in Personal Identification*, YAHOO! HEALTH (July 18, 2013), http://health.yahoo.net/articles/healthcare/thermal-face-scanning-next-best-way-id-everybody.

18. FACELOOK, http://www.ifacelook.com (last visited Mar. 3, 2013).

The accuracy of the algorithm is another significant limitation. In 2010, the National Institute of Standards and Technology reported a 99.71% accuracy rate for algorithms comparing two sets of still frontal images.[19] However, the accuracy rate drops when conditions are below optimal. Changes in lighting, position, facial hair, and blurriness can all decrease the effectiveness of an algorithm."[20] Even slight changes, like adding makeup, can make it difficult to match nodal points around the cheeks.[21] This problem manifested itself in April 2013 when law enforcement officials attempted to use facial recognition technology to identify suspects in connection with the 2013 Boston Marathon bombing. Despite the fact that photographs of suspects Dzhokar and Tamerlan Tsarnaev were in the photograph database used by law enforcement, the facial recognition system could not promptly match the photographs to the low-resolution images captured by surveillance cameras.[22] Algorithms are quickly improving, so this issue may become less significant as the technology matures. After the Boston bombing suspects were captured using other means, researchers at Michigan State University were able to match one suspect's photograph to a video provided by law enforcement.[23]

A substantial limitation comes from the size of the photograph database upon which the algorithm draws. A larger database of faceprints means that a larger percentage of the faces caught by the camera can be identified. The NGI pilot program uses a criminal database, so its algorithm can only identify people from captured camera images if they have a criminal history. When the program expands to its full scope, its usefulness will be amplified with each additional database of faceprints from which it

---

19. Emily Steel, *A Face Launches 1,000 Apps*, WALL ST. J. (Aug. 5, 2011), http://online.wsj.com/article/SB10001424053111903885604576488273434534638.html.

20. Carl Bialik, *Humans Trump Machines in Facial Recognition*, WALL ST. J. (Sept. 2, 2011), http://blogs.wsj.com/numbersguy/humans-trump-machines-in-facial-recognition-1085/.

21. Sarah Downey, *The Top 6 FAQs About Facial Recognition*, ONLY PRIVACY BLOG (Dec. 8, 2011), http://www.abine.com/blog/2011/the-top-6-facial-recognition-faqs/.

22. Sean Gallagher, *Why Facial Recognition Tech Failed in the Boston Bombing Manhunt*, ARSTECHNICA (May 7, 2013), http://arstechnica.com/information-technology/2013/05/why-facial-recognition-tech-failed-in-the-boston-bombing-manhunt/.

23. Tom Oswald, *Facial Recognition Technology Proves Its Mettle*, MSU TODAY (May 24, 2013), http://msutoday.msu.edu/news/2013/facial-recognition-technology-proves-its-mettle/.

can draw. The Department of Motor Vehicles (DMVs) of many states is a fruitful source; to prevent identify theft, many states' DMVs collect faceprints from driver's license applicants. The Oregon DMV started using facial recognition software in 2008 and anticipates "virtually all Oregonians will someday soon be part of the DMV facial recognition database."[24] Other government agencies with large databases include the Department of State, which possessed a database of 75 million photographs as of December 2011. However, some of the largest photograph databases have been collected by the private sector: in 2011, Flickr had a database of 3.4 billion photographs, Photobucket had 7.2 billion, and Facebook had a whopping 140 billion photographs, with an estimated 70 billion more to be added in 2012.[25] Although faceprints can likely be drawn from some of these photographs, the rights these websites' users possess to prevent their photographs from being used to collect faceprints remain undefined.

A. Existing and Planned Uses of Facial Recognition Technology

Facial recognition technology has been used for security purposes for over a decade. In 2000, the Mexican Federal Election Institute used a facial recognition system during Mexico's presidential election to prevent duplicate voter registration; a camera equipped with facial recognition technology verified each voter's identity to ensure that the voter had not previously registered under a different name.[26] In 2001, cameras scanned the crowd at Super Bowl XXXV, collecting biometric information, comparing primitive faceprints to a criminal database, and alerting security to the presence of any known criminals.[27] The technology has evolved significantly since then—in 2012, undercover police patrolled crowds at the Republican National Convention armed with smartphones that could snap photographs of "suspicious" people and transmit them to police computers for instant

---

24. Oregonian News Network, *Oregon DMV's Facial Recognition Program Hits 1.8 Million Photos*, OR. LIVE (Nov. 28, 2011), http://www.oregonlive.com/news-network/index.ssf/2011/11/oregon_dmvs_facial_recognition.html.

25. Downey, *supra* note 21.

26. *Mexican Government Adopts FaceIt Face Recognition Technology to Eliminate Duplicate Voter Registrations in Upcoming Presidential Elections*, L-1 IDENTITY SOLUTIONS (May 11, 2000), http://ir.l1id.com/releasedetail.cfm?releaseid=208762.

27. Declan McCullagh, *Call It Super Bowl Face Scan I*, WIRED MAG. (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571.

comparison to a faceprint database.[28] Law enforcement has begun to utilize the technology by maintaining faceprint databases with which to compare security camera footage, a tactic that has resulted in some success. In April 2013, the NYPD was able to acquire an arson suspect's name based on a side view of his head captured by a security camera.[29] The footage provided enough biometric information to create a match to the department's facial recognition database, and officers were able to apprehend the suspect in his girlfriend's apartment.[30] In another case, a suspect in a string of Bronx robberies was apprehended using a similar approach.[31] The suspect would call for-hire car services to request transportation, and would rob the drivers at gunpoint upon entering the vehicle.[32] The police retrieved a screenshot of the suspect's face captured by the dash camera of one of the vehicles, and were able to match it to a name by running it through a facial recognition database of criminal mug shots.[33]

The uses of facial recognition technology continue to expand, as Facebook,[34] iPhoto, and Picasaweb all have facial recognition features that can automatically tag people who appear in photographs.[35] SceneTap and Apple have filed patent applications for projects that will take the technology a step further. SceneTap's application describes an "apparatus and method for recording customer demographics in a venue or similar facility using cameras"[36]—the company sets up cameras enabled with facial

---

28. Josh Smith, *Undercover Police Used Smartphones to Keep Tabs on Protests in Tampa*, NAT'L J. (Sept. 17, 2012), http://www.nationaljournal.com/tech/smartphones-used-to-monitor-tampa-protests-20120917.

29. Rocco Parascandol & Joe Kemp, *Mezuzah Arsonist Snagged by an Ear Thanks to Facial Recognition Technology*, NEW YORK DAILY NEWS (Apr. 11, 2013), http://www.nydailynews.com/new-york/mezuzah-arsonist-snagged-ear-thanks-facial-recognition-technology-article-1.1313919.

30. *Id.*

31. Murray Weiss, *High-Tech NYPD Unit Tracks Criminals Through Facebook and Instagram Photos*, DNAINFO N.Y (Mar. 25, 2013), http://www.dnainfo.com/new-york/20130325/new-york-city/high-tech-nypd-unit-tracks-criminals-through-facebook-instragram-photos.

32. *Id.*

33. *Id.*

34. Justin Mitchell, *Make Photo Tagging Easier*, FACEBOOK BLOG (June 30, 2011), https://blog.facebook.com/blog.php?post=467145887130.

35. Josh Lowensohn, *Facial Recognition Face-off: Three Tools Compared*, CNET NEWS (Sept. 30, 2009), http://news.cnet.com/8301-27076_3-10363727-248.html.

36. U.S. Patent Application No. 13/324,671, Publication No. 20120147169 (published June 14, 2012) (Joseph Cole Harper, applicant).

recognition technologies at social venues that transmit information to its servers, and informs those who have downloaded SceneTap's smartphone application[37] how crowded the venue is, as well as the approximate age and gender distribution of its patrons. Cameras are currently installed at approximately four hundred bars nationwide.[38] Though the company has not yet enabled such in-depth capabilities, the patent application also describes the potential collection of patrons' ethnicities, heights, weights, and levels of attractiveness.[39] The company's CEO, Cole Harper, has said in an interview that he "could imagine SceneTap partnering with the government, say if it was trying to find a wanted person."[40] Apple's application describes a password protection system for personal electronic devices in which a person uses his or her face as a biometric password to unlock the device rather than entering a passcode into the device.[41] If this feature is ultimately implemented, every enabled mobile device will, by default, be able to capture and distinguish faceprints.

II. CONCERNS THAT ARISE FROM THE USE OF FACIAL RECOGNITION TECHNOLOGY

A. Privacy and Security

A concern that unavoidably arises from the use of facial recognition technology is that identifying information can be collected and stored *en masse* without the need for any physical restraint or contact; as a result, a person is vulnerable to having identifying information captured and stored by the government or a private company (or even an individual) just by appearing in public.[42] With a sufficiently broad network of cameras, a person's

37. SCENETAP, http://scenetap.com/download (last visited Oct. 27, 2013).

38. Kashmir Hill, *SceneTap Wants to One Day Tell You the Weights, Heights, Races and Income Levels of the Crowd at Every Bar*, FORBES.COM (Sep. 25, 2012), http://www.forbes.com/sites/kashmirhill/2012/09/25/scenetap-wants-to-one-day-use-weight-height-race-and-income-to-help-you-decide-which-bar-to-go-to/.

39. *Id.*

40. *Id.*

41. U.S. Patent Application No. 13/049,614, Publication No. 20120235790 (published Sept. 20, 2012) (Lihua Zhao, applicant).

42. Michael Kelley, *Nothing Is Preventing the Feds from Putting You in a Facial Recognition Database*, BUS. INSIDER (Sept. 11, 2012), http://www.businessinsider.com/nothing-is-preventing-the-government-from-placing-you-into-a-facial-recognition-database-2012-9.

faceprint can be used as a tracking mechanism.[43] Unlike other tracking mechanisms, such as those requiring GPS tagging, the target would not have to be interfered or interacted with in any way other than by being captured on camera. Short of donning masks and ensuring their photographs do not appear anywhere on the Internet, individuals would be largely helpless in preventing themselves from being captured and tracked.

Particularly troubling is the fact that a faceprint is generally permanent and unchangeable.[44] Once a person's faceprint has been acquired and stored in a database, any party with access to that database can link that person's likeness to his identity. Unlike assigned identifiers, such as credit card numbers, a faceprint cannot be changed if a security breach causes the data to fall into undesirable hands.[45] Although the appearance of a person's face can change due to weight fluctuations, plastic surgery, or aging, future algorithms may be able to take such changes into account in determining matches. A research team at one university has gathered a database of pre- and post-surgery images of several hundred subjects, and has worked on determining the effectiveness of existing algorithms at identifying faces that have been modified by various types of plastic surgery.[46] In a 2010 paper, they determined that plastic surgery causes significant drops in accuracy of both appearance-based algorithms and texture-based

---

43. Joseph J. Atick, *Face Detection & Face Recognition Consumer Applications: Recommendations for Responsible Use*, INT'L BIOMETRICS & IDENTIFICATION ASS'N 1, 3 (Dec. 8, 2011), http://www.ibia.org/download/datasets/956/IBIA_recommendations_final.pdf.

44. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary), *available at* http://www.judiciary.senate.gov/pdf/12-7-8FrankenStatement.pdf.

45. *Id.* ("Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you. And facial recognition technology can allow others to access all of that information from a distance, without your knowledge and in about as much time as it takes to snap a photo.").

46. *Plastic Surgery Face Database*, IMAGE ANALYSIS AND BIOMETRICS @ IIIT-DELHI, http://research.iiitd.edu.in/groups/iab/facedatabases.html#plastic (last visited Sept. 29, 2013).

algorithms.[47] The type of surgery also affected the algorithm's effectiveness, with surgeries that changed the nodal points (such as variations to the nose, chin, and cheeks) affecting the algorithm more than changes to other areas such as the ear.[48] In a recent paper, an algorithm was developed that could automatically detect surgery on the nose, eyelid, forehead, and large-scale surgery (such as a face-lift).[49] The algorithm was even able to match subjects who had undergone surgery that affected the nodal points with reasonable accuracy (such as eyelid surgery, at 89.52%). Surgery that did not affect the nodal points, such as skin peeling, was matched as high as 97.26%.

The consequences of a third party's acquisition of a person's faceprint were demonstrated in 2011 by a team of researchers at Carnegie Mellon led by Alessandro Acquisti. Acquisti's group used a common webcam in combination with commercially available facial recognition software to photograph students on a college campus, draw faceprints from the photographs and compare them to Facebook data that was publicly available via search engine. With these simple tools, Acquisti's researchers were able to identify by name approximately one-third of the photographed students.[50] In a follow-up experiment, Acquisti combined the Facebook data he was able to extract using facial recognition technology with an algorithm that predicted a person's social security number based on location and date of birth.[51] In some cases, Acquisti was able to derive enough digits of an individual's social security number to conduct "effective, brute force identity-theft attacks."[52]

---

47. R. Singh et al., *Plastic Surgery: A New Dimension to Face Recognition*, *5 IEEE TRANSACTION ON INFO. FORENSICS & SECURITY* 441-48 (2010), *available at* http://research.iiitd.edu.in/groups/iab/TIFS10-FacePS.pdf.

48. *Id.* at 4.

49. Xin Liu et al., *Face Recognition after Plastic Surgery: A Comprehensive Study*, 7725 LECTURE NOTES IN COMPUTER SCI. 565-76 (2013), *available at* http://www.jdl.ac.cn/doc/2011/201319111512879_2012_accv_xliu_a%20comprehensive%20study.pdf.

50. James Temple, *Facial Recognition Software's Privacy Concerns*, SFGATE (June 20, 2012), http://www.sfgate.com/business/article/Facial-recognition-software-s-privacy-concerns-3645779.php. *See also* Alessandro Acquisti, *Face Recognition Study – FAQ,* CARNEGIE MELLON U., http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/ (last visited Oct. 30, 2013).

51. Alessandro Acquisti, *supra* note 50.

52. *Id.*

B. Stalking

In similar fashion, the use of facial recognition can enable stalking. This technology can facilitate the association of an unidentified faceprint with identifying information. Faceprints, devoid of any identifying information, can be gathered from many sources: online dating websites like Match.com and OKCupid, photo repositories like Picasa and Flickr, or even live faces on the street or on closed-circuit television.[53] Other faceprint repositories are inherently tied to identifying information: Facebook profiles, professional networking profiles (e.g. LinkedIn), and government or corporate databases. Before facial recognition technology existed, no direct line existed which could tie an unidentified faceprint to identifying information.[54] With the use of such technology, a faceprint can be extracted from a photograph taken of a stalking victim and matched to another photograph containing identifying information such as name or hometown.[55]

C. Freedom of Association and Speech

Furthermore, an unregulated proliferation of facial recognition technology, in combination with the increased presence of public cameras, could lead to an Orwellian suppression of self-expression. With cameras scanning crowds at rallies, protests, bars, and nightclubs, people may become fearful of acting in any way that they would not be comfortable revealing to the general public.[56] As discussed above, identifying information can be captured and stored without any need for physical interaction or disruption.[57] A relatively innocuous example could occur with a person who attends a political ceremony, but who

---

53. Alessandro Acquisti et. al., *Faces of Facebook: Privacy in the Face of an Augmented Reality*, CARNEGIE MELLON U. 12 (2011), http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

54. *Id.* at 7-8.

55. Mary Beth Griggs, *8 Weird Ways People Are Using Facial Recognition Software*, POPULAR MECHANICS, http://www.popularmechanics.com/technology/how-to/software/8-weird-ways-people-are-using-facial-recognition-software (last visited Oct. 30, 2013).

56. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. 16 (2012) (statement of Jennifer Lynch, Staff Attorney, Electronic Frontier Foundation), *available at* http://www.judiciary.senate.gov/pdf/12-7-18LynchTestimony.pdf.

57. Kelley, *supra* note 42.

wishes to keep his political beliefs otherwise private; such a person may find that his control of this information is limited. If any photographs are taken of him at the event—even without his knowledge—and uploaded to a social networking website enabled with facial recognition technology, the technology can generate a faceprint based on that photograph, which can be matched to other photographs of that person appearing on that website, or other websites enabled with such technology.[58]

III. PROTECTIONS IN THE CURRENT STATUTORY SCHEME

A. State Statutes

Currently, no federal law explicitly addresses the collection and storage of faceprints.[59] However, some states have dealt with the issue in their legislatures. A representative example is Illinois.[60] The Illinois law, known as the Biometric Information Privacy Act, cites concerns about the growing use of biometrics, particularly in its metropolitan areas, which corporations use "as pilot testing sites for new applications of biometric-facilitated financial transactions."[61] The statute requires any private entity to develop guidelines for destroying such information after a time not to exceed three years,[62] and requires any private entity that collects or obtains a person's biometric identifier to inform the subject of the fact of the collection, the length of the term for which it is being kept, and its purpose.[63] However, the statute is not perfect. "Biometric identifier," as it relates to faceprints, is defined to include only scans of "face geometry."[64] It is unclear whether its protection will extend to biometric information acquired through

58. *See, e.g.*, Acquisti, *supra* note 53, at 18-23 (using facial recognition technology to link student photographs taken on campus to photographs of those students appearing on Facebook).

59. *See What Facial Recognition Technology Means for Privacy and Civil Liberties*, *supra* note 44, at 3 (statement of Sen. Al Franken, Chairman, Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary) ("Unlike what we have in place for wiretaps and other surveillance devices, there is no law regulating law enforcement use of facial recognition technology.").

60. The states of Texas and Washington have enacted similar laws, codified respectively as TEX. BUS. & COM. CODE ANN. § 503.001 (West 2012) and WASH. REV. CODE. § 46.20.037 (West 2012). Washington's law is limited in subject matter only to drivers' licenses, permits, and identification cards.

61. Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14/5 (2008).

62. *Id.* at 14/15(a).

63. *Id.* at 14/10(b).

64. *Id.* at 14/10.

the use of advanced facial recognition technology, such as algorithms that use the idiosyncrasies of facial texture as an identifier, rather than a set of nodal points. Further, the remedy provided by the statute is a private right of action against the offending party. This is unlikely to lead to much recovery, as it puts the onus to keep track of biometric data usage on the individual, and requires the individual to go through the time and effort of bringing suit for damages capped by statute at just $5000, unless the individual can prove actual damages are greater.[65] Such a low cap may not provide sufficient incentive for an individual to pursue a claim, and it may amount to little more than a slap on the wrist for the offender. Lastly, because it is a state statute, the Biometric Privacy Act's protections are limited to offenses committed within Illinois. The statutes of Texas and Washington also suffer from limitations. The Texas statute caps damages at $25,000 per violation,[66] and the scope of Washington's law is limited to facial recognition systems used for state-issued drivers' licenses and identification cards.[67]

At the federal level, some statutory and constitutional sections are written with sufficient breadth to potentially govern the collection and storage of faceprints. Three frontrunners are the Privacy Act of 1974, the Stored Communications Act, and the Fourth Amendment to the United States Constitution.

B. The Privacy Act of 1974

The Privacy Act of 1974, codified as 5 U.S.C. § 552a, governs collection, maintenance, and storage of records on individuals in the United States. "Record" is defined to include "any item, collection or grouping of information about an individual that is maintained by an agency...and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual."[68] Subsection (d) of the Privacy Act, entitled "Access to records," mandates that the agency must provide an individual with an opportunity to review the record and request amendments.[69] If a government agency maintains a record that includes a person's faceprint, acquired

65. *Id.* at 14/20.
66. TEX. BUS. & COM. CODE ANN. § 503.001(d).
67. WASH. REV. CODE. § 46.20.037(1).
68. Privacy Act of 1974, 5 U.S.C. § 552a(a)(4) (2012).
69. *See id.* at § 552a(d)(1).

without his authorization, this could be a potential channel for individuals to request removal of that information.

However, the courts have interpreted this clause to permit amendment for incorrect information, rather than for unwanted information.[70] Furthermore, subsection (j) lists the exemptions to the statute, which include records "maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals."[71] Since much surveillance can be tied to "police efforts to prevent, control, or reduce crime," this statute is unlikely to provide much protection to individuals unless it is amended to permit removal of unwanted—not simply inaccurate—biometric identifiers.

C. The Stored Communication Act

The Stored Communications Act will offer the strongest protection in the situation in which a faceprint is acquired from a photograph. The Act protects two categories of information: electronic communications services and remote computing services. Thus, users can reap this Act's protection insofar as media containing faceprint data fits into one of these two categories. As stated above, a massive repository of photographs is available online, notably on social networking sites like Facebook. Because these sites have only recently become tools for law enforcement, case law is scarce. However, the federal court in *Crispin v. Christian Audigier* stated that social networking websites—specifically Facebook, MySpace, and Media Temple—are electronic communications services, and thus governed by the Stored Communications Act.[72] The same court also stated that for "messages that have been opened and retained by [plaintiff]...the three entities operate as [remote computing service] providers providing storage services."[73] As discussed below, protection is stronger for providers of electronic communications services—

70. *See, e.g.*, Lee v. Geren, 480 F. Supp. 2d 198, 208 (D.C. Cir. 2007) (denying amendment because "[p]laintiff...is not seeking to correct any true errors in his records.").

71. § 552a(j)(2).

72. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal. 2010) ("Recognizing that all three sites provide private messaging or email services, the court is compelled to apply the voluminous case law cited above that establishes that such services constitute ECS.").

73. *Id.* at 987.

which can only be compelled to disclose by a warrant under § 2703(a) of the Act—than for providers remote communications services, which can be compelled by subpoena under § 2703(b)(1)(B)(i).

The Stored Communications Act[74] penalizes unauthorized access of any "facility through which an electronic communication service" is provided.[75] When it was passed, the statute sought to "update and clarify Federal privacy protections and standards in light of dramatic new changes in computer and telecommunications technologies."[76] Notably, protection under this Act can reach private entities, unlike protection that relies on the Fourth Amendment.[77] For purposes of the Act, an "electronic communication service" includes "any service which provides to users thereof the ability to send or receive wire or electronic communications"[78] with "electronic communication" further defined to mean "any transfer of signs, signals, writing, *images*, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system...."[79] *Crispin* did not address photographs explicitly in its ruling because they were not at issue; the ruling addressed "wall postings and comments."[80] However, the protection afforded to "images" stems from the same definition that offers protection to "writing," so photographs should receive similar protection. By contrast, the definition does not explicitly address videos, which can also be uploaded to Facebook.[81] In the context of drawing faceprints, there is no distinction between a photograph and a well-lit, well-framed video still, so a court may be inclined to afford the same protection to videos as to images. A court may also afford protection to videos by defining videos as electronically transmitted "signals" or "intelligence of any nature."

---

74. Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2012).

75. *See id.* at § 2701(a).

76. S. REP. NO. 99-541, at 1 (1986).

77. 18 U.S.C. § 2707(a) ("[A] person aggrieved by any violation of this chapter...may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.").

78. Wiretap Act § 1, 18 U.S.C. § 2510(15) (2012) (defining terms used in the Stored Communications Act).

79. *See id.* at § 2510(12) (emphasis added).

80. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989-90 (C.D. Cal. 2010).

81. *Uploading & Viewing Videos*, FACEBOOK, https://www.facebook.com/help/video (last visited Mar. 3, 2013).

The *Crispin* court ruled that Facebook is an electronic communications service provider in part because it "provide[s] private messaging or e-mail services."[82] Although the privacy settings for photographs on Facebook can be manipulated independently of the privacy settings for text communications,[83] the options for the two are similar and they can be made equally "private" for purposes of electronic communication. Notably, if it were not possible to restrict viewing access for photographs, the photographs would lose their protection under the Stored Communications Act.[84] However, the fact that user-manipulated privacy settings can hide photographs uploaded to social networks from the public suggests that the disclosure requirements that apply to "electronic communications in electronic storage" under § 2703(a) will be applicable to those hidden photographs. The *Crispin* court also ruled that with respect to messages that have been opened and retained by plaintiff, social networks also act as remote computing service providers.[85] For the purposes of the Stored Communications Act, a remote computing service provider is an entity that provides to the public "computer storage or processing services by means of an electronic communications system."[86] As photographs were not at issue in the case, it is unclear whether this ruling extends to them. Notably, the fact that photographs fall under the protection of the social network in its function as an electronic service provider does not prevent them from also receiving protection as items stored by the social network in its function as a remote computing service.

In addition to the *Crispin* court, at least two other district courts have ruled that a service can be both an electronic communications service and a remote computing service. In *United States v. Weaver*,[87] the court ruled that as soon as an e-mail message was opened, the server that housed that e-mail maintained the message "solely for the purpose of providing storage or computer processing services."[88] As the *Crispin* court affirmed, this

82. *Crispin*, 717 F. Supp. 2d at 980.

83. *Photos Privacy*, FACEBOOK, https://www.facebook.com/help/385017548218624 (last visited Mar. 3, 2013).

84. *See, e.g.*, Snow v. DirecTV, Inc., 450 F.3d 1314, 1320-21 (11th Cir. 2006) ("Congress did not intend to criminalize or create civil liability for acts of individuals who 'intercept' or 'access' communications that are otherwise readily accessible by the general public.").

85. *Crispin*, 717 F. Supp. 2d at 987-88.

86. Stored Communications Act § 11, 18 U.S.C. § 2711(2) (2012).

87. United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009).

88. *Id.* at 772.

is the point at which the e-mail service "ceased to be an [electronic communication service] provider and became a [remote computing service] provider."[89] The crux of the server's status as a remote computing service provider, stated the *Weaver* court, was that the server was now "the only place [the user] stores messages." Similarly, the court in *Flagg v. City of Detroit* found a text message service to be a remote computing service because it was "a 'virtual filing cabinet'" of messages.[90] Although these cases only address text communications, the rationale provided by the court for concluding that the providers were "remote service providers" apply with equal force to the servers that maintain Facebook photographs. Specifically, they are maintained solely to provide storage or computer processing services, like a virtual filing cabinet, or in this case, a virtual photograph album.

The *Weaver* court was clear in its decision that providing e-mail services made a company an electronic communication provider with respect to the messages until they were opened; at that point, the user makes an active decision to leave the messages on the server for storage, and the e-mail service becomes a remote computing service provider.[91] This is a crucial distinction: the messages, though they were protected both by the provider's function as an electronic communication service and its function as a remote computing service, did not receive these protections simultaneously. Until the messages were opened, they received the protection of data transferred through an electronic communications service. Once a user made a conscious decision to leave them on the server for storage, they received the protection of data stored by a remote computing service. In the case of photographs, however, the user's action of uploading the photographs to the site represents an active decision to have the photographs stored on the website, so no triggering event (such as "opening" an e-mail) should be necessary. However, photographs that a user does not upload, but which are electronically tagged to indicate that the user appears in them, are distinguishable. Until a user views these photographs and passively permits the electronic tag to remain[92] or does not request the photographs' removal from

89. *Crispin*, 717 F. Supp. 2d at 985.

90. Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (quoting Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008)).

91. *Weaver*, 636 F. Supp. 2d at 772-73.

92. *See, e.g.*, *How do I Remove a Tag From a Photo or Post I'm Tagged In?*, FACEBOOK, https://www.facebook.com/help/140906109319589 (last visited

the website, they are much like unopened e-mails; the user does not know of their existence or content, and has not implicitly approved of their existence. Under the reasoning of *Weaver* and *Flagg*, social networks would be providing electronic communications services with respect to photographs the social network presence of which a user has not implicitly approved, and a remote computing service with respect to those photographs of which a user has approved. The fact that the statute makes such fine distinctions has been cited as a reason in support of amending the statute to eliminate the distinction between electronic communication service providers and remote computing service providers.[93] Commentators have noted that because the multitude of services offered online so often encompass both categories, the distinction between the two no longer serves any functional purpose.[94] However, until change comes from the legislature, an analysis of the protections offered by the Stored Communications Act must take the distinction into consideration.

While the statute provides fairly strong protection from faceprint gathering for some parties, the protection is somewhat weak for others. In the context of a litigation in which one party seeks another's Facebook data for evidentiary purposes, Federal Rule of Civil Procedure 34 limits a party's ability to withhold discovery documents. The *Flagg* court noted that "a party has an obligation under Rule 34 to produce materials within its control, and this obligation carries with it the attendant duty to take the steps necessary to exercise this control and retrieve the requested documents."[95] However, if a party to a suit attempts to discover information about a third party by way of a subpoena under Federal Rule of Civil Procedure 45, the Stored Communications Act provides some protection. As the *Crispin* court acknowledged, "[a]lthough the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection."[96] As images are protected by the same "electronic communication" language of the Act as e-mails, they too should receive the augmented protection of the Act. The protection

---

Oct. 26, 2013) (like many social networking sites, permitting electronic tags to be removed by the person to whom the tag refers).

93. *See* Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1288 (2012).

94. *Id.*

95. *Flagg*, 252 F.R.D. at 363.

96. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (internal citations omitted).

resulting from this scheme is particularly significant when the subpoenaed third party is the entity that possesses the database on which images are stored, i.e. Facebook itself. A subpoena to an individual user can only reach the photographs that are within his "possession, custody, or control,"[97] which will include the photographs uploaded to the site by that user, and possibly the photographs that have been electronically tagged to indicate that he appears in them. The photographs that are within Facebook's "possession, custody, and control," by contrast, are the hundreds of billions that have been uploaded to the site. In the constraints of civil litigation, it is difficult to imagine a situation in which a party would be able to successfully subpoena the entirety of the Facebook database, as discovery "must be narrowly tailored and cannot be a fishing expedition"[98] and must be "reasonably calculated to lead to the discovery of admissible evidence."[99] However, the protections of the Act go beyond that, compelling disclosure of data held by third parties only in very specific situations.

Although, as the *Crispin* court noted, the Stored Communications Act "creates a set of Fourth Amendment-like privacy protections by statute,"[100] it also provides a set of circumstances under which there is "required disclosure of customer communications or records."[101] These circumstances provide different protections for electronic communications services and remote computing services. Section 2703(a) states:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction.

---

97. Fed. R. Civ. P. 34(a)(1).

98. Groom v. Standard Ins. Co., 492 F. Supp. 2d 1202, 1205 (C.D. Cal. 2007).

99. Fed. R. Civ. P. 26(b)(1).

100. *Crispin*, 717 F. Supp. 2d at 972 (internal quotations omitted).

101. Stored Communications Act § 3, 18 U.S.C. § 2703 (2012).

Under this section, the only way to access a photograph—the existence of which has not been implicitly approved by the party from whom it is being sought—is by way of a warrant. This effectively provides judicial oversight over law enforcement's gathering of faceprints for this category of photographs. However, just as every e-mail must have a receiver and a sender, every photograph in this category must have an uploading user and a tagged user. This section of the statute only protects against compulsory production by the electronically tagged user; the user who uploaded the photograph, as well as the social network itself,[102] is protected by § 2703(b), which relates to remote computing services.[103]

Subsection 1(A) provides the same judicial oversight for remote computing services as § 2703(a) provides for electronic communications service providers.[104] While this may not be as efficient or uncompromising as legislative regulation, this protection will ensure that law enforcement will not be able to subversively collect faceprints without an external check on the legitimacy of the reason for doing so, and the scope of the gathering.

---

102. Any argument that the social networking website does not have the right to disclose such information is dispelled in the case of Facebook by the website's Statement of Rights and Responsibilities:

> For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook.

Statement of Rights and Responsibilities, FACEBOOK (Dec. 11, 2012), https://www.facebook.com/legal/terms.

103. Section 2703(b) provides:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication...
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or
>
> (B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—
>
> (i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
>
> (ii) obtains a court order for such disclosure.

18 U.S.C. § 2703(b).

104. *Id.* at § 2703(b)(1)(A).

Subsection 1(B) provides for more troubling evasions from the protections of the Stored Communications Act. The subsection allows the government to acquire the photographs in question by way of an administrative subpoena or subpoena from the court.[105] Notably, the latter category has been held to exclude civil discovery subpoenas, which significantly narrows its scope.[106] However, the former category gives law enforcement an ever-expanding exclusion from judicial oversight. Administrative subpoenas are issued by administrative agencies and have the power to compel disclosure by private parties of documents to further the agencies' performance of their duties.[107] It would be difficult to enumerate all the situations in which agencies would want to make use of this power—there are roughly 335 federal statutes alone that confer administrative subpoena power on dozens of agencies[108]—but the situations illustrated above in which state law enforcement officers used facial recognition technology in pursuit of locating a suspect could certainly occur in FBI or Drug Enforcement Administration investigations. Without judicial oversight, the scope of these subpoenas and their frequency of use are almost entirely self-monitored. This creates a significant soft spot in the privacy protection offered by the Stored Communications Act. To restore this protection, argues one commentator, § 2703(b)(1)(B)(i) should be struck from the statute in its entirety, leaving courts to decide whether to compel production of documents under § 2703(b)(1)(B)(ii).[109] While this would certainly be a good first step in moderating the dystopian use of facial recognition technology, direct regulation of faceprint collection and use may be warranted.

D. The Fourth Amendment

The Fourth Amendment may protect individuals in situations where their faceprints are drawn from footage caught by surveillance cameras, or in other situations in which individuals

---

105. *Id.* at § 2703(b)(1)(B)(i).

106. *In re* Subpoena Duces Tecum to AOL, L.L.C., 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

107. David Kravets, *We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena*, WIRED MAG. (Aug. 28, 2012), http://www.wired.com/threatlevel/2012/08/administrative-subpoenas/all/.

108. *Id.*

109. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 70 GEO. WASH. L. REV. 1208, 1234-35 (2004).

have a reasonable expectation of privacy. While no court has recognized Fourth Amendment protection of faceprints, the acquisition of faceprints without a warrant may implicate the subjects' Fourth Amendment right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Supreme Court has ruled that other types of biometric data are constitutionally protected. In *Davis v. Mississippi*, defendant Davis was held without a warrant or probable cause during the course of a rape investigation. During this time, the defendant's fingerprints were taken by authorities and matched to a set of fingerprints found at the scene of the crime. The evidence of the match was used at trial, and defendant was convicted of rape. Davis appealed, alleging that the acquisition of the fingerprints was the result of an unreasonable search and seizure.[110] The Supreme Court agreed, stating that fingerprints could not be collected without a warrant. Like possessions taken from a person, fingerprints bear "evidentiary value which the public authorities have caused an arrested person to yield."[111] If a faceprint can be used to confirm or reject suspicions that a particular individual was located near the scene of a crime, it bears similar evidentiary value. However, the *Davis* decision was made in the context of a detention, while faceprint collection requires no detention or even close proximity. Some guidance is provided by *Skinner v. Railway Labor Executives Ass'n*, in which labor organizations challenged the drug testing procedures used by their employers, which included collection of blood and urine.[112] The court found such procedures, without warrant or probable cause, to be in violation of Fourth Amendment protections, citing "concerns about bodily integrity."[113] While such concerns differ from those that arise in the use of facial recognition technology, *Skinner* is indicative of the notion that the Fourth Amendment includes protection against having potential evidentiary material be impermissibly drawn from a person's body. The most significant distinction between claims in the *Davis* and *Skinner* line of cases and a similar claim involving faceprints (instead of fluids or fingerprints) is that faceprint collection does not involve detention, physical contact, or, arguably, an onerous violation of "bodily integrity." In the context of being free from "unreasonable searches

110. Davis v. Mississippi, 394 U.S. 721, 722-23 (1969).

111. *Id.* at 725.

112. Skinner v. Ry. Labor Exec. Ass'n, 489 U.S. 602, 606-07 (1989).

113. *Id.* at 617.

and seizures," this distinction could prove damaging for a Fourth Amendment claim for warrantless faceprint collection.

Another line of cases that could offer some protection relates to privacy concerns. The most recent case in this line is *United States v. Jones*, in which authorities planted a tracking device on the defendant's car.[114] The Supreme Court found that tracking the defendant's public movements through a Global Positioning System unit violated the Fourth Amendment because the placement of the device on the vehicle constituted a seizure.[115] Five justices, in separate concurrences, were concerned about the device's specific use in tracking the vehicle's movements over a prolonged period of time.[116] If a case were to arise in which a person's faceprint was collected and used for tracking purposes, *Jones* may prove to be particularly useful jurisprudence in establishing Fourth Amendment protection of faceprint data.

The government in *Jones* argued that because the defendant willingly exposed his vehicle and its location to the public, he had no "reasonable expectation of privacy in the area accessed by Government agents."[117] The court rejected this theory, noting that it needed to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[118] This protection, the court explained, "was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[119] While the court has not taken on any case in which biometric information was drawn from a person without restraining him, *Jones* supports the assertion that an unauthorized collection of biometric information for the purpose of tracking a person's movements is an unacceptable trespass upon the person. However, in order for such a claim to succeed, courts would have to recognize the existence of a non-physical trespass on the person. The current state of the law is moving toward recognition of such a trespass, but has not yet reached it. In 1974, the Supreme Court rejected certiorari in *United States v. Holland*,[120] in which the lower court decided that the compelled physical examination of

114. United States v. Jones, 132 S. Ct. 945, 948-49 (2012).

115. *Id.* at 952.

116. *Id.* at 955, 963-64.

117. *Id.* at 950.

118. *Id.* (quoting Kyllo v. United States, 553 U.S. 27, 34 (2001)).

119. *Id.*

120. United States v. Holland, 378 F. Supp. 144, 155 (E.D. Pa. 1974), *aff'd sub nom.* United States v. Murphy, 506 F.2d 1053 (3d Cir. 1974), *cert. denied,* 420 U.S. 994 (1975).

the interior of a man's mouth did not constitute a Fourth Amendment violation. Citing Supreme Court precedent,[121] the district court reasoned "the Fourth Amendment does not protect what a person knowingly exposes to the public even in his home or office...[l]ike a man's facial characteristics or handwriting."[122] Twelve years later, however, the Colorado Supreme Court ruled that the inspection of a person's hands under an ultraviolet light violated Fourth Amendment protections, stating that "the reach of the Fourth Amendment...should certainly encompass a detailed inspection, by special instrument, of one's skin."[123] The Supreme Court denied certiorari again, permitting the lower court's ruling to stand. While this progression demonstrates a trend by the courts toward recognizing barely physical trespasses, the court has been unwilling to recognize entirely non-physical trespasses on the person.[124]

However, even if the Court refuses to recognize a trespass upon the person that does not involve physical contact, additional Fourth Amendment protection was recognized in *Katz v. United States*. There, the court abandoned a need for a physical trespass upon a container in order to find a violation of Fourth Amendment rights.[125] In *Katz*, the defendant entered a telephone booth, closed the door, and placed a call in which he implicated himself in illegal gambling. Unbeknownst to him, FBI agents had attached a listening device to the outside of the booth, and had recorded his statements to be used against him at trial.[126] Though the devices did not physically intrude on the area occupied by Katz, and did not make contact with him, the court overruled the prior case law that had required a physical trespass onto a location, and found the warrantless search unreasonable.[127] As the *Jones* court pointed out, recent cases have followed the interpretation by Justice Harlan in

121. United States v. Dionisio, 410 U.S. 1, 14 (1973).

122. *Holland*, 378 F. Supp. at 155 (internal citations omitted).

123. People v. Santistevan, 715 P.2d 792, 795 (Colo. 1986) (quoting United States v. Kenaan, 496 F.2d 181, 182 (1st Cir. 1974)), *cert. denied,* 479 U.S. 965 (1986).

124. *See, e.g.*, Florence v. Bd. of Chosen Freeholders of Burlington, 621 F.3d 296, 311 (3d Cir. 2010) (ruling that a visual strip search of incoming inmates in a prison did not violate Fourth Amendment rights), *aff'd,* 132 S. Ct. 1510, 1522 (2012).

125. Katz v. United States, 389 U.S. 347, 353 (1967).

126. *Id.* at 348.

127. *Id.* at 358.

the *Katz* concurrence,[128] which stated that Fourth Amendment protection exists where there is a "reasonable expectation of privacy" and that "electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment."[129] The *Jones* court made it clear that this protection "has been added to, but not substituted for, the common-law trespassory test."[130] The electronic collection of faceprints via public camera could certainly be embraced as an electronic intrusion, but there is likely to be debate about the absence of a reasonable expectation of privacy. With respect to the reasonable expectation of privacy of photographs stored on online social networks, at least one court has stated that there is none. The New York trial court in *Romano v. Steelcase, Inc.* stated unequivocally that "neither Facebook nor MySpace guarantee complete privacy, [so] Plaintiff has no legitimate reasonable expectation of privacy,"[131] regardless of privacy settings.

Proponents of expanding Fourth Amendment protection to faceprints will point out that although a person willingly exposes his faceprint to the public, there is no way to avoid doing so. Opponents will argue that expanding this protection to cover faceprints unreasonably stretches the bounds of the Fourth Amendment; there should be no protection where there is no expectation of privacy, such as in the case of non-physical intrusions or intrusions to items that people have taken no efforts to protect. As the use of facial recognition technology becomes more prevalent and faceprints gain prominence as a form of biometric identification, these theories are likely to be further tested in court.

IV. A CASE FOR DIRECT REGULATION

In July 2012, Senator Al Franken called on Facebook and the FBI to change the way they use facial recognition technology.[132] He further called for the technology's regulation,

---

128. *See, e.g.*, Bond v. United States, 529 U.S. 334, 337-38 (2000) (reasoning that a bus passenger has a "reasonable expectation of privacy" when he places his carry-on luggage into an overhead compartment, which is violated by probing tactile examination).

129. *Katz*, 389 U.S. at 360.

130. United States v. Jones, 132 S. Ct. 945, 952 (2012).

131. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656 (Sup. Ct. 2010).

132. Grant Gross, *Regulation of Facial Recognition May be Needed, US Senator Says*, COMPUTERWORLD MAG. (July 18, 2012),

citing privacy and civil liberty concerns. Specifically, Franken asked the U.S. Federal Trade Commission "to require private companies to get permission before identifying a person with facial recognition."[133] This is certainly a desirable characteristic of direct regulation, as it would give the subject some control over the use of the deeply personal subject matter of his face. While many interests need to be balanced in creating a regulatory scheme, the elements laid out below would further the goal of clear and efficient regulation of facial recognition technology. Each could be enacted piecemeal as a standalone regulation, or multiple elements could be combined in a comprehensive scheme.

A. Opt-in Consent for Any Formal Collection

Recognizing that some state agencies, such as the DMV, may need to use facial recognition technology to prevent fraud, the practice of using the technology in government functions should not be prohibited entirely. However, due to the uniqueness and permanence of a faceprint, the person forfeiting his faceprint should be fully and affirmatively informed of the consequences of the use of the technology. To that end, people whose photographs are taken by government agencies for identification purposes should not be required to also permit the agency to use their faceprints. If they do choose to submit their faceprints for anti-fraud functions, doing so should be an affirmative act, such as checking an opt-in box on a driver's license application (rather than being required to locate the opt-out box). Some states have a similar system for registering organ donors.[134] Such a system should also account for the concern that opt-in consent could make the database smaller, and therefore less useful in fraud prevention. To mitigate this concern, the task of opting in or remaining opted out should be active, rather than passive, and the permitted use of the faceprint kept as narrow as possible.[135] An ideal solution would permit the agency to ask the subject to submit his faceprint solely

---

http://www.computerworld.com/s/article/9229343/Regulation_of_facial_recognition_may_be_needed_US_senator_says.

133. *Id.*

134. *See, e.g.*, *About Donate Life California*, DONATE LIFE CAL., http://donatelifecalifornia.org/about-us/ (last visited Nov. 13, 2013) (describing opt-in consent for California's organ donor registry via indication on a driver's license application).

135. For example, in the driver's license application scenario, some response should be required on the opt-in box before the application can be considered complete.

for fraud prevention uses and would permit him to decline without any negative consequences. Admittedly, some groups may be reluctant to ever submit their faceprints into such a database, such as individuals who have committed a crime for which they have not been apprehended, or those who plan to commit a crime, and want to avoid getting identified via faceprint. At the very least, a faceprint database could effectively be used to exculpate other suspects who are willing to opt in to the faceprint database, increasing the chances that the actual culprit—even if he is unwilling to opt in to the faceprint database—will be apprehended via process of elimination.

B. Limit Collection and Storage of Faceprints

The circumstances under which collection of faceprints is permitted should be limited to mitigate the risk that the database could be used for improper purposes. For example, when an identifying biometric already exists on record (e.g. fingerprint, iris scan, etc.) it may be unnecessary to collect a faceprint as well. Only when a faceprint is the sole biometric identifier by which the stated goal can be achieved should collection be permitted. Further, use of biometrics for any goal beyond the narrow purpose for which it was collected should be categorically prohibited.

The sources from which a faceprint can be collected could be restricted. In most cases, faceprints should be collected directly from the individual, and collection from social networks, government agencies, or other third parties should be treated with extreme skepticism. Third-party collection is a potential indicator that the faceprint was not submitted willingly to the government by the subject. Therefore, such submission should only be permitted in very limited circumstances, such as when there is probable cause to believe the subject committed a violent felony, and use of his faceprint can confirm or disprove an alibi. Collection without detention, such as collection of a faceprint from a crowd photograph, is a similarly strong indicator that the subject did not agree to forfeit his faceprint and should be treated with equal skepticism.

Further, each faceprint should have an established "shelf life"—a length of time for which it may be kept. This length could be defined by the purpose of the faceprint, and require that the faceprint must be destroyed when the task for which it was acquired is complete. This would likely be a weak standalone remedy, since photo databases—especially in the public context—are often used for long-term goals such as crime prevention, and

any limitation on storage time would frustrate the purpose of using of the faceprint, or be meaninglessly lengthy. However, as part of a multifaceted strategy, a temporal limitation could provide protection that reflects the concern that one's faceprint cannot be changed. A person would not have to worry about an unchangeable and deeply individual piece of his or her identity being kept by the government for an extended period of time. Such a provision would require statement of a specific initiative at the time of acquisition, and immediate termination of a person's faceprint if it becomes likely that retention will result in physical harm or violation of an established constitutional right.

C. Create Oversight and Effective Right of Action

The consequences of a mistaken disclosure or security breach with respect to faceprint data are significant; once the disclosure has been made, the damage cannot be undone, as a faceprint cannot be changed. To ensure that faceprints do not fall into undesirable hands, and to ensure that faceprint collection and storage protocols are being followed, an independent overseeing body should be created, either in the form of a congressional committee or a federal agency. Such an overseer would propound standards of conduct describing the situations in which collection of biometric information by law enforcement should be permitted, would establish standards for transfer and disposal of biometric data, and would dissuade eager law enforcement bodies from bending the regulations for their purposes. For example, an overseeing body could monitor government agencies that have been granted access to a faceprint database for a specific purpose to ensure that the agency does not exceed the bounds of its granted authority (e.g. by using a faceprint database to track a suspect's movements when it was only given permission to use the database for identification purposes).

To complement the overseeing body, the regulation should grant a right of action to the subject of the faceprint, for both money damages and equitable relief, to remedy improper use or disclosure of faceprint data. The Illinois Biometric Privacy Act, mentioned above, could function as a template for such a provision. That statute provides a right of action to aggrieved parties by which they can recover either liquidated or actual damages, attorneys' fees, litigation fees, and "other relief, including an injunction, as the State or federal court may deem

appropriate."[136]

D. Acknowledge Quasi-Property Rights

To directly confront the risk that faceprints could be collected without the knowledge of the subject, a statute could require the subject to be notified every time his faceprint is collected in connection with his identity. Such a notification would include the following: 1) an alert that the faceprint has been collected, 2) a statement describing the use for which it has been collected and the length of storage, and 3) directions to request its removal from the database.

In the public use context, a faceprint could remain in use if it serves a narrowly tailored, compelling government purpose. In the private sector context, a person would have an absolute right to be removed from unwanted databases. However, this proposal has high transaction costs. If organizations are collecting faceprints *en masse*, or not directly from the subject, it may not always be clear how to contact the subject. Due to the permanent and sensitive nature of the faceprint, a harsh version of the regulation would state that failure to contact the subject means the faceprint must be removed from the database. A more reasonable statute may require only the organization's "best efforts" to contact the subject.

V. CONCLUSION

Although the use of surveillance and facial recognition technology continues to rise, the collection, storage, and exchange of faceprints remains unregulated. It is possible to find some protection against the unfettered collection of faceprints in the existing law, notably the Fourth Amendment and Stored Communications Act. However, a statute that directly addresses the concerns regarding the use of biometric information in law enforcement would represent a great improvement over the uncertain and piecemeal existing protections.

136. 740 ILL. COMP. STAT. 14/20 (2008).