Digital Commons @ LMU and LLS

Loyola Marymount University and Loyola Law School
Digital Commons at Loyola Marymount University and Loyola Law School

Loyola of Los Angeles Entertainment Law Review

Law Reviews

3-1-2012

Facebook or Face Bank?

Carmen Aguado
Loyola Law School Los Angeles

Recommended Citation

Carmen Aguado, *Facebook or Face Bank?*, 32 Loy. L.A. Ent. L. Rev. 187 (2012).
Available at: http://digitalcommons.lmu.edu/elr/vol32/iss2/2

FACEBOOK OR FACE BANK?

*Carmen Aguado**

On June 7, 2011, social media giant Facebook Inc. debuted its facial recognition tool to all of its users. The facial recognition tool has the capability of identifying individuals automatically in photographs uploaded to Facebook by its users. Soon thereafter, the facial recognition tool prompted privacy concerns and ultimately led to a complaint being filed with the Federal Trade Commission. While at first denying its use of facial recognition technology, Facebook eventually admitted to its use of the technology. However, Facebook failed to acknowledge that it collected and stored the biometric data—data that is considered highly sensitive—of all of its users without their consent. Accordingly, Facebook violated the privacy rights of its users when it covertly collected and stored the data. Although it may be possible for users to bring a private action against Facebook for privacy violations, they would, nevertheless, be confronted with a tremendous roadblock—the issue of standing. Without the ability to legally protect their data, Facebook users are left with little recourse. Accordingly, the United States Government and courts must heighten privacy protections of personalized information, such as biometric data, to prevent companies like Facebook from usurping highly sensitive personalized data of their users.

* J.D. Candidate, Loyola Law School, 2013; B.A., Loyola Marymount University, 2007. The author would like to thank her loving family (Rodolfo Jr., Jacqueline, Cynthia, Rodolfo III, and Ava) for their support, encouragement, and laughter throughout the author's life and for the always enlightening Sunday night dinners. The author would also like to thank "Amigo" for burning the midnight oil with her while completing this article and Loyola Law School Professor Karl Manheim for his expertise, suggestions, and assistance in editing this article when it was merely an outline. Finally, the author would like to give a tremendous thanks to Note and Comment Editor John Toton, whose enthusiasm encouraged her to pursue the topic, and to the editors and staffers of the *Loyola of Los Angeles Entertainment Law Review* for their efforts and help in making this publication possible.

I. INTRODUCTION

In early June of 2011, Facebook unveiled a new feature called "tag suggestions" to all of its users.[1] Tag suggestions activate when a user uploads a picture to his or her Facebook page.[2] Immediately, Facebook's facial recognition software identifies the people in the photographs.[3] Facebook states that the facial recognition tool "speed[s] up the process of identifying and labeling people in photos."[4] However, the strength of Facebook's facial recognition technology relies on the depth of its facial recognition database.[5] The database is comprised of Facebook users that have previously been tagged in photographs, many of whom were unaware that Facebook was storing their unique facial features.[6] This process may sound harmless at first—Facebook is simply making it easier to tag pictures. However, when users learn how facial recognition technology works, the "convenience" of this technology may make many feel uneasy because it arguably constitutes an invasion of privacy.

[1] *See* Justin Mitchell, *Making Photo Tagging Easier*, FACEBOOK BLOG (June 30, 2011, 5:16 PM), https://www.facebook.com/blog.php?post=467145887130 [hereinafter Mitchell I].

[2] *See* Justin Mitchell, *Making Photo Tagging Easier*, FACEBOOK BLOG (Dec. 15, 2010), http://www.facebook.com/blog/blog.php?post=467145887130 [hereinafter Mitchell II] ("When [users] upload new photos, [Facebook] use[s] face recognition software . . . to match . . . new photos to other photos you're tagged in. [Facebook] group[s] similar photos together and, whenever possible, suggest[s] the name of the friend in the photos."); *see also* Sarah Jacobsson Purewal, *Why Facebook's Facial Recognition is Creepy*, PCWORLD (June 8, 2011), http://www.pcworld.com/article/229742/why_facebooks_facial_recognition_is_creepy.html ("Basically, Facebook is using facial recognition technology to 'suggest' tags to users who upload photos.").

[3] *See* Mitchell II, *supra* note 2 ("When [users] upload new photos, [Facebook] use[s] face recognition software . . . to match [] new photos to other photos you're tagged in. [Facebook] group[s] similar photos together and, whenever possible, suggest[s] the name of the friend in the photos.").

[4] *See* Alexei Oreskovic & Georgina Prodhan, *Facebook Gives Regulators Info on Facial Recognition*, REUTERS (June 8, 2011), http://www.reuters.com/article/2011/06/08/facebook-idUSN0826171920110608.

[5] *See* Declan McCullagh, *Face-matching with Facebook Profiles: How It Was Done*, CNET NEWS (Aug. 4, 2011), http://news.cnet.com/8301-31921_3-20088456-281/face-matching-with-facebook-profiles-how-it-was-done/#ixzz1n3uRVy17 (stating that Facebook has a "vast database" of "wide-open profile photos"); *see also* Purewal, *supra* note 2 (explaining that Facebook's facial recognition technology "learns" more about a what a person looks each time they are identified in a photo and, further, that the information is stored in a facial recognition database). *See generally General Info*, FACE RECOGNITION HOMEPAGE, http://www.face-rec.org/general-info/ (last visited Apr. 15, 2012) (explaining that facial recognition works by comparing a still image to a stored database of faces).

[6] *See* Mark Milian, *Facebook Lets Users Opt Out of Facial Recognition*, CNN TECH (June 7, 2011), http://articles.cnn.com/2011-06-07/tech/facebook.facial.recognition_1_facebook-ceo-mark-zuckerberg-facial-recognition-face-recognition?_s=PM.

This invasion of privacy has unnerved many in the industry.[7] Eric Schmidt, former Google CEO, saw no privacy concern in 2010 when he said, "[Google doesn't] need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."[8] Schmidt, however, does find facial recognition technology to be problematic.[9] He stated that Google would not use facial recognition technology because its accuracy was "very concerning" and it was "too creepy."[10]

Schmidt's concerns are not without merit. The ways in which the information generated by the technology can be used makes the facial recognition software bothersome. For example, someone could casually snap a photo of an unsuspecting stranger and then match that stranger to his or her online identity within minutes using a computer application that integrates facial recognition technology with data accessible on the Internet.[11] Facebook's user profile pictures,[12] which are now public by default,[13] and other accessible data on Facebook, could facilitate this process.[14] With the images that are available online, including every Facebook user's profile picture, technologically savvy individuals can potentially match a face with a

[7] *See, e.g.*, Daily Mail Reporter, *"Too Creepy Even for Google": Search Engine Boss Warns Government Against Facial Recognition Technology*, MAIL ONLINE (May 20, 2011), http://www.dailymail.co.uk/sciencetech/article-1388855/Google-CEO-Eric-Schmidt-warns-governments-facial-recognition-technology.html#ixzz1bYgc8E6f (explaining that Schmidt believes the use of facial recognition technology by organizations crosses the proverbial line and can amount to an invasion of privacy).

[8] Derek Thompson, *Google's CEO: "The Laws Are Written by Lobbyists"*, ATLANTIC (Oct. 1, 2010), http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/.

[9] *See* Daily Mail Reporter, *supra* note 7 (explaining that Schmidt believes the use of facial recognition technology by organizations crosses the proverbial line and can amount to an invasion of privacy).

[10] *See id.*

[11] *See* Jared Keller, *Cloud-Powered Facial Recognition Is Terrifying*, ATLANTIC (Sept. 29, 2011), http://www.theatlantic.com/technology/archive/2011/09/cloud-powered-facial-recognition-is-terrifying/245867/ ("With Carnegie Mellon's cloud-centric new mobile app, the process of matching a casual snapshot with a person's online identity takes less than a minute.").

[12] *Profile*, FACEBOOK, https://www.facebook.com/about/profile/ (last visited Apr. 15, 2012) ("Your [Facebook] profile begins with a quick summary of who you are, giving friends an easy way to see where you live now, where you're working and more."); *see also Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last visited Apr. 15, 2012) (stating that a profile picture is to "help[] your friends and family recognize you" and is always publicly available).

[13] *See Basic Privacy Controls*, FACEBOOK, http://www.facebook.com/help/?page=132569486817869 (last visited Apr. 16, 2012) (explaining your Facebook profile picture is made visible to everyone, including individuals not on Facebook).

[14] *See* Keller, *supra* note 11.

Social Security number.[15] Three days after Facebook launched tag suggestions, the Electronic Privacy Information Center ("EPIC") filed a Complaint, Request for Investigation, Injunction, and Other Relief ("EPIC Complaint") with the Federal Trade Commission ("FTC"), urging the FTC to investigate Facebook's new automated tagging feature.[16] The complaint alleges, *inter alia*, that: (1) Facebook is involved in "unfair and deceptive acts and practices" by its continued use of the automatic tagging feature; (2) Facebook's implementation of the facial recognition technology is an invasion of privacy, which not only causes harm to consumers, but is done without their consent; and (3) Facebook's collection of biometric data from children is contrary to the Children's Online Privacy Protection Act of 1988.[17] Additionally, the EPIC complaint requests that the FTC require Facebook to:

1. Immediately suspend Facebook-initiated tagging or identification of users based on Facebook's database of facial images;
2. Not misrepresent how it "maintains and protects the security, privacy, confidentiality, and integrity of any consumer information";
3. Provide additional disclosures to users prior to new or additional sharing of information with third parties; and
4. Establish, implement, and maintain a comprehensive privacy program.[18]

The EPIC Complaint focuses on Facebook's business practices[19] because the FTC is equipped to pursue such violations under section 5(a) of

[15] *See id.*; *see also More than Facial Recognition*, CARNEGIE MELLON UNIV., http://www.cmu.edu/homepage/society/2011/summer/facial-recognition.shtml (last visited Apr. 15, 2012) (explaining how researchers were able to use facial recognition technology to predict personal interest and in a few instances Social Security numbers).

[16] *See* Complaint, Request for Investigation, Injunction, and Other Relief, *In re* Facebook, Inc. and the Facial Identification of Users (2011) (on file with FTC), *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

[17] *See generally id.*

[18] *Id.* at 24, 33–34.

[19] The FTC settled the complaint with Facebook in November of 2011. *See* Press Release, FTC, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 11, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm. However, the November 2011 settlement between the FTC and Facebook does not mention the facial recognition tool or Facebook's acquisition of biometric data. *See* Agreement Containing Consent Order, *In re* Facebook, Inc. (No. 092-3183), *available at* http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf. The settlement does not apply retroactively, thus the data that has already been obtained without consent can remain in Facebook's database. *See id.* How-

the FTC Act.[20] However, a private party should also be able to file a complaint against Facebook for constitutional privacy violations and privacy tort violations.

This Comment will explain the sensitive nature of biometric data and the reasons that it should be awarded greater legal protections. Part II of this Comment will (1) provide a brief overview of the history of facial recognition technology, (2) describe the sequence of events leading to Facebook's implementation of its facial recognition technology, and (3) address reasons why Facebook users should be concerned about this new technology. Part III explains the violations Facebook has committed in illegally obtaining its users' biometric data.[21] Part IV will discuss the two primary issues that a private party might face when filing a suit, notwithstanding the applicability of various privacy laws. Finally, Part V of this Comment will provide suggestions on steps that the United States Government and courts should take to ensure that private information, such as biometrics, receives greater protections.

II. THE ORIGINS OF BIOMETRIC DATA

Biometric data use has grown substantially since the 1960s.[22] In the 1960s, facial recognition technology became semi-automated, whereby a

ever, the settlement requires Facebook to create a "comprehensive privacy program" that is designed to address privacy risks related to the facial recognition tool. *See id.* at 5 ("It is further ordered that Respondent shall . . . establish . . . a comprehensive privacy program . . . to (1) address privacy risks related to the development and management of new and *existing* products and services for consumers." (emphasis added)). The privacy program is to be designed by Facebook employees and gives the *employees* the responsibility of identifying the issues. *See id.* Thus, the great responsibility of rectifying the privacy issues related to Facebook's taking of biometric data falls on the shoulders of Facebook.

[20] *See A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC, http://www.ftc.gov/ogc/brfovrvw.shtm (last visited Apr. 15, 2012) ("The basic consumer protection statute enforced by the [FTC] is Section 5(a) of the FTC Act, which provides that 'unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful.'" (emphasis omitted) (citation omitted)).

[21] The violations discussed in Part III are not exclusive. For example, Facebook could also be found in violation of the Electronic Communications Privacy Act, which protects individuals from interception and monitoring of their electronic communications. *See generally* Electronic Communications Privacy Act, 18 U.S.C. § 2511(2)(a)(i) (2011). Because e-mail and data stored electronically are covered by this definition, monitoring of such communications is generally prohibited. *Id.* Facebook violates the Act because it has intentionally intercepted electronic data by taking their users' biometric data from photographs without consent.

[22] *See generally* NSTC Subcomm. on Biometrics, *Biometrics History*, BIOMETRICS.GOV, 8, 13 (2006), http://www.biometrics.gov/documents/biohistory.pdf (explaining that in the 1960s facial recognition was semi-automated, whereas, by the 1990s, the technology advanced to become fully-automated).

system administrator had to locate key features in the photographs.[23] Once the key features were manually identified, the system would calculate the distances from the key facial features and automatically compare the image to the reference data.[24] Law enforcement agencies began to use the semi-automated technology by the 1980s.[25] This was illustrated in 1988, when the Lakewood Division of the Los Angeles County Sheriff's Department used images of suspects captured in surveillance tapes and compared those images against its database of mug shots to find matches.[26] Semi-automated facial recognition was only the beginning of facial recognition technology. By the late 1980s and early 1990s, facial recognition technology became fully-automated with "eigenface technology," which allowed for real-time face recognition.[27] Simply stated, with fully-automated real-time facial recognition, an image of one's face can be automatically recognized and matched to other images in a database, without a system administrator manually locating the key features.[28]

After the September 11, 2001 terrorist attack on the United States, the federal government paid "significantly enhanced attention" to biometric technologies.[29] By 2009, there were more than thirty publicly available databases for facial recognition analysis.[30] Today, applications such as Google's Picasa, Apple iPhoto, Sony's Picture Motion Browser, Windows Live Photo Gallery, and Facebook, all use facial recognition technology.[31] However, Facebook, unlike the other companies, impinged on the privacy rights of its users by *covertly* accumulating its robust database of biometric data.[32] The potentially exploitative nature of personal biometric data suggests that keeping this information private is extremely important.

[23] *Id.* at 8.

[24] *Id.*

[25] *See id.* at 13 (stating the Lakewood Division of the Los Angeles County Sheriff's Department began using a semi-automated facial recognition system).

[26] *Id.* at 13.

[27] *Id.*

[28] *See* Matthew A. Turk & Alex P. Pentland, *Face Recognition Using Eigenfaces*, BLAVATNIK SCH. COMPUTER SCI. – TEL AVIV UNIV., http://www.cs.tau.ac.il/~shekler/Seminar2007a/PCA%20and%20Eigenfaces/eigenfaces_cvpr.pdf (last visited Apr. 15, 2012).

[29] *See* NSTC Subcomm. on Biometrics, *BIOMETRICS in Government POST-9/11: Advancing Science, Enhancing Operation*, OFF. SCI. & TECH. POL'Y 13 (2008), *available at* http://www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf.

[30] *See id.*

[31] *See* Emily Shultz, Comment to *Activate Face Recognition Log On in Laptop*, TECHYV.COM (Sept. 4, 2011), http://www.techyv.com/questions/activate-face-recognition-log-laptop.

[32] *See* Tharun Venkatesan, *Google Plus Facial Recognition: Find My Face*, TECHNOSTREAK.COM (Dec. 10, 2011), http://technostreak.com/web/social/google-plus/google-

A. A Glimpse into Facial Recognition Technology and Its Significance

Biometric data consists of "measurable . . . distinctive physical characteristic[s] or personal trait[s] that can be used to identify an individual."[33] For example, facial recognition software initially locates distinctive features on the face and the measurements of the facial features, such as the distance between eyes or width of nose.[34] These measurements are compiled to create an algorithm or biometric template of a person's face.[35] Facial recognition software then stores the template of the facial image in a database and compares the template to other stored images.[36] Advancements in facial recognition technology have allowed for individuals and private companies like Facebook to scan an image of a face and correlate the image to a Facebook user's profile.[37]

The biometric data fueling facial recognition technology is highly personal, individualized information, such that the data could eventually be used to link a stranger on the street to his or her credit score.[38] It employs unique identifiers such as fingerprints.[39] Because of the importance and private nature of this data and the accelerated advancements in biometric technology, the National Science and Technology Council ("NSTC"), a Cabinet-level Council,[40] established a subcommittee to specifically re-

plus-facial-recognition-find-my-face/ (explaining that Google Plus also uses facial recognition technology, but unlike Facebook, Google Plus allows users to opt in or out).

[33] John D. Woodward, Jr., Christopher Horn, Julius Gatune & Aryn Thomas, *Biometrics: A Look at Facial Recognition*, RAND, 2003, at 1, *available at* http://www.rand.org/content/dam/rand/pubs/documented_briefings/2005/DB396.pdf.

[34] *See* Kevin Bonsor & Ryan Johnson, *How Does Facial Recognition Work?*, GLOBE & MAIL (Jul. 25, 2011), http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition1.htm/.

[35] *See* Bryan Gardiner, *Engineers Test Highly Accurate Face Recognition*, WIRED (Mar. 24, 2008), http://www.wired.com/science/discoveries/news/2008/03/new_face_recognition.

[36] *See id.*

[37] *See* McCullagh, *supra* note 5.

[38] *See generally* NSTC Subcomm. on Biometrics, *Biometrics Frequently Asked Questions*, BIOMETRICS.GOV, 21 (2006), http://www.biometrics.gov/Documents/FAQ.pdf; s*ee also* Natasha Singer, *Face Recognition Makes the Leap From Sci-Fi*, N.Y. TIMES (Nov. 12, 2011), http://www.nytimes.com/2011/11/13/business/face-recognition-moves-from-sci-fi-to-social-media.html (quoting researchers explaining how facial recognition software can be used by marketers to infer personal information about random individuals on the street).

[39] *See For Unique ID, Photo No Alternative to Fingerprint*, DECCAN HERALD (Jan. 25), http://www.deccanherald.com/content/48769/for-unique-id-photo-no.html (explaining that although fingerprints were found more accurate than facial recognition technology, at that time, both use biometric data that is personalized).

[40] *See About NSTC*, OFFICE SCI. & TECH. POL'Y, http://www.whitehouse.gov/administration/eop/ostp/nstc/about (last visited Apr. 15, 2012).

search biometric technology in 2003.[41] While the NSTC primarily serves as a medium for government agencies and the public to access information concerning the Government's use of technology in general,[42] the subcommittee on Biometrics and Identity Management ("BIM") assists in coordinating development in federal biometrics.[43]

By 2006, recognizing the public concern surrounding biometrics, the sensitivity of the information obtained, and highly personal nature of the data collected, BIM urged companies to use privacy assessments whenever the use of biometric information is employed.[44] BIM's concern in protecting the data stems from the ability of biometrics to detect human emotions[45] and its potential to identify an individual's ethnicity—information that is generally regarded as private.[46] Accordingly, the U.S. government considers biometric data to be "*sensitive* personal information"[47] and believes that standards and regulations should be followed in *any* implementation of technology that uses biometric data.[48]

Appreciating the sensitive nature of biometrics, the U.S. government classifies biometric data as Personally Identifiable Information ("PII").[49] PII is any information that can be used to trace an individual's identity,[50]

[41] *See NSTC Subcommittee on Biometrics and Identity Management Room*, BIOMETRICS.GOV, http://www.biometrics.gov/nstc/default.aspx (last visited Apr. 15, 2012).

[42] *See About NSTC*, *supra* note 40.

[43] *See NSTC Subcommittee on Biometrics and Identity Management Room*, *supra* note 41 (explaining the purpose and objectives of BIM).

[44] *See* PETER E. SAND ET AL., NSTC SUBCOMM. ON BIOMETRICS, PRIVACY & BIOMETRICS: BUILDING A CONCEPTUAL FOUNDATION 35 (2006), *available at* http://www.biometrics.gov/docs/privacy.pdf (explaining how the Government should apply privacy to biometric technology).

[45] *See* Daniel Shemesh, *Face Recognition Software Could Detect Pain in Patients*, PIPE DREAM (May 6, 2011), http://www2.bupipedream.com/news/face-recognition-software-could-detect-pain-in-patients-1.2223624#.Tp6PSt5 (noting that facial recognition technology can potentially detect pain in patients); *see also* Omri Ceren, *Creepy Airport Facial Recognition Automatically Detects Lying*, JAUNTED (Sept. 7, 2011), http://www.jaunted.com/story/2011/9/7/134855/2920/travel/creepy+airport+facial+recognition+automatically+detects+lying (noting facial recognition in airports can detect lying).

[46] *See* NSTC Subcomm. on Biometrics, *supra* note 38, at 4.

[47] *Id.* at 21 (emphasis added).

[48] *Id.* at 14.

[49] *See Biometrics & Personally Identifiable Information: Assessing the Impact of U.S. Policy and Laws on the Use of Biometrics by Government Agencies and Evaluating Solutions to Meet Government Operational Requirements*, NAT'L BIOMETRIC SECURITY PROJECT, 9, 13 (2010), *available at* http://www.nationalbiometric.org/downloads/biometrics-and-privacy-report-final-2011-02-22.pdf (defining biometrics as personally identifiable information and discussing the privacy issues that arise from biometrics being classified as PII).

[50] *Protection of Personally Identifiable Information (PII)*, NARA 1608, 3 (Aug. 6, 2009), http://www.archives.gov/foia/directives/nara1608.pdf.

and, often, Congress enacts legislation to protect PII.[51] For example, in 2006, Congress enacted 18 U.S.C. section 1028, which criminalizes the use of identification documents to steal one's identity.[52] The statute gives biometric data, the information used in facial recognition technology, the same weight as a Social Security number, a government-issued driver's license, or an identification number.[53] However, despite the recognition that biometric data is as personal and as important to protect as Social Security numbers, it has yet to receive the same level of attention from legislators and protection on the Internet.[54]

Because biometric data is sensitive and is classified as PII,[55] Facebook should have given its users' privacy greater deference prior to collecting their biometric data. Due to this lack of attention and its surreptitious collection of the data, Facebook is in violation of several privacy laws.

B. A Snapshot of Facebook's Use of Facial Recognition Technology

Facebook has become the largest social networking website, boasting approximately 800 million users worldwide.[56] It is the second most-trafficked site[57] in the world and brands itself as a company that "facilitate[s] the sharing of information through the social graph."[58] Over 400 mil-

[51] Peter Gray, *Protecting Privacy and Security of Personal Information in the Global Electronic Marketplace*, *available at* http://www.ftc.gov/bcp/icpw/comments/ico2.htm (explaining how Congressmen have proposed online privacy bills to protect personally identifiable information).

[52] *See* 18 U.S.C. § 1028(a)(1)–(8) (2006).

[53] *See id.* § 1028(d)(7)(A)–(D) (listing biometric data as a means of identification in conjunction with name and Social Security number).

[54] The need to protect Social Security numbers has generated widespread attention from government agencies. *See* Soc. Sec. Admin., *Identity Theft and Your Social Security Number*, SSA Pub. No. 05-10064 (2009), *available at* www.ssa.gov/pubs/10064.html (providing information on the importance of protecting your Social Security number and how to prevent identity theft); *see also* CAL. CIV. CODE § 1798.85(a)(3)–(4) (prohibiting businesses and non-government entities from displaying Social Security numbers over the Internet, unless the connection is secure); S. 1691, 110th Cong. §§ 1–3 (2007) (proposing the restriction of the use and display of Social Security numbers to prevent identity theft and fraud. The proposed bill has been reintroduced several times, but has not yet passed). The actions taken to protect Social Security numbers, at the state and federal level, as described, display the government's support in protecting Social Security numbers and further, its acknowledged importance of the information.

[55] *See Biometrics & Personally Identifiable Information: Assessing the Impact of U.S. Policy and Laws on the Use of Biometrics by Government Agencies and Evaluating Solutions to Meet Government Operational Requirements*, *supra* note 49 (explaining that biometric information is PII).

[56] *See Newsroom*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited Apr. 15, 2012).

[57] *Top Sites*, ALEXA.COM, http://www.alexa.com/topsites (last visited Apr. 15, 2012).

[58] *Peering*, FACEBOOK, http://www.facebook.com/peering/ (last visited Apr. 15, 2012).

lion of Facebook's users log in to their Facebook accounts daily,[59] 250 million photos are uploaded onto Facebook every twenty-four hours,[60] and more than 7 million applications and websites are integrated with Facebook.[61] Facebook's privacy policy,[62] monitored by TRUSTe,[63] assures the information that users share through their Facebook profile is safeguarded.[64]

Facebook's privacy policy is broken into several categories.[65] It covers the type of information Facebook receives about users, the information that can be accessed by users with their username or user identification, the information made public (that which can be viewed by anyone, including people who are not on Facebook), and the way that Facebook uses the information it collects.[66] Facebook's privacy policy states that Facebook receives and stores metadata from a user's computer, such as the time, place, and date of photo uploads.[67] However, the policy fails to mention that users' biometric data is stored as well.[68]

Facebook's *The Facebook Blog* chronicled Facebook's increasingly advanced use of facial recognition technology.[69] The first mention of the enhanced tagging features was in July of 2010 when Facebook blogged, "With this new feature, tagging is faster since you don't need to select a

[59] *See Newsroom*, *supra* note 56.

[60] Ben Parr, *Facebook by the Numbers [INFOGRAPHIC]*, MASHABLE SOC. MEDIA (Oct. 21, 2011), http://mashable.com/2011/10/21/facebook-infographic/.

[61] Derrick Harris, *Facebook Shares Some Secrets on Making MySQL Scale*, GIGAOM (Dec. 6, 2011), http://gigaom.com/cloud/facebook-shares-some-secrets-on-making-mysql-scale/; *see also* Kate Freeman, *Facebook Apps: Highlights of the 60 New Integrated Applications*, MASHABLE SOC. MEDIA (Jan. 22, 2012), http://mashable.com/2012/01/22/facebook-apps/ (explaining how applications integrated with Facebook allow Facebook users to share their activity on the application with their Facebook friends).

[62] *See Data Use Policy*, *supra* note 12.

[63] *See* TRUSTE, http://www.truste.com/about_TRUSTe/ (last visited Apr. 15, 2012) (stating that TRUSTe is a third-party company that monitors private companies to ensure compliance with the companies' stated privacy policy).

[64] *See Newsroom*, *supra* note 56.

[65] *See generally Data Use Policy*, *supra* note 12.

[66] *See id.*

[67] *See id.*

[68] *See id.*

[69] *See* FACEBOOK BLOG, http://blog.facebook.com/ (last visited Apr. 15, 2012) (providing a forum where Facebook employees give updates regarding new Facebook tools and features. To access THE FACEBOOK BLOG, users have to navigate their way through the Facebook "About" section, then to the "Info" section, and then click on the hyperlink that connects to the blog. THE FACEBOOK BLOG then opens in a new window. Users unaware of the blog had no notice of the changes Facebook was implementing.).

face. It's already selected for you, just like those rectangles you see around your friends' faces when you take a photo with a modern digital camera."[70]

Facebook subsequently acquired Divvyshot, a photo-sharing site.[71] In September 2010, Sam Odio, Facebook's Photo Products Manager, explained the technology behind the bulk tagging features Facebook began to use:

> This isn't face recognition. . . . Picasa and iPhoto—they'll detect a face and say, "This is Sam," and they'll suggest that it's Sam. We're not doing that. We're not linking any faces to profiles automatically. Right now, we want to stay away from that because it's a very touchy subject.[72]

However, this statement was inaccurate. Picasa and iPhoto use facial recognition data in a *similar* fashion to Facebook.[73] As a matter of fact, the only difference between Picasa, iPhoto, and Facebook is that Facebook uses a different facial recognition software company.[74] By December of 2010, Facebook reported to its users that the website would begin using "tag suggestions,"[75] and that the tool would be implemented in the United States starting in December 2010 and continue through January 2011.[76] Facebook further explained:

> When you or a friend upload new photos, we use face recognition software—similar to that found in many photo editing tools—to match your new photos to other photos you're tagged

[70] Sam Odio, *Making Facebook Photos Better*, FACEBOOK BLOG (July 1, 2010, 5:37 PM), http://blog.facebook.com/blog.php?post=403838582130.

[71] *See* Erick Schonfeld, *Facebook Buys Up Divvyshot To Make Facebook Photos Even Better*, TECHCRUNCH (Apr. 2, 2010), http://techcrunch.com/2010/04/02/facebook-buys-up-divvyshot-to-make-facebook-photos-even-better/ (stating Facebook purchased Divvyshot, a group photograph-sharing site).

[72] *See* Caroline McCarthy, *Facebook Photos Get High Resolution, Bulk Tagging*, CNET NEWS (Sept. 30, 2010), http://news.cnet.com/8301-13577_3-20018211-36.html.

[73] *Compare* Josh Lowensohn, *Facial Recognition Face-Off: Three Tools Compared*, CNET NEWS (Sept. 30, 2009), http://news.cnet.com/8301-27076_3-10363727-248.html (comparing the facial recognition software that iPhoto and Picasa use and how the software is able to automatically recognize individuals in the photographs), *with* Purewal, *supra* note 2 (stating Facebook is using facial recognition software that has the ability to recognize individuals in photographs posted on Facebook) (emphasis added).

[74] *See* Lowensohn, *supra* note 73 (explaining how the facial recognition software works).

[75] *See* Mitchell II, *supra* note 2.

[76] *See id.*

> in. We group similar photos together and, whenever possible, suggest the name of the friend in the photos.[77]

This announcement marked the first time Facebook confirmed it was using facial recognition software.[78]

Although Odio stated that Facebook was not using facial recognition technology,[79] less than a year later, Facebook's Engineering Manager, Justin Mitchell, admitted Facebook was essentially actively using facial recognition technology with its tag suggestion software.[80] The immediate availability of tag suggestions inevitably meant that Facebook had been collecting its users' biometric data before the 2011 release of the tag suggestion tool, otherwise Facebook would not have been able to make the new technology instantly available to its users. Facebook soon thereafter admitted it had misled users regarding its use of facial recognition software.[81]

However, Facebook and its blog entries do not explain how the tag suggestions tool actually functions.[82] For instance, the blog states that the tag suggestion tool is a default setting for all users,[83] but there is no disclosure that Facebook collects the data necessary to run the tool without user consent.[84] Facebook users are only given the option to turn off the automatic tagging feature and have their biometric data deleted only *after* the feature is installed.[85] To turn off this feature, a user must navigate through

[77] *See id.*

[78] *See* Caroline McCarthy, *Facial Recognition Comes to Facebook Photo Tags*, CNET NEWS (Dec. 15, 2010), http://news.cnet.com/8301-13577_3-20025818-36.html ("Facebook announced [Dec. 15, 2010] that it will soon enable facial-recognition technology," which is "the first time facial recognition software has been incorporated into Facebook's consumer service.").

[79] *See* McCarthy, *supra* note 72.

[80] Mitchell I, *supra* note 1; *see also* Alexei Oreskovic, *Facebook Facial Recognition Technology Sparks Renewed Concerns*, REUTERS (June 8, 2011) ("On Tuesday, Facebook said it had expanded the availability of its "Tag Suggestions" product, which uses facial recognition technology to automatically identify the people who appear in certain photos posed on Facebook.").

[81] *See* Oreskovic, *supra* note 80 (quoting Facebook's spokesperson as saying, "[w]e should have been more clear with people during the roll-out process when this became available to them").

[82] Megan Geuss, *Facebook Facial Recognition: Its Quiet Rise and Dangerous Future*, PCWORLD (Apr. 26, 2011), http://www.pcworld.com/article/226228/facebook_facial_recognition_its_quiet_rise_and_dangerous_future.html (assisting Facebook users in understanding how Facebook's facial recognition tool works because Facebook did not explain the facial recognition feature it had implemented).

[83] *See* Mitchell I, *supra* note 1.

[84] *See id. See generally* FACEBOOK BLOG, *supra* note 69.

[85] *See In re Facebook and the Facial Identification of Users*, EPIC (June 10, 2011), http://epic.org/privacy/facebook/facebook_and_facial_recognitio.html (emphasis added).

his or her privacy settings to "opt out" of the tag suggestion service.[86] In addition to opting out, a user has to send a message to Facebook and specifically request that Facebook delete the data that it has collected.[87] This multi-layered process is confusing and there is no instruction page or notification alerting users that opting out is an option.[88] To compensate for Facebook's instructional shortcomings, various news outlets began posting systematic manuals to assist Facebook users through the numerous steps required to remove the information.[89]

C. Facebook Users Should Be Concerned

Facebook users should be concerned that Facebook stores their personally identifiable information for three main reasons. First, Facebook has been involved in litigation as a result of its lack of privacy controls. Second, Facebook does not publicize how the biometric data is secured. Finally, Internet hackers have shown their resilience and capacity to infiltrate the Internet servers of security firms to obtain sensitive information,[90] thus posing a potential threat to Facebook. Without added protections and safeguards to ensure the safe storage of biometric data, Facebook users should request that Facebook delete their biometric data.

[86] Facebook customers are automatically opted into having their biometric data stored. *See* Oreskovic, *supra* note 80 (explaining Facebook users had their data stored without their knowledge). However, due to a November 2011 settlement between the FTC and Facebook, the FTC now requires Facebook to let users opt into changes that alter how their personal information is shared and stored. *See* Elinor Mills, *Facebook Privacy Practices Get FTC Shakeup*, CNET NEWS (Nov. 29, 2011), http://news.cnet.com/8301-27080_3-57333008-245/facebook-privacy-practices-get-ftc-shakeup/ (discussing the settlement that was reached between the FTC and Facebook).

[87] *See EPIC Warns of Facebook 'Biometric Data Collection'*, INT'L BUS. TIMES (June 14, 2011), http://www.ibtimes.com/articles/162891/20110614/epic-ftc-facebook-facial-recognition.htm.

[88] *See Data Use Policy*, *supra* note 12 (explaining how tag suggestions work, but noticeably lacking instructions on how users can compel Facebook to remove their biometric data from the database).

[89] *See e.g.*, Amy Lee, *How to Disable Facebook's New Facial Recognition Feature*, HUFFINGTON POST TECH. (June 8, 2011), http://www.huffingtonpost.com/2011/06/08/disable-facebook-facial-recognition-photo-feature_n_873018.html.

[90] *See e.g.*, Nate Anderson, *How One Man Tracked Down Anonymous—and Paid a Heavy Price*, ARS TECHNICA (Feb. 2011), http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars/.

1. Old Habits Die Hard: Facebook's Privacy Litigation

Facebook has a nonchalant attitude toward its users' privacy,[91] which has been highlighted in various lawsuits involving Facebook's lack of privacy protections.[92] For example, in *In re Facebook Privacy Litigation* the district court held that Facebook did not violate the law when it provided its users' personally identifiable information to third-party advertisers because the advertisers were the intended recipients of the information.[93] Nevertheless, without its users' knowledge, Facebook facilitated the transmission of its users' personally identifiable information to third parties when a user clicked on an advertisement posted on Facebook.[94]

Another more recent example is *In Re Zynga Privacy Litigation*, a class action alleging the Facebook application Zynga was transmitting Facebook User IDs ("UIDs") to third parties, such as advertisers and Internet tracking firms.[95] Each Facebook user has his or her own unique UID,[96] and when an advertiser has access to a user's UID, that advertiser is able to discover a user's personal information.[97] The information accessible to the advertiser includes the user's real name, any public information listed on his or her profile, and the user's web-browsing history—information the user did not know was being transmitted to the advertiser.[98] Accordingly, Facebook users need not only be aware of Facebook's privacy policy, but they must also understand the privacy policies of Facebook's advertising partners.

Although these two lawsuits are only a fragment of the litigation in which Facebook has been involved, both cases emphasize that Facebook passes along its users' private information, often without specific permis-

[91] *See* Jessica E. Vascellaro, *Facebook Grapples With Privacy Issues*, WALL ST. J. TECH. (May 19, 2010), http://online.wsj.com/article/SB10001424052748704912004575252723109845974.html (describing Facebook's various privacy problems and the view of Facebook's founder, Mark Zuckerberg, that users should be more open with their information).

[92] *See id.*

[93] *See In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011).

[94] *See id.* at 709, 711–13.

[95] *See* Ian Paul, *Zynga Hit With Lawsuit Over Facebook Privacy Breach*, PCWORLD (Oct. 20, 2010), http://www.pcworld.com/article/208267/zynga_hit_with_lawsuit_over_facebook_privacy_breach.html.

[96] *See id.*

[97] *See id.*

[98] *See id.*; *see also* Richard Esguerra, *Facebook's Broken Promises: Facebook Apps Leaking Private Data to Advertisers and Trackers*, ELECTRONIC FRONTIER FOUND. (Oct. 18, 2010), https://www.eff.org/deeplinks/2010/10/facebooks-broken-promises-facebook-apps-leaking ("Internet advertising networks claim to track users 'anonymously,' but the Facebook leak allows these web marketing snoops to associate Facebook users with the supposedly-anonymous browsing-history cookies that trackers use to see a user's movements across the web.").

sion from the user. This litigation illuminates the way in which Facebook will likely treat the biometric data currently in its control and should undoubtedly raise concern among Facebook users.

2. Facebook Should Create a Strategy to Prevent Privacy Violations

Federal agencies have developed and implemented strategies to ensure that their collection of biometric data will not violate individual privacy concerns, and, further, to prevent the compromising of valuable personal information.[99] While the purpose of the use varies among federal agencies, facial recognition technology is often used for national security.[100] For example, the technology allows law enforcement agencies to identify unknown individuals in photos using the Federal Bureau of Investigation's ("FBI") database of 10 million stored mug shots.[101] Unlike Facebook, before the implementation of facial recognition technology, the FBI studied research from the National Institute of Standards and Technology's Biometrics and Identity Management subcommittee and released a Privacy Impact Assessment ("PIA").[102] The model described in the FBI's PIA is similar to the model suggested by the Biometrics and Identity Management subcommittee to determine whether a biometric system adequately protects information privacy.[103]

The Biometrics and Identity Management subcommittee's ("BIM") model is geared toward government agencies, but, nevertheless, the model lends insight into what a proper privacy assessment should entail.[104] BIM recommends that the privacy assessment should begin at the collection phase by determining the expectations of the participants who have *chosen* to enroll in the data collection system.[105] Subsequently, there should be: (1) documentation of the purpose and scope of the data collection to make

[99] SAND ET AL., *supra* note 44, at 43–49.

[100] *Face Recognition*, EPIC.ORG, http://epic.org/privacy/facerecognition/ (last visited Apr. 15, 2012) (stating the Government has used facial recognition technology for security purposes such as border control and general policing purposes).

[101] *See* Aliya Sternsteing, *FBI to Launch Nationwide Facial Recognition Service*, NEXTGOV.COM (Oct. 7, 2011), http://www.nextgov.com/nextgov/ng_20111007_6100.php.

[102] *See id.*

[103] *Compare* SAND ET AL., *supra* note 44, at 40, *with Privacy Impact Assessment for the Next Generation Identification Interstate Photo System*, FBI.GOV (June 9, 2008), http://www.fbi.gov/foi/privacy_impact-assessments/interstate-photo-system.

[104] *See* SAND ET AL., *supra* note 44, at 54 (stating the primary objective of NSTC is "the establishment of clear national goals for *Federal* science and technology investments," and NSTC's research and development strategies are to assist *Federal* agencies in coordinating national goals (emphasis added)).

[105] *See id.* at 45 (emphasis added).

certain the data is not used for unintended purposes; (2) a privacy review of the data to ensure the minimal amount of data is being collected to achieve the purpose of the agency; (3) identification of other technologies being used to better assess how the personal data will be used; (4) routine audits of the data and its uses and assessment of the control of individuals to use the information; (5) a review of the created template from the observed data; and (6) a decision regarding which data will be stored.[106] If implemented properly, BIM projects the system is less apt to infringe on the privacy rights of the data subjects.[107] Again, while this model is focused at government agencies and their use of biometric data, it is accessible by private companies, such as Facebook.

Supposing Facebook users know that their data fuels the facial recognition tool, there is still no assurance from Facebook that this data will solely be used in the tag suggestions tool.[108] Without a clear statement of purpose, as suggested in the BIM model and followed by Government agencies, there is a strong likelihood the biometric data will be used by Facebook for purposes other than those originally intended and used without the informed and voluntary consent of users.[109] The process of using information beyond the originally intended scope has been termed "function creep."[110]

Despite the potential privacy violation, function creep is almost inevitable because "[t]he existence of a relatively high integrity scheme would create *irresistible temptations* to apply it widely, and interrelate many hitherto separate collections of personal information."[111] Accordingly, in terms of Facebook's collection of biometric data, function creep is a viable and likely possibility, as Facebook does not guarantee its users' biometric data will be used solely for the purpose of facilitating the tagging process.[112] In

[106] *See id.* at 45–49.

[107] *See id.* at 53.

[108] *See* Purewal, *supra* note 2.

[109] *See* JOHN D. WOODWARD ET AL., ARMY BIOMETRIC APPLICATIONS: IDENTIFYING AND ADDRESSING SOCIOCULTURAL CONCERNS 24 (RAND 2001).

[110] *See* Simon G. Davies, *Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine*, 7 INFO. TECH. & PEOPLE 44 (1994); *see also* Sloan v. SC Dep't of Pub. Safety, No. 25689 (filed Aug. 4, 2003), *available at* http://www.sccourts.org/opinions/HTMLFiles/SC/25689.htm (describing an example of function creep that occurred in 1998. The South Carolina Department of Public Safety sold information and photographs used on South Carolina drivers' licenses and identification cards to Data Image, LLC. Plaintiff was aware that her information was used for her driver's license, but the transmittal and use of the information beyond its immediate and obvious scope of use, for driver's licenses, was a surprise to Plaintiff. As a result, the sale eventually resulted in a privacy lawsuit.).

[111] *See* Davies, *supra* note 110, at 38–47 (emphasis added).

[112] *See Privacy Settings*, FACEBOOK, https://www.facebook.com/settings/?tab=privacy (last visited Apr. 15, 2012) (allowing Facebook users to turn off the tag suggestions feature, but

addition, Facebook does not have a posted policy stating its projected use of the biometric data.[113] The lack of a strategic model makes privacy violations more likely, based on BMI's and privacy experts' projections.

3. Facebook is Not Hacker[114] Proof

Facebook is not immune from the wrath of hackers and security threats, thus making its database of information a potential target for external abuse.[115] Facebook's Security page contains an instructional aide to assist users who have had their Facebook profiles compromised (also known as "hacked") and provides information on how to avoid being a victim of online fraud.[116] Despite this instructional aid, Facebook estimates it has approximately 600,000 imposters accessing users' personal information on a daily basis.[117] In fact, in January of 2011, Facebook Founder Mark Zuckerberg's Facebook fan page was hacked.[118]

lacking explanation regarding what the data will additionally be used for or that users can request that Facebook delete their biometric data). While Facebook does explain that it will extract metadata, Facebook fails to include that in addition to the time, date, and place the photograph was taken, it also measures the facial features of the people in the photographs. *See Data Use Policy*, *supra* note 12 (explaining to Facebook users that "[w]hen [users] post things like photos or videos on Facebook, [Facebook] may receive additional related data (or metadata), such as the time, date, and place [users] took the photo or video."). Also, by mere definition, biometric data and metadata are not one and the same—biometric data is information that can identify an individual, while metadata is background information about a photograph or document, such as when the photograph was taken or if it has been modified. *Compare* Woodward, Horn, Gatune & Thomas, *supra* note 33 (defining biometric data as "a measurable . . . distinctive physical characteristic or personal trait that can be used to identify an individual"), *with* Autotech Techs. Ltd. P'ship v. AutomationDirect.com, Inc., 248 F.R.D. 556, 557 (N.D. Ill. 2008) (defining metadata as information regarding "when the document was created [and] when it was modified . . . .").

[113] *See Data Use Policy*, *supra* note 12 (discussing the use of data, but failing to mention the full extent of the use of biometric data).

[114] The term "hacker" is used to describe an individual who secretly manipulates network connections and/or breaks into computer systems. *See* Ken Hess, *What Is a Hacker?*, ZDNET (Sept. 27, 2011, 3:05 AM), http://www.zdnet.com/blog/security/what-is-a-hacker/9468.

[115] *See e.g.*, Emma Barnet, *Hackers Go After Facebook Sites 600,000 Times Every Day*, TELEGRAPH (Oct. 29, 2011), http://www.telegraph.co.uk/technology/facebook/8856417/Hackers-go-after-Facebook-sites-600000-times-every-day.html.

[116] *Facebook Security, How To Help Your Friends with Security Issues*, FACEBOOK (Apr. 27, 2011), https://www.facebook.com/note.php?note_id=10150165098990766.

[117] *See* Barnet, *supra* note 115.

[118] *See* Ian Paul, *Mark Zuckerberg's Facebook Fan Page Hacked*, PCWORLD (Jan. 26, 2011), http://www.pcworld.com/article/217784/mark_zuckerbergs_facebook_fan_page_hacked.html.

While Facebook has been previously hacked, the damage from hacking has not been exceedingly detrimental to its users.[119] However, this does not mean the potential for hackers to delve into the Facebook database does not exist. Hackers have flaunted their abilities by hacking into the databases of gaming companies and accessing gamers' personal information, including credit card information.[120] A recent example of the prowess of hackers is the ambush on the security firm HBGary.[121] HBGary provides resources to protect the assets and information of governments and private corporations from espionage.[122] Despite HBGary's background and field of expertise, in February 2011, a notorious group called Anonymous hacked HBGary's database.[123] Anonymous[124] was able to access the security firm's database, including the log-in credentials of its Chief Executive Officer, which were used to administer a corporate e-mail account.[125]

Anonymous's members later threatened to target Facebook in November 2011.[126] Although the attack did not occur and Anonymous later claimed the threat was merely a hoax, the implication caused security specialists to contemplate the possibility of an attack on Facebook.[127] Again, Facebook has been fortunate in that it has managed to avoid a major breach of their database; nevertheless, the possibility does exist in light of the capabilities of groups such as Anonymous. Facebook users should thus be

[119] *See e.g.*, *Facebook Hacked: Are you Seeing Images of Porn and Violence?*, ZDNET (Nov. 14, 2011, 8:21 PM), www.zdnet.com/blog/facebook/facebook-hacked-are-you-seeing-images-of-porrn-and-violence/5314 (discussing that Facebook was hacked, resulting in select users being flooded with pornographic images); *see also Facebook Security: Take Action*, FACEBOOK, https://www.facebook.com/security?sk=app_10442206389 (last visited Apr. 15, 2012) (stating accounts have been taken over and used to send spam messages).

[120] Winda Benedetti, *Steam Game Service Hacked, Credit Card Theft Investigated*, MSNBC.COM (Nov. 10, 2011), http://ingame.msnbc.msn.com/_news/2011/11/10/8742607-steam-game-service-hacked-credit-card-theft-investigated.

[121] *See* John Leyden, *Anonymous Security Firm Hack Used Every Trick In Book*, REGISTER (Feb. 17, 2011, 4:52 PM), http://www.theregister.co.uk/2011/02/17/hbgary_hack_redux.

[122] *Company*, HBGARY, http://hbgary.com/company (last visited Apr. 15, 2012).

[123] *See* Leyden, *supra* note 121.

[124] Declan McCullagh, *Alleged Anonymous Members Plead Not Guilty*, CNET NEWS (Sept. 1, 2011), http://news.cnet.com/8301-31921_3-20100790-281/alleged-anonymous-members-plead-not-guilty/ (describing Anonymous as a group of "activists who have electronically assaulted commercial and governmental Web sites" by computer hacking).

[125] *See* Leyden, *supra* note 121.

[126] *See* Adam Clark Estes, *Nobody Believes Anonymous Can Hack Facebook*, ATLANTIC WIRE (Aug. 10, 2011), http://www.theatlanticwire.com/technology/2011/08/nobody-believes-anonymous-can-hack-facebook/41086/.

[127] *See id.*

concerned with Facebook storing information regarding the intimate details of their faces and identities.

III. FACEBOOK'S PRIVACY VIOLATIONS

When Facebook users began identifying their friends in photos, few knew that Facebook was storing their friends' biometric data with each identifying click.[128] Facebook's act of collecting biometric data from its consumers is an invasion of privacy because biometric data that is continuously used is collected without user consent.[129] The data, as shown above, is highly personal and private to all Facebook users.[130] Additionally, most users may not anticipate that Facebook uses facial recognition technology to create an algorithm of their faces[131] when they simply upload photos to Facebook.[132] The following section provides an analysis of the potential constitutional privacy violations and potential violations of the applicable privacy torts as a result of Facebook's conduct.

A. Constitutional Violations

Due to the state action doctrine, private conduct generally does not have to comply with the Constitution.[133] However, there are circumstances where the acts of a private individual may be deemed that of the state.[134] Simply put, a private individual may be deemed a state actor when the actions of the private party can be considered "fairly attributable" to the

[128] *See* Purewal, *supra* note 2 (explaining that each time a Facebook user is "tagged" or identified in an image by a Facebook user, Facebook's facial recognition technology learns more about the identified member's appearance). *See generally* Gardiner, *supra* note 35 (explaining that face recognition tools are able to recognize faces by creating algorithms consisting of biometric data or "meaningful facial features").

[129] *See* Purewal, *supra* note 2 (suggesting that Facebook collects users' biometric information to use for its facial recognition tool).

[130] *See supra* Part II.

[131] *See* Angela Moscaritolo, *Shocker: Facebook Users Hate Surprise Photo Tagging*, PCMAG.COM (Feb. 16, 2012), http://www.pcmag.com/article2/0,2817,2400357,00.asp (stating Facebook uses facial recognition technology for its tag suggestions tool and that the tag suggestions tool was turned on by Facebook without warning to Facebook users); *see also* Gardiner, *supra* note 35 (explaining that facial recognition systems use algorithms (composed of key facial features) to identify individuals in photographs).

[132] *See* Milian, *supra* note 6 (explaining that when Facebook users upload a photograph on Facebook, Facebook uses facial recognition technology to identify the individuals in the photograph).

[133] ERWIN CHEMERINSKY, CONSTITUTIONAL LAW 548 (Vicki Been et al. eds. 3d ed. 2009).

[134] *See id.* at 552 (describing the exceptions to the state action doctrine).

state.[135] To be "fairly attributable," the private party must either be: (1) performing a sovereign function;[136] (2) engaging in a joint activity with the state, resulting in either a concerted activity or a mutually beneficial relationship;[137] or (3) performing an act that is affirmatively authorized by the state.[138] Once a private actor is found to be performing an action fairly attributable to the state, the private actor is deemed a "state actor."[139] Although a very difficult standard to meet, Facebook could potentially be considered to be in a mutually beneficial relationship[140] with the Government, thus making the United States Constitution applicable. Facebook allows the United States Government access to Facebook's database and user information.[141] The standard for a mutually beneficial relationship

[135] *See* Rendell-Baker v. Kohn, 457 U.S. 830, 836–38 (1982) (discussing that in order for the Fourteenth Amendment to be made applicable to the plaintiff, the actions of the plaintiff must be "fairly attributed" to the State).

[136] *See generally id.* at 842.

[137] *See* Moose Lodge No. 107 v. Iris, 407 U.S. 163, 172, 175 (1972). *See generally* Burton v. Wilmington Parking Auth., 365 U.S. 715, 725 (1961).

[138] *See generally* Reitman v. Mulkey, 387 U.S. 369, 375 (1967).

[139] Sheila Kennedy, *When is Private Public? State Action in the Era of Privatization and Public-Private Partnerships*, 11 GEO. MASON U. CIV. RTS. L.J. 203, 209–10 (2001) (stating a private act becomes attributable to the government, or a state action, "[w]hen the relationship between government and citizen becomes more complex than that between a mere commodity or service provider and its customers").

[140] *See Burton*, 365 U.S. at 724–25 (holding that the City and the private party had a mutually beneficial relationship; a relationship where, considering numerous factors, the state and private actor both profited from the relationship).

[141] *Accord* Julie Masis, *Is this Lawman Your Facebook Friend?*, BOS. GLOBE (Jan. 11, 2009), http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend?page=full (stating there are documented incidents where law enforcement has in fact used Facebook in pursuing investigations). *See generally Data Use Policy*, *supra* note 12 (explaining Facebook shares user information when lawfully requested. For Facebook to share user information there need only be "good faith belief" that the disclosure is required or that it is necessary to protect users.); *see also Safety Center, Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ (last visited Apr. 16, 2012) (stating Facebook "disclose[s] account records solely in accordance with [its] terms of service and applicable law, including the federal Stored Communications Act," which prohibits Facebook from releasing contents of a user account without a civil subpoena, court order, or warrant); *Facebook and Law Enforcement*, FACEBOOK, https://www.facebook.com/safety/groups/law (last visited Apr. 16, 2012) (disclosing Facebook provides a limited amount of information to help law enforcement officials do their jobs); JOHN LYNCH & JENNY ELLICKSON, OBTAINING AND USING EVIDENCE FROM SOCIAL NETWORKING SITES: FACEBOOK, MYSPACE, LINKEDIN, AND MORE, COMPUTER CRIME & INTELL. PROP. SEC., DEPT. OF JUSTICE (Mar. 3, 2010), *available at* https://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf (explaining in the Department of Justice's training materials that employees are able to use social media networks to "[r]eveal personal communications; [e]stablish motives and personal relationships; [p]rovide location information; [p]rove and disprove alibis; [and] [e]stablish crime or criminal enterprise," among other "instrumentalities or fruits of crime." Although the materials do not

requires interdependence, with the state profiting from the specific activity challenged.[142] Here, the challenged activity would be Facebook's collection and use of its users' biometric data. Although the state is not responsible for Facebook's collection of biometric data, it could be shown that both the state and Facebook derive a benefit from the relationship.[143]

Facebook permits the United States Government access to user information when there is a "good faith belief" that disclosure to the Government is required or necessary to protect users.[144] In fact, the Government paid a private company $11 million to "monitor and prepare surveillance reports on public reaction [to major Government proposals] posted on Facebook."[145] While this example does not furnish direct insight into the Government's handling of biometric data on Facebook, it does suggest the Government is readily accessing Facebook users' information and demonstrates the types of information Facebook is able to provide to the government. In addition, state law enforcement agencies are able to access Facebook databases for policing purposes.[146] With access to Facebook's database, the Government conceivably has access to the biometric data of all Facebook users—approximately 800 million people.[147]

While it is certainly feasible that law enforcement and/or the Government is using Facebook's biometric data, the extent of the relationship is uncertain because Facebook does not reveal how frequently the Government traffics and utilizes the website.[148] It is clear, however, that Facebook

expressly mention Facebook, there is information in the training materials regarding "tagging"—verbiage unique to Facebook.).

[142] *Burton*, 365 U.S. at 724–25 (holding that the City and the private party had a mutually beneficial relationship; a relationship where, considering numerous factors both parties profited from the relationship).

[143] *See Rendell-Baker*, 457 U.S. at 842–43 (explaining that in order for the defendant to be found a state actor the relationship must be mutually beneficial and both parties must derive a benefit from the precise activity being challenged).

[144] *See Data Use Policy*, *supra* note 12 (stating Facebook will share information in response to legal requests from jurisdictions inside and outside of the United States).

[145] *See* Andrea Stone, *DHS Monitoring of Social Media Under Scrutiny By Lawmakers*, HUFFINGTON POST (Feb. 16, 2012), http://www.huffingtonpost.com/2012/02/16/dhs-monitoring-of-social-media_n_1282494.html.

[146] *See Facebook and Law Enforcement*, *supra* note 141 (stating Facebook allows law enforcement agencies to access the Facebook database as long as a court order or civil subpoena is granted).

[147] *Id.*

[148] *See* Jeff John Roberts, *The Relationship Between Facebook and the Law*, GLOBE & MAIL (Jul. 12, 2011), http://www.theglobeandmail.com/news/technology/digital-culture/social-networking/the-relationship-between-facebook-and-the-law/article2094889/ (stating "Facebook apparently did not inform account-holders or their lawyers about government snooping" and further describing the relationship between Facebook and the government. Notably, in an interview

donates money to federal candidates to protect itself from stringent privacy policies, further entangling the two parties.[149] Facebook has formed a political action committee that allows employees to funnel contributions to federal candidates who share objectives similar to those of Facebook.[150] Moreover, on the "Facebook Live" page, Facebook frequently endorses candidates by featuring their discussions live.[151] The connection between Facebook and the Government appears to continually expand, and arguably, so does their mutually beneficial relationship.[152]

1. The Fourth Amendment's Privacy Protection of the Person and Possessions

Assuming Facebook can surpass the difficult test of being deemed a state actor, a Facebook user may choose to invoke his or her Constitutional right to privacy.[153] The Constitution does not expressly grant the right to privacy; however, a privacy right is implied through the "penumbras" found within the Constitution.[154] Precedent holds that the Fourth Amendment provides each individual with a right to privacy where there is: (1) an actual expectation of privacy, and (2) the expectation is reasonable based on societal standards.[155] However, any reasonable expectation of privacy is relinquished when information is given to a third party because the third party then has the ability to inspect and consume the information in any manner he or she sees fit.[156] This doctrine is termed the "third party doctrine" and undoubtedly becomes an obstacle for Facebook users bringing suit.[157]

Nevertheless, Facebook is violating its users' privacy irrespective of the third party doctrine.[158] Facebook users have an expectation of privacy

Facebook Chief Security Officer Joe Sullivan remained silent when pressed to reveal how many warrants had been served on Facebook.).

[149] *See* Jim Puzzanghera, *Facebook to Launch Its Own Political Action Committee*, L.A. TIMES TECH. (Sept. 26, 2011, 3:03 PM), http://latimesblogs.latimes.com/technology/2011/09/facebook-to-launch-its-own-political-action-committee-.html.

[150] *See id.*

[151] *See Facebook Live*, FACEBOOK, https://www.facebook.com/FBLive?sk=wall (last visited Apr. 16, 2012).

[152] *See* Roberts, *supra* note 148 (explaining the expanding relationship between Facebook and the Government).

[153] *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing the right to privacy as legitimate and preventing state actors from influencing intimate decisions).

[154] *Id.* at 484.

[155] Katz v. United States, 389 U.S. 347, 353 (1967).

[156] California v. Greenwood, 486 U.S. 35, 40–41 (1988).

[157] *See id.*

[158] *See id.*

in their biometric data. The many users who were both surprised and hostile upon discovering that their biometric data was being extracted from pictures exemplify an actual expectation of privacy in this information.[159] Society seems to agree that this information is private. Most individuals, for instance, protect personally identifiable information, such as their social security numbers, which is comparable to biometric data.[160] The challenge becomes the third party doctrine. When users upload photos on Facebook, they transmit and share information with third parties, such as their Facebook friends and Facebook itself.[161] Based on the third party doctrine, Facebook users lose any reasonable expectation of privacy in their photographs upon such transmittal. While users lose their reasonable expectation of privacy to their photographs, do they additionally lose their reasonable expectation of privacy to their biometric data?[162]

As technology advances, so does the idea of privacy rights.[163] For example, in *Kyllo v. United States*, the U.S. Supreme Court held that searches involving technological advances that reveal "intimate details" of the home are an improper search and thus violate a person's privacy rights.[164] Similarly, Facebook is using advanced technology to extract intimate details from a person's photo.[165] Thus, the argument could be made that a Facebook user has a reasonable expectation of privacy concerning his or her biometric data, since the technology used to collect the data is not just a simple enhancement, but rather an invasion into a person's intimate details.[166] Overall, as discussed, finding a Constitutional violation would be a difficult task with multiple hurdles. Accordingly, a California user may have a greater chance in bringing suit by alleging violations of the California Constitution.

[159] *See* Daily Mail Reporter, *supra* note 7.

[160] Joshua J. McIntyre, *Balancing the Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected As Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 903 (describing how Social Security numbers and biometric data can both identify specific individuals).

[161] *Data Use Policy*, *supra* note 12 (describing that when users post images on Facebook, Facebook receives the information from the photographs, in addition to the individual users allowed to see the image).

[162] *Greenwood*, 486 U.S. at 40–41 (explaining that generally, when an individual gives information to a third party, the individual then loses his or her reasonable expectation of privacy in that information).

[163] Kyllo v. United States, 533 U.S. 27, 35 (2001).

[164] *See id.*

[165] McCullagh, *supra* note 5.

[166] *Kyllo*, 533 U.S. at 38.

2. The California Constitutional Violations

States have the ability to afford greater rights than the federal government, ergo the state of California has granted its citizens more privacy protection than the federal government.[167] As a result, Facebook has violated the California Constitution as well. Assuming Facebook is a state actor, the California Constitution is applicable to Facebook because there is personal jurisdiction—the right to subject Facebook to California laws.[168] The personal jurisdiction analysis necessary to determine whether Facebook is subject to California law is as follows: (1) the corporation's headquarters are in Menlo Park,[169] and (2) the privacy violations occurred in, were directed from, and emanated from California.[170] Additionally, personal jurisdiction exists for the following reasons:

1. [A] substantial portion of the wrongdoing took place in California;[171]
2. Facebook is authorized to do business in California;[172]
3. Facebook has sufficient minimum contacts with the state;[173] and

[167] Leonel v. Am. Airlines, Inc., 400 F.3d 702, 711 (9th Cir. 2005).

[168] Int'l Shoe Co. v. Washington, 326 U.S. 310, 316–320 (1945) (holding that personal jurisdiction exists when a corporation is carrying on systematic and continuous activities within a state, and those activities result in a "large volume of interstate business, in the course of which [that corporation] received the benefits and protection of the laws of the state").

[169] *Careers*, FACEBOOK, https://www.facebook.com/careers/life.php (last visited Apr. 16, 2012).

[170] Facebook's headquarters, where decisions regarding the facial recognition tool were made, are in California. *See id.*

[171] The wrongdoing argued in this Comment is the taking of biometric data from Facebook users' images. This decision to implement the facial recognition tool was likely made at the Facebook headquarters because the headquarters are the location where the decision-making individuals are stationed and perform their work. *See Careers: Menlo Park, CA*, FACEBOOK, https://www.facebook.com/careers/department.php?dept=menlo-park (last visited Apr. 16, 2012) (discussing the positions that are stationed at Facebook headquarters include Corporate Communications, Business Development, Program Management, Data Center Designs, etc.).

[172] Complaint at 8, Juror Number One v. California, No. 11CV00397, 2011 WL 507296 (E.D. Cal. Feb. 11, 2011) ("Defendant FACEBOOK, INC., is . . . authorized to do business in California.").

[173] Since a majority of Facebook's decisions and work is done at its headquarters in California, minimum contacts can be established. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 464, 487 (1985) (discussing that minimum contacts can be determined by establishing the company had "substantial and continuing relationship" in the jurisdiction. Factors considered to make the determination that a relationship exists include, but are not limited to, the percent of business completed at the operation.).

4. Facebook intentionally avails itself of the markets in the state through the promotion, marketing and sale of products and services in the state.[174]

With personal jurisdiction established, California's constitutionally established "inalienable right" to privacy is thus applicable to Facebook.[175] There is no categorical test to prove a privacy violation in California.[176] Instead, a plaintiff must meet a threshold to establish a valid claim.[177] To support a valid claim, the plaintiff must establish, at the minimum: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest."[178]

If a plaintiff is able to meet the threshold requirements, the court will engage in a balancing test that measures the countervailing interests supporting the conduct in question and the intrusion of privacy resulting from the conduct.[179] A plaintiff may rebut a showing of countervailing interests by demonstrating that there were "'feasible and effective alternatives' with a 'lesser impact on privacy interests.'"[180] The California standard is easier to meet than the federal Constitution's Fourth Amendment standard because in California, the plaintiff's reasonable expectation of privacy is based on "customs, practices, and physical settings" surrounding the alleged violation, any notice provided, and any consent obtained.[181]

The *Four Navy Seals v. Associated Press* decision, in which the court held that the Associated Press did not violate any privacy rights by reposting photographs originally posted on a website maintained by the plaintiff, highlights the application of the California standard.[182] In *Four Navy Seals*, the wife of a Navy Seal maintained an online photo album,

[174] *Burger King Corp.*, 471 U.S. at 475–76 (establishing that for personal jurisdiction to exist, defendant must meet the purposeful availment criteria, which take into account defendant's activities within a state).

[175] *See* Hooser v. Super. Ct., 84 Cal. App. 4th 997 (2000).

[176] *Leonel*, 400 F.3d at 712.

[177] *See id.*

[178] *See id.*

[179] Norman-Bloodsaw v. Lawrence Berkeley Lab, 135 F.3d 1260, 1271 (9th Cir. 1998).

[180] *Id.* at 1271.

[181] *Compare id.* at 1269 (stating that the test for a violation of privacy is a balancing test that considers the degree of intrusiveness, the state's interests in requiring intrusion, and the efficacy of the state's means for meeting its needs), *with* Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 30 (1994) ("[T]he diversity of federal constitutional 'privacy' interests has left the federal right to privacy . . . without any coherent legal definition or standard.").

[182] Four Navy Seals v. Associated Press, 413 F. Supp. 2d 1136, 1143 (S.D. Cal. 2005).

which included images of her husband and other active duty Navy Seal members in full uniform abusing war prisoners.[183] An Associated Press reporter discovered the images while performing a search on the Internet, downloaded them, and eventually published them.[184] The court stated that the Navy Seals did not have a reasonable expectation that the images would remain private after posting the images online, and thus the members had no right to privacy under California's constitution.[185]

Similar to the wife in *Four Navy Seals*, Facebook users are willingly posting images online.[186] Nonetheless, Facebook's actions are distinguishable. Facebook did more than simply repost the image in a different forum; Facebook used the image to extract sensitive information from unsuspecting users.[187] The act of extracting biometric data is not foreseeable, especially when Facebook users were unaware Facebook was using facial recognition technology.[188] Most users know how to download a photograph from Facebook because it is a simple process.[189] However, due to the complex nature of creating facial recognition algorithms, the vast majority of users likely does not compile information from photographs posted on Facebook to create a facial template of their friends, thus enabling them to link a user to his or her Facebook profile and other sensitive information.[190]

Thus, when applying the standard emanated in *Four Navy Seals*, Facebook users cannot expect the image itself to remain private, but have a reasonable expectation of privacy as to their biometric data. Before the data collection, Facebook did not provide notice or obtain consent from its users, as it was only after the data collection that Facebook announced its

[183] *Id.* at 1141.

[184] *See id.*

[185] *See id.* at 1143.

[186] *See id.*

[187] *See* Oreskovic, *supra* note 80 (stating that sensitive information like e-mail addresses may become associated with the Facebook database, and quoting Facebook's spokesperson as saying, "we should have been more clear with people during the roll-out process when this became available to them").

[188] *Id.* ("[W]e should have been more clear during the roll-out process when this became available to them.").

[189] *See* Jaime A. Madell, *The Poster's Plight: Bringing the Public Disclosure Tort Online*, 66 N.Y.U. ANN. SURV. AM. L. 895, 900 (2011) ("[A] user could simply click the 'download' link that appears underneath photos in the Facebook viewing console.").

[190] *See Face Recognition*, BIOMETRICS.GOV, 1 (2006), *available at* http://www.biometrics.gov/Documents/facerec.pdf (describing how facial recognition has become a "science of sophisticated mathematical representations and matching processes"); *see also* Keller, *supra* note 11 (describing how, with the use of facial recognition programs, individuals can connect a stranger to his or her identity and other private information).

use of facial recognition technology.[191] Additionally, it was not the usual practice and custom of Facebook to collect the biometric data of its users.[192] As a result, Facebook users would have a reasonable expectation of privacy as to the collection of their biometric data.

B. Facebook's Common Law Tort Violations

Privacy torts protect individuals from the "mental pain and distress" inflicted by the broadcasting of personal details.[193] There are four different torts that encompass the common theme of the right "to be let alone"[:][194] (1) intrusion upon seclusion; (2) publicity given to private life; (3) publicity placing person in a false light; and (4) appropriation of name or likeness.[195] The two torts Facebook is potentially violating are: (1) appropriation of name or likeness and (2) intrusion upon seclusion.

1. Appropriation of Name or Likeness

There is an appropriation of name or likeness when: (1) a plaintiff's name or likeness is used for the commercial benefit (2) without consent or a license.[196] The primary interest is similar to a property right—the ability of an individual to have the exclusive rights to his or her identity.[197]

It is no secret Facebook uses its members for commercial benefit; Facebook's members have become tools to attract advertisers.[198] As a result, Facebook has an incentive to increase its user base, thus enabling it to have

[191] *See* Oreskovic, *supra* note 80 ("[W]e should have been more clear with people during the roll-out process when this became available to them.").

[192] *See Data Use Policy*, *supra* note 12 (stating that one's name, profile pictures, network, and username are always publically available, but all other data collected is that which one may choose to make public).

[193] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

[194] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[195] *Id.* at 389 (dividing privacy torts into four distinct torts).

[196] RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977).

[197] *Id.* ("The interest protected by the rule stated in this Section is the interest of the individual in the exclusive use of his own identity . . . .").

[198] *See* Eric Eldon, *Facebook Revenues up to $700 Million in 2009, On Track Towards $1.1 Billion in 2010*, INSIDE FACEBOOK (Mar. 2, 2010), http://www.insidefacebook.com/2010/03/02/facebook-made-up-to-700-million-in-2009-on-track-towards-1-1-billion-in-2010/; *see also Facebook Ads*, FACEBOOK, https://www.facebook.com/advertising/?campaign_id=402047449186&placement=pf&extra_1=0 (last visited Apr. 15, 2011) (indicating to potential clients that Facebook provides the ability to "[c]onnect with more than 800 million potential customers").

more users to market.[199] Facebook is able to increase its user base and compete with similar networking websites by updating its features and tools to enhance and facilitate the networking experience—one such enhancement being the tag suggestions feature.[200] With each enhancement, Facebook collects more user data[201] and is able to use this data to entice advertisers to market their products on Facebook.[202] Facebook's database of biometric data is especially appealing to marketing companies that are already using facial recognition technology to tailor ads and suggestions to consumers.[203]

Furthermore, Facebook often bestows advertising companies with its users' personal information, their names and likenesses, for financial profit without those users' consent and knowledge.[204] For example, Facebook faced a lawsuit in October 2010 concerning a leak of user ID numbers to outside advertising firms.[205] Facebook's privacy policy states it will not sell its users' personal information.[206] However, when a user clicks on a third party advertisement, Facebook simultaneously sends a referral.[207] The referral "reveals the specific webpage [sic] address that the user was looking at prior to clicking on the advertisement," and may transmit "substan-

[199] *See* Jeff Macke, *3 Ways Facebook Plans to Exploit Users*, YAHOO! FIN. (Feb. 2, 2012), http://finance.yahoo.com/blogs/breakout/3-ways-facebook-ipo-exploit-users-172215377.html (discussing how ninety percent of Facebook's revenue is derived from Facebook selling users' information to advertisers, which had generated a revenue of $3.7 billion. Thus, Facebook is able to generate $4.50 with each user.).

[200] *See* Jason DeRusha, *Good Question: Why Does Facebook Keep Changing?*, CBSMINNESOTA.COM (Sept. 22, 2011), http://minnesota.cbslocal.com/2011/09/22/good-question-why-does-facebook-keep-changing/; *see also* Barbara Ortutay, *Q&A: The latest "New Facebook"*, USA TODAY (Sept. 23, 2011), http://www.usatoday.com/tech/news/story/2011-09-23/facebook-user-guide/50529242/1.

[201] *See* Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUND. (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline/ (explaining how Facebook has evolved and now requires users to list particular information and also allow the information to be made public).

[202] *See Facebook for Business*, FACEBOOK, https://www.facebook.com/business/ads/ (last visited Apr. 16, 2012) (showing advertisers that they will be able to hand pick their audience based on information users have listed on their profile, such as their location and education).

[203] *See* Shan Li & David Sarno, *Advertisers Start Using Facial Recognition to Tailor Pitches*, L.A. TIMES (Aug. 21, 2011), http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

[204] *See* Macke, *supra* note 199 (discussing how Facebook sells its user's information).

[205] *See District Court Upholds Facebook's Practice of Forwarding User Information to Online Advertisers*, LAW, TECH. & ARTS BLOG (July 17, 2011), http://wjlta.wordpress.com/2011/07/17/ninth-circuit-upholds-facebook%E2%80%99s-practice-of-forwarding-user-information-to-online-advertisers/.

[206] *See Data Use Policy*, *supra* note 12.

[207] *See District Court Upholds Facebook's Practice of Forwarding User Information to Online Advertisers*, *supra* note 205.

tial" information about the user.[208] Despite the court's holding that Facebook's practice of disclosing information was not illegal,[209] the court recognized that Facebook "shares users' personal information with third-party advertisers without users' knowledge or consent, in violation of [Facebook]'s own policies."[210]

Facebook has already collected its users' facial templates (their likenesses) without their consent.[211] In light of Facebook's past and current use of its users' data, it is evident Facebook is familiar with profiting from its users' likenesses.[212] Now, with access to each of its users' personally identifiable information, Facebook conceivably will be able to further profit from its users' likenesses.

2. Intrusion Upon Seclusion

Facebook could also be liable for intrusion upon seclusion. Under this tort theory, a plaintiff needs to prove the defendant has substantially interfered and intruded upon the plaintiff's personal and private affairs.[213] An act is considered a substantial intrusion if it is an intentional interference with a private place or matter in which a plaintiff has a reasonable expectation of privacy.[214] There are two primary obstacles in applying this tort. First, if the image is taken in a public arena, courts have held that intrusion upon seclusion does not apply.[215] Second, even if the photograph was not taken in a public forum, by posting the image on Facebook, the plaintiff is placing the photograph in an arena that is not secluded.[216] However, there is an applicable exception. An individual, even if in a public

[208] *See id.*

[209] *See id.*

[210] *In re* Facebook Privacy Litig., 791 F. Supp. 2d 705, 709 (N.D. Cal. 2011).

[211] *In re Facebook and the Facial Identification of Users*, *supra* note 82 (stating the biometric data collection "occurred without the knowledge or consent of Facebook users").

[212] *See* Macke, *supra* note 199 (stating Facebook sells its users' information to marketing companies).

[213] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[214] *See generally id.* § 652B cmts. a–b.

[215] *Id.* § 652B cmt. c ("Nor is there liability for observing him or even taking his photograph while he is walking on the public highway, since he is not then in seclusion . . . .")

[216] *See Data Use Policy*, *supra* note 12 (explaining that Facebook is not a secluded arena because select information is made public and thus is available to "anyone, including people off of Facebook"); *see also* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977) ("The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself.").

arena, can allege intrusion upon seclusion if the information that is intruded upon is not available to "public gaze."[217]

The National Science and Technology Council's report acknowledges that biometric data is sensitive and personal information,[218] and arguably a private affair. Though Facebook users post images that are taken in the public arena,[219] a user's biometric data is still private information because the data (for example, the exact measurement between a user's eyes) is information that is not available to public gaze.[220] Biometric data is thereby more than a mere image publicly posted on Facebook—it is a template of data and a breakdown of one's face.[221] Most persons may feel like the exact nature of their facial shape—the exact measurements between their eyes, the width of their nose, the length of their jawbone—is private information.[222] Also, Facebook's intrusion into the private affairs of its users was covert and intentional.[223] Since the extraction of the data requires a complex methodology,[224] it is unlikely the information was collected in error. Therefore, users could legitimately claim that Facebook has substantially intruded upon its users' private affairs by secretively collecting the facial template of each of its users.

Finally, there is not a clear set of directions on Facebook regarding how to opt out of the tag suggestion tool and have Facebook delete stored

[217] RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) ("Even in a public place, however, there may be some matters about the plaintiff . . . that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters.").

[218] *See* NSTC Subcomm. on Biometrics, *supra* note 38, at 8.

[219] *See* Chris Cox, *Making it Easier to Share with Who You Want*, FACEBOOK BLOG (Aug. 23, 2011, 11:00 AM), http://blog.facebook.com/blog.php?post=10150251867797131 (suggesting Facebook users upload photographs taken in public locations).

[220] RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) ("Even in a public place, however, there may be some matters about the plaintiff . . . that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters."); *see also* Bosnor & Johnson, *supra* note 34 (explaining that facial recognition systems collect biometric data and then measure the distances between 80 reference points on the face by creating numerical codes).

[221] *VeriLook Algorithm Features and Capabilities*, NEUROTECHNOLOGY, http://www.neurotechnology.com/verilook-technology.html (last visited Apr. 16, 2012) (explaining how facial recognition technology creates a template of the face and stores the information in a database).

[222] *See* Bonsor & Johnson, *supra* note 34 (discussing the facial features facial recognition software measures).

[223] *See In re Facebook and the Facial Identification of Users*, *supra* note 85 (stating Facebook intentionally collected the biometric data, and the collection was "without the knowledge or consent of Facebook users").

[224] Nathan Chandler, *How Facebook Tags Work*, HOWSTUFFWORKS (July 12, 2011), http://computer.howstuffworks.com/internet/tips/facebook-photo-tags2.htm (discussing how facial recognition involves complex algorithms and programming).

biometric data. As a result, users are likely required to navigate their way through a multi-layered process and to refer to an instruction guide from an outside source.[225] Consequently, it is difficult for users to prevent and stop the intrusion.

IV. THE HURDLES IN SUING FACEBOOK

Two primary issues plague private lawsuits against Facebook and can deter individuals from pursuing litigation against Facebook. First, in order to have standing[226] there must be an injury-in-fact.[227] However, this element is hard to prove because of the difficultly in ascertaining the compensable injury suffered by the collection, possession, and use of the biometric data.[228] Second, when users upload their photographs to Facebook, they consent to Facebook's privacy policy.[229] However, this procured consent is unconscionable.[230]

In light of these difficulties, courts should place an intrinsic value on privacy, thereby creating a compensable injury-in-fact and allowing individuals to bring claims against companies, such as Facebook, that violate privacy rights.

A. The Difficulty of Defining Damages

To assert a claim against Facebook, the harm that results in the collection, possession, and use of the biometric data must be quantifiable because

[225] Erica Ho, *How to Make Facebook Stop Recognizing Your Face in Photos*, TIME TECHLAND (June 8, 2011, 8:00 AM), http://techland.time.com/2011/06/08/how-to-make-facebook-stop-recognizing-your-face-in-photos/ (describing how it is confusing for users to navigate their way through the opt out process); *see also Data Protection Issues with Facebook's Facial Recognition Function*, DR. WIDMER & PARTNERS, ATT'YS LAW (Sept. 2011), http://www.widmerpartners-lawyers.ch/en/news/news/newsitems/Data+protection+issues+with+Facebook%E2%80%99s+new+facial+recognition+function.htm ("[T]he opt-out feature is both difficult for users to find on the website and difficult to use. [Further,] it is unclear whether users who have chosen to opt out of the feature actually have their biometric data deleted, or whether the tagging mechanism is merely blocked . . . .").

[226] *See* Allen v. Wright, 468 U.S. 737, 752 (1984) (holding that to appear in court, a party must have standing to sue; the right to adjudicate their claim(s)).

[227] U.S. CONST. art. III; *see also Allen*, 468 U.S. at 752.

[228] *See What's the Harm? Disputing Damages in Privacy Violation Cases*, WILEY REIN LLP PRIVACY FOCUS (June 2002), http://www.wileyrein.com/publications.cfm?sp=articles&newsletter=4&id=3079 (stating that courts have had difficulty in finding the value of privacy and non-tangible items because of the difficulty in quantifying the damage). As such, because biometric data is non-tangible, it would be difficult for the court to assess the damage.

[229] *Data Use Policy*, *supra* note 12.

[230] *See infra* Part IV.B.

federal and state courts can only adjudicate actual "cases and controversies."[231] To prove standing, there must be an injury-in-fact, a casual connection between the injury and the alleged conduct, and the injury must be susceptible to resolution through a favorable decision.[232] An injury-in-fact must be "distinct and palpable,"[233] meaning it must be inimitable, tangible, and not abstract.[234] Courts also typically do not find standing in cases where the issues are of broad social impact.[235] Similarly, to have standing in California, there must be an injury-in-fact; however, if the injury is not compensable by restitution, a court may still find standing exists if the injury was caused by an unfair business practice.[236]

Facebook's facial recognition tool is a recent advent and the totality of the injuries have yet to manifest;[237] thus it is difficult to determine the damages that will result from Facebook's invasion of privacy. Unfortunately, current privacy law does not consider the collection of personal information[238] or the risk of damage[239] enough to constitute an injury. This sentiment has become a common theme, and courts frequently find that personal information, including information that is collected online and easily manipulated, is not intrinsically valuable.[240] However, the majority of lawsuits that consumers have filed against companies collecting personal data have dealt with consumers' email addresses, mailing addresses, and purchasing history.[241] This information is personal but not as sensitive in

[231] *See Allen*, 468 U.S. at 750 ("Article III of the Constitution confines the federal courts to adjudicating actual 'cases' and 'controversies.'").

[232] *See id.* at 750–51.

[233] *See* Warth v. Seldin, 422 U.S. 490, 501 (1975).

[234] *See id.* at 508 (stating a plaintiff must allege "specific, concrete facts demonstrating that the challenged practices harm him, and that the plaintiff would personally benefit in a tangible way from the court's intervention").

[235] *See id.* at 499 (holding that a litigant must assert an injury that is peculiar to himself or to a distinct group of which he is a part, rather than one "shared in substantially equal measure by all or a large class of citizens").

[236] *See* Allergan, Inc. v. Athena Cosmetics, Inc., 640 F.3d. 1377, 1382 (Fed. Cir. 2011).

[237] *See* Singer, *supra* note 38 (discussing the potential harms that can be a result of Facebook's facial recognition software).

[238] *See What's the Harm? Disputing Damages in Privacy Violation Cases*, *supra* note 228.

[239] *See generally* Aronson v. Sprint Spectrum L.P., 767 A.2d 564 (Pa. Super. Ct. 2001).

[240] *See* Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (holding that a cardholder's name and spending information have little intrinsic value); *see also What's the Harm? Disputing Damages in Privacy Violation Cases*, *supra* note 228.

[241] *See generally* Powers v. Pottery Barn, Inc., 177 Cal. App. 4th 1039, 1045–46 (2009) (holding that e-mail addresses are *not* personal information as defined in the California Song-Beverly Credit Card Act, an Act that prohibits retailers from collecting personally identifiable information).

nature as biometric data largely because it is information that is readily placed on the Internet and does not include unique, personal identifiers.[242]

If injury is established, the court still needs to find that injury compensable.[243] For example, in the case *Pisciotta v. Old National Bancorp*, the plaintiffs alleged that a hacker *accessed* their personal information from Old National Bancorp's website, but did not allege identity theft.[244] The Seventh Circuit court found the alleged injury, accessing personal information, sufficient to confer standing, but did not find the injury compensable.[245] Nevertheless, the court held that the "time spent . . . seeking to prevent or undo the harm" from a data breach is a compensable injury.[246]

Facebook's privacy breach has not created a discernible, *compensable* injury. Although it is difficult and time consuming to figure out how to have Facebook remove the facial recognition tool, it is not impossible.[247] The difficulties do not rise to the level of causing a compensable injury since, as previously stated, there are several media outlets that have published instructional guides on how to remove one's biometric data from Facebook.[248]

In light of the difficulty in finding a compensable injury, courts need to consider placing a greater value on the biometric data and the protection of the data to prevent privacy intrusions. Already courts have allowed non-tangible claims such as economic advantage and family development to have an intrinsic interest.[249] The list of non-tangible claims that have been granted an intrinsic interest must expand as technology advances and, con-

[242] *Compare* NSTC Subcomm. on Biometrics, *supra* note 38, at 8, 21 (discussing how biometric data is "sensitive personal information" and how biometrics are "affected by the individual's unique genetic makeup"), *with* McIntyre, *supra* note 160 (explaining that e-mail addresses do not expressly identify an individual because "[e]-mail addresses may be shared, for example, by multiple people in one household (familyname@serviceprovider.com) or by multiple employees who sign in to a generic company account (info@company.com)").

[243] *See* Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 635 (7th Cir. 2007) ("[A] *compensable* injury proximately caused by the [defendant]" must be established to find the defendant in violation and establish damages (emphasis added)).

[244] *See id.* at 631 (emphasis added).

[245] *See id.* at 640; *see also* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (2010) (concluding, despite plaintiffs meeting the standing requirement, that they failed to allege an injury sufficient to state a claim under relevant state law).

[246] *See generally* Kuhn v. Capital One Fin. Corp., No. 05-P-810, 2006 WL 3007981, at 3 (Mass. App. Ct. Oct. 23, 2006).

[247] Lee, *supra* note 89.

[248] *See id.*

[249] *See* Gene R. Nichol, Jr., *Injury and the Disintegration of Article III*, 74 CALIF. L. REV. 1915, 1931 (1986).

sequently, makes the collection of biometric data easier for private companies capable of developing facial recognition software.[250]

B. Facebook's Privacy Policy Is Unconscionable and Negates User Consent

A contract that arises out of unequal bargaining power is deemed to be unconscionable and unenforceable.[251] To make this determination there must be procedural and substantive unconscionability, both of which are determined by examining the terms of the contract and the circumstances surrounding the transaction.[252] For procedural unconscionability, there must be an indication of unequal bargaining power and the element of surprise; meaning the unconscionable clause is usually buried in fine print and legalese.[253] Substantive unconscionability is established when the terms are unreasonably favorable to one party; when the contract is "one-sided."[254]

Facebook's data use policy ("user agreement") is potentially procedurally unconscionable because it incorporates an element of surprise by not including information regarding Facebook's biometric data collection.[255] Facebook states that by creating an account and logging into one's Facebook account, a user has agreed to its privacy policy.[256] The disclosure regarding this agreement is in fine print and notice of it only appears on a user's initial login.[257] After the first login, the disclosure no longer appears on the main login screen; however, the privacy policy can still be

[250] *See id.* (stating that the Court has found an intrinsic interest in non-tangible claims such as economic advantage, family development, the full power of the vote, not being forced to disclose religious contributions, and not being forced to go to public schools).

[251] *See* Henningsen v. Bloomfield Motors, Inc., 32 N.J. 358, 388 (1960) (stating differences in bargaining power can enable courts to find a contract unenforceable); *see also* Williams v. Walker-Thomas Furniture Co., 350 F.2d 445, 448 (D.C. Cir. 1965) ("It has been held as a matter of common law that unconscionable contracts are not enforceable.").

[252] *See generally Williams*, 350 F.2d at 449.

[253] *See generally id.*

[254] *See id.* at 449 ("[O]ne who signs an agreement without full knowledge of its terms might be held to assume the risk that he has entered a one-sided bargain. But when a party of little bargaining power . . . signs a commercially unreasonable contract with little or no knowledge of its terms, it is hardly likely that his consent, or even an objective manifestation of his consent, was ever given to all the terms. In such a case the . . . court should consider whether the terms of the contract are so unfair that enforcement should be withheld.").

[255] *See Data Use Policy*, *supra* note 12.

[256] FACEBOOK, http://www.facebook.com (last visited Apr. 16, 2012).

[257] *Id.*

viewed by locating the link in the bottom right corner of the website.[258] In pertinent part, the privacy policy states:

> When you post things like photos or videos on Facebook, we may receive additional related data (or metadata[259]), such as the time, date, and place you took the photo or video.
>
> We receive data from the computer, mobile phone or other device you use to access Facebook. This may include your IP address, location, the type of browser you use, or the pages you visit. . . . .
>
> . . . .
>
> We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.[260]

The privacy policy does not disclose that Facebook collects and stores biometric data, thus creating an element of surprise.[261]

Finding information on Facebook's biometric data collection can prove to be a difficult task.[262] In the "About" section, located at the bottom right corner on Facebook's homepage, there is a link to Resources, which in turn links to "Bloggers at Facebook."[263] There, the search function yields only one result when the term "biometrics" is searched.[264] While the result does suggest biometric data is private and needs to be protected, the result does not state, or even allude to, Facebook's collection of biometric

[258] *Id.*

[259] While the data use policy does state that it extracts metadata, this data is distinguishable from biometric data. *Compare* Woodward, Horn, Gatune & Thomas, *supra* note 33 (stating biometric data is "a "measurable . . . distinctive physical characteristic or personal trait that can be used to identify an individual"), *with* Autotech Techs. Ltd. P'ship v. AutomationDirect.com, Inc., 248 F.R.D. 556, 557 (N.D. Ill. 2008) (defining metadata as information regarding "when the document was created [and] when it was modified . . . .").

[260] *See Data Use Policy*, *supra* note 12.

[261] *See id.*

[262] *See* FACEBOOK, *supra* note 256.

[263] FACEBOOK BLOG, *supra* note 69.

[264] *Id.*; Tim Sparapani, *Viewpoints on Privacy for the Digital Age*, FACEBOOK BLOG (Jan. 28, 2010, 10:41 AM), https://blog.facebook.com/blog.php?blog_id=company&blogger=636748905.

data and Facebook's facial recognition tool.[265] Additionally, when searching for information regarding "facial recognition," the search yields seven results, only one of which specifically relates to Facebook's use of facial recognition technology.[266] Again, this result does not mention that biometric data is collected in conjunction with the facial recognition tool. It is likely only a technologically savvy user would know facial recognition software requires the collection of biometric data.[267] The blog entry referencing the tag suggestions provides a link to a separate page called the "Help Center."[268] Only when searching through the Help Center with the phrase "photo comparison" does information alluding to biometric data collection finally emerge: "When you're tagged in a photo, we associate the tags with your account, compare what these tagged photos have in common and store a summary of this comparison."[269] As demonstrated, information regarding the mechanics of the tag suggestions tool is spread among several pages and requires a user to perform keyword searches. Thus, it is conceivable that the user agreement is buried within the Facebook website, further contributing to the procedural unconscionability of the user agreement.

The substantive element is slightly more difficult to establish because the contract concerning the biometric data is not entirely one-sided.[270] On one hand, Facebook users can network more efficiently with access to the feature,[271] which is the primary objective of Facebook.[272] On the other hand,

[265] Sparapani, *supra* note 264 (quoting Ann Cavoukian, the "Information and Privacy Commissioner for Ontario, Canada," as stating, "[t]he growth of privacy-invasive technologies such as biometrics . . . has intensified the need to sharpen our focus on privacy and the best methods to protect it.").

[266] Mitchell I, *supra* note 1.

[267] *See* Chandler, *supra* note 224 (discussing how facial recognition involves complex algorithms and programming that require a computer programmer's skill level).

[268] *See* Mitchell I, *supra* note 1; *see also* FACEBOOK BLOG, *supra* note 69.

[269] *Help Center*, FACEBOOK, https://www.facebook.com/help/search/?q=photo+comparison (last visited Apr. 16, 2012); *What Information Does Facebook Use to Tell that a Photo Looks Like Me and to Suggest that Friends Tag Me?*, FACEBOOK, https://www.facebook.com/help/?faq=218540514842030#What-information-does-Facebook-use-to-tell-that-a-photo-looks-like-me-and-to-suggest-that-friends-tag-me? (last visited Apr. 16, 2012).

[270] *See Williams*, 350 F.2d at 449 ("[O]ne who signs an agreement without full knowledge of its terms might be held to assume the risk that he has entered a one-sided bargain. But when a party of little bargaining power . . . signs a commercially unreasonable contract with little or no knowledge of its terms, it is hardly likely that his consent, or even an objective manifestation of his consent, was ever given to all the terms. In such a case the . . . court should consider whether the terms of the contract are so unfair that enforcement should be withheld.").

[271] *See* Geuss, *supra* note 82 ("Facial recognition is a cool technology that Facebook is using to add more convenience to the act of tagging people in photos. The technology may indeed create more connections between friends . . . .").

Facebook's financial gains from the feature outweigh any efficiency given to the users because Facebook can make a profit from each piece of information Facebook stores regarding its users.[273] Further evidencing the one-sided nature of the user agreement, Facebook misleads users as to the terms of the agreement.[274] As such, the contract with regard to Facebook's acquisition of biometric data is unconscionable and its terms should be unenforceable.

V. SUGGESTIONS

Biometric data is personally identifiable information that the government has recognized to be highly sensitive,[275] therefore needing greater legal protections.[276] The cry for assistance in creating protections does not only come from individuals concerned about their privacy, but also from the Biometrics industry.[277] Industry leaders have asked for guidelines to ensure the privacy of individuals who have had their biometric data collected without their consent—a situation similar to Facebook's method of biometric data collection.[278] For the guidelines to be most effective, they need to be technology-based.[279]

Nevertheless, the United States has not created a uniform standard to protect privacy rights by preventing companies such as Facebook from col-

[272] *Info*, FACEBOOK, http://www.facebook.com/facebook#!/facebook?sk=info (last visited Apr. 2, 2012) ("Facebook's mission is to give people the power to share and make the world more open and connected.").

[273] *See* Macke, *supra* note 199; *see also* Somini Sengupta & Evelyn M. Rusli, *Personal Data's Value? Facebook is Set to Find Out*, N.Y. TIMES, Feb. 1, 2012, at A1, A15. ("Every time a person shares a link, listens to a song, clicks on one of Facebook's ubiquitous 'like' buttons, or changes a relationship status to 'engaged,' a morsel of data is added to Facebook's vast library. It is a siren to advertisers hoping to leverage that information to match their ads with the right audience.").

[274] Julia Angwin, Shayndi Raice & Spencer E. Ante, *Facebook Retreats on Privacy*, WALL. ST. J. (Nov. 11, 2011), http://online.wsj.com/article/SB10001424052970204224604577030383745515166.html (discussing a settlement reached between the U.S. government and Facebook over allegations Facebook misled users about its use of user information).

[275] *See* NSTC Subcomm. on Biometrics, *supra* note 38, at 21.

[276] *See id.* at 14 (discussing how because biometric data is sensitive information, there should be a system implemented to ensure the data remains private and does not infringe on individual rights).

[277] David George, *Face Recognition May Enhance Airport Security*, CNN (Sept. 28, 2001), http://articles.cnn.com/2001-09-28/us/rec.airport.facial.screening_1_biometric-technology-face-recognitionvisionics?_s=PM:US.

[278] *See id.* ("The [International Biomteric Industry Association] says there need to be rules to protect the privacy of people whose faces are scanned in public places" such as airports, where the individual is unaware his or her data is being collected).

[279] *See id.* ("The harsh new realities [of biometrics] require vigorous, technology-based responses . . . .").

lecting the data without user consent.[280] Similarly, Congress failed to require companies to ensure that proper measures have been taken to secure the data once it has been collected.[281] This section provides suggestions on how the United States should protect individuals' biometric data, particularly online. Conveniently, the United States can look to Europe for guidelines.[282] In addition, the United States Government should implement legislation to protect biometric data similar to the legislation enacted to protect medical information.[283] Finally, if Congress does not enact legislation heightening the protection of biometric data, the Federal Trade Commission should both continue to intervene when companies place the privacy of their consumers at risk and actively enforce settlements reached.[284]

[280] *See generally* Helen Pidd, *Facebook Facial Recognition Software Violates Privacy Laws, Says Germany*, GUARDIAN (Aug. 3, 2011), http://www.guardian.co.uk/technology/2011/aug/03/facebook-facial-recognition-privacy-germany ("The tool runs all photos uploaded to the social networking site through a [program] . . . . [T]hough users can opt out of the *automatic* tagging, Facebook can still gather and store (indefinitely) all photos added to the site." (emphasis added)).

[281] In November of 2011, the Federal Trade Commission reached a settlement with Facebook that requires Facebook to gain users' affirmative consent before disclosing "nonpublic user information" and that prevents Facebook from misleading users about the information that is being collected. *See* Agreement Containing Consent Order at 4, *In re* Facebook, Inc. (No. 092-3183), *available at* http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf. The settlement also requires Facebook to create a privacy program that addresses privacy risks of new products. *Id.* at 5. Notably, the settlement does not create any guidelines and leaves the responsibility of creating a comprehensive privacy scheme to Facebook. *See generally id.*

[282] *See supra* Part V.A.

[283] *See id.*

[284] The Federal Trade Commission ("FTC") recently developed the Privacy and Identity Protection division to assist in enforcing Section 5 of the FTC Act, which prohibits unfair or deceptive acts. *See Division of Privacy and Identity Protection*, FTC, http://www.ftc.gov/bcp/bcppip.shtm (last visited Apr. 16, 2012) (explaining the purpose of the Division of Privacy and Identity Protection). The FTC found Facebook in violation of Section 5 of the FTC Act, which led to the settlement between the FTC and Facebook. *See* Press Release, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises, FTC (Nov. 11, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm ("The social networking service Facebook has agreed to settle Federal Trade Commission charges that it deceived consumers . . . ."). As part of the settlement, the FTC will monitor Facebook to ensure compliance with the order. *See id.* While the settlement does showcase the FTC's move to enforce privacy protections, there are nevertheless potential issues with the private settlements and the ability of the FTC to enforce the orders. *See* Jeff Roberts, *Facebook Settlement Shows FTC Getting New Traction with Privacy Enforcement*, PAIDCONTENT (Nov. 11, 2011), http://paidcontent.org/article/419-facebook-settlement-shows-ftc-getting-new-traction-with-privacy-enforce/ ("The settlement[] . . . confirm[s] that . . . the FTC's Consumer Bureau called 'Privacy and Identity Protection' aspires to make a name for itself in online privacy issues."); Tim Bukher, *The Facebook FTC Settlement Will Just Give Users a False Sense of Security*, BUS. INSIDER (Dec. 1, 2011), http://articles.businessinsider.com/2011-12-01/tech/30462143_1_facebook-privacy-pract ("The problem is that this latest FTC settlement may . . . get users to drop their guards with a false sense that the FTC has covered all the bases."). For example, if a company breaches an FTC settlement, penalties *can* be imposed, but rarely are imposed. *See* Roberts, *supra* ("Technically, a

A. Borrowing the Privacy Model from Europe

After Facebook disclosed its tags suggestions, European privacy regulators immediately began inquiring about Facebook's facial recognition technology.[285] Namely, Germany alleged that Facebook is in violation of both European and German privacy laws because the biometric database has been compiled without user consent.[286] Johannes Caspar, the Data Protection Supervisor in Hamburg, suggested there would be grave results if the data Facebook has stored were to fall into the wrong hands.[287] The United Kingdom and Ireland have taken cue and are currently investigating the feature.[288]

European countries were able to allege privacy violations because these countries enacted a more stringent and sweeping privacy protection program than the United States.[289] The significant difference in the legal policies was noted at the European Parliament's Privacy Platform when Facebook's spokesperson acknowledged that Facebook honors the "transatlantic agreement to ensure European data remains safe and secure *by European standards* while in the United States."[290] The statement implies the

company that breaches the terms of an FTC settlement is liable for major civil penalties. In reality, though, such penalties are rarely imposed."). Other issues with the FTC settlement include, but are not limited to, the following: (1) Facebook is not required to admit wrongdoing; (2) without a legal proceedings, the privacy violations are not placed in the public spotlight; and (3) the settlement applies only to Facebook; thus, there is an not as widespread an impact in the social media arena. *See id.* (discussing the shortfalls of the FTC settlement).

[285] Ryan Singel, *Singel-Minded: Anatomy of a Backlash, or How Facebook Got an 'F' for Facial Recognition*, WIRED EPICENTER (June 9, 2011), http://www.wired.com/epicenter/2011/06/anatomy-of-backlash/.

[286] *See* Pidd, *supra* note 280.

[287] *See id.*

[288] *See* Steven Musil, *Facebook Faces Lawsuit Over Facial-Recognition Feature*, CNET NEWS (Nov. 10, 2011), http://news.cnet.com/8301-1023_3-57322815-93/facebook-faces-lawsuit-over-facial-recognition-feature/?part=rss&subj=latest-news&tag=title.

[289] Matthew Taylor, *Superinjunctions, Injunctions and Privacy Laws Around the World*, GUARDIAN (Apr. 26, 2011), http://www.guardian.co.uk/law/2011/apr/26/superinjunctions-injunctions-privacy-laws; *see also* Byron Acohido, *Critics Say Privacy Hearing Skewed Against Consumers*, USA TODAY (Sept. 15, 2011), http://content.usatoday.com/communities/technologylive/post/2011/09/critics-say-privacy-hearing-skewed-against-consumers/1 (noting California Representative Mary Bono Mack held a public hearing in September of 2011 titled "Internet Privacy: The Impact and Burden of EU Regulation." When it was announced there would not be a European witness to support the approach to privacy taken in the U.S., one privacy advocate explained, "this hearing could throw cold water on efforts to enact strong privacy protections, such as those that exist in Europe, in the United States.").

[290] Zack Whittaker, *Facebook Rebuked by EU Privacy Platform; Patriot Act a "Distraction"?*, ZDNET (Sept. 7, 2011), http://www.zdnet.com/blog/btl/facebook-rebuked-by-eu-privacy-platform-patriot-act-a-distraction/57482 (emphasis added).

standards between the two continents are different, and that the European standards are stricter than those of the United States.

Paul Schwartz, a law professor at the University of California, Berkeley, and a director of the Berkeley Center for Law & Technology, stated: "In Europe, there is a comprehensive privacy law in each nation which requires that online privacy be protected. In the U.S., we regulate sector by sector, and there are notable gaps in protection."[291]

Schwartz is likely referring to the 1995 Directive Authorized ("1995 Directive") by the European Union ("EU"),[292] which was further embellished in 2000 ("2000 Directive").[293] The European model is beneficial because it creates a uniform law among EU members, who were *required* to adopt the Directives,[294] and establishes clear requirements.[295] As a result, the EU is less prone to gaps in privacy protections.[296] Notably, the European Union Safe Harbor requires companies to give prior opt-in consent before collecting sensitive personal information.[297] The United States government should construct a scheme similar to the European model by creating uniform laws to help prevent inevitable future privacy violations.[298]

[291] John Moe, *What Can We Learn From Europe About Online Privacy?*, AM. PUB. MEDIA (Sept. 14, 2011), http://marketplace.publicradio.org/display/web/2011/09/14/tech-report-what-we-can-learn-from-europe-about-online-privacy/?refid=0.

[292] *See* S. REP. NO. 107-240, at 5 (2002) (explaining the 1995 European Directive governs online and offline data collection).

[293] *See generally* Council Directive 45/2001 (EC) 2001 O.J. (L 8) 1 (EC).

[294] *See* S. REP. NO. 107-240 at 5 (discussing that as of 1998, when the 1995 Directive was adopted, each member state of the European Union was required to adopt a policy mirroring the 1995 Directive); *see also* Council Directive 45/2001, art. 3, 2001 O.J. (L 8) 1 (EC) ("This Regulation shall apply to the processing of personal data by [the European Community] and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.").

[295] *See* S. REP. NO. 107-240 at 5–6 (explaining that the 1995 Directive requires companies "in both their online and offline practices, to provide: (1) notice; (2) an opt-out with respect to non-sensitive commercial marketing of personal information; (3) an opt-in with respect to sensitive personal information; (4) a right of access to personal information collected; and (5) reasonable security protections for that information.").

[296] *See* Moe, *supra* note 291 (explaining Europe has a "comprehensive privacy law in each nation," thus Europe is less prone to gaps in regulation, whereas the U.S. regulates sector by sector, which allows for inconsistencies); *see also* S. REP. NO. 107-240 at 6 (explaining that Europe had to create the European Union Safe Harbor in 2000, a set of less intrusive regulations that allow U.S. companies to comply with the Directive).

[297] S. REP. NO. 107-240 at 6.

[298] *Id.* (suggesting state legislatures have enacted inconsistent privacy laws and would prefer a more uniform standard).

B. Applying the Same Protection for Medical Information to Biometrics

Despite the surge of interest in protecting personally identifiable information, Congress has been grappling with how to create laws that encourage innovation in technology, while also ensuring that information collection is "fair, transparent, and subject to law."[299] Congress's struggle is evidenced in proposed legislation such as the Online Personal Privacy Act of 2002,[300] the Consumer Privacy Protection Act of 2002,[301] and the Privacy Act of 2005.[302] However, those laws have not yet been enacted.[303] For now, the legislature has focused on protecting medical information because health insurance companies and various businesses keep client health and medical information in electronic databases.[304]

Although medical information is considered extremely private, so is facial recognition data, which can reveal unique characteristics about people.[305] Additionally, the subcommittee on Biometrics explained that with specialized training, some biometric models could potentially be used to detect medical information or drug use.[306] Thus, the legislature should give biometric data the same protection as medical data.

[299] *Id.*

[300] Online Personal Privacy Act, S. 2201, 107th Cong. § 401 (2002).

[301] Consumer Privacy Protection Act of 2002, H.R. 1263, 109th Cong. (2005).

[302] *See* Consumer Privacy Protection Act of 2005, H.R. 4678, 107th Cong. § 401 (2002).

[303] *See* S. 2201; *see also* H.R. 1263.

[304] *Summary of the HIPPA Privacy Rule*, U.S. DEPT. OF HEALTH & HUM. SERVS., 1 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html (explaining the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") was enacted to protect the electronic storage of health information and ensure a patient's health information is private). The Department of Health and Human Services also developed the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"), which "appl[ies] to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form . . . ." *Id.* at 2. Overall, "[t]he Privacy Rule protects all 'individually identifiable health information' held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral." *Id.* at 3 (emphasis omitted). The general principle of the Privacy Rule is to require covered entities to disclose and request only the minimum amount of protected health information. *Id.* at 6. Congress has since been vigilant in enforcing HIPPA and, consequently, protecting medical information. *See* Rachel Grunberger, *Senate Hearings Focus on Lack of HIPPA Enforcement, Final HITECH Rule*, INSIDE PRIVACY (Dec. 22, 2011), http://www.insideprivacy.com/senate-hearings-focus-on-lack-of-hipaa-enforcement-final-hitech-rule/.

[305] *See* NSTC Subcomm. on Biometrics, *supra* note 38, at 14.

[306] *Id.*

C. Federal Agencies Avoid the Hurdle of Defining Damages

The Federal Trade Commission ("FTC") protects consumers from unfair or deceptive business practices through investigation and enforcement actions.[307] To pursue an enforcement action, the FTC must find a "reason to believe" that the law has been violated.[308] The "reason to believe" standard to initiate proceedings is a less rigid standard than the standing requirement of injury-in-fact.[309] Accordingly, the FTC is better suited to tackle Facebook's privacy violation, as the compensable-injury hurdle does not exist under the FTC.[310]

However, this avenue might not be the most effective way to combat Facebook's privacy intrusion. In June 2011, Electronic Privacy Information Center ("EPIC") filed its Complaint with the FTC; however, the FTC is under no obligation to respond.[311] In fact, after three months, the FTC's indirect response to the complaint was to host a workshop discussing the privacy issues related to facial recognition technology.[312] Thus, Facebook had the opportunity to continue to violate its users' privacy rights for 90 days while awaiting the FTC workshop.[313] In contrast, Facebook would have had 21 days to respond to a complaint filed in federal court[314] and 30 days to respond in California,[315] which could have allowed for a quicker remedy. Af-

[307] *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, *supra* note 20, at 3.

[308] *Id.* at 2.

[309] *Compare A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, *supra* note 20, at 2 ("[T]he Commission may initiate an enforcement action if it has 'reason to believe' that the law is being or has been violated."), *with* Warth v. Seldin, 422 U.S. 490, 499 (1975) (holding that litigant must assert an actual injury that is peculiar to himself or to a distinct group of which he is a part, rather than one "shared in substantially equal measure by all or a large class of citizens").

[310] *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, *supra* note 20 (discussing that the FTC need only have *reason to believe* there is a violation of the law to begin an investigation).

[311] *See* John E. Villafranco, *Challenging a Competitor's Advertising Claims*, ANTITRUST SOURCE (May 2005), http://www.americanbar.org/content/dam/aba/publishing/antitrust_source/may05_villafranco.authcheckdam.pdf (explaining that the FTC uses its own discretion to determine which complaints it will pursue).

[312] Press Release, FTC, FTC To Host Workshop on Facial Recognition Technology (Sept. 9, 2011), http://ftc.gov/opa/2011/09/facialrec.shtm.

[313] *Id.*

[314] FED. R. CIV. P. 12(a)(1)(i).

[315] CAL. CIV. PROC. § 438(h)(2) (West 2011).

ter five months, the FTC finally responded to EPIC's complaint by reaching a settlement with Facebook in November 2011.[316]

VI. Conclusion

Facebook violated the privacy rights of its users when it collected their biometric data without consent. Even though users can possibly establish Constitutional violations and potentially establish privacy tort violations, the lack of value afforded to keeping biometric data private makes it very difficult to establish damages.[317] While the Federal Trade Commission ("FTC") remains a viable source to file a complaint,[318] it may not be the most successful means because the FTC has the ability to choose which complaints to pursue.[319] Since it is difficult for private parties to protect their personal information through the courts, Congress should step in and either (1) create a uniform privacy model similar to Europe's, or (2) create legislation that protects biometric data similar to the legislation that has been created to protect health care information.[320] If Congress were to apply greater protections to biometric data, thereby heightening privacy protections of personalized information, courts would be able to follow suit.

[316] *See* Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises, *supra* note 19.

[317] *See supra* Part IV.A.

[318] *See supra* Part V.C.

[319] *See* Villafranco, *supra* note 311 (explaining that the FTC uses its own discretion to determine which complaints it will pursue).

[320] *See supra* Part V.A–B.