Harvard Journal of Law & Technology
Volume 26, Number 1 Fall 2012

A FACE TELLS MORE THAN A THOUSAND POSTS: DEVELOPING FACE RECOGNITION PRIVACY IN SOCIAL NETWORKS

*Yana Welinder**

TABLE OF CONTENTS

---

* Visiting Assistant Professor, California Western School of Law; Junior Affiliate Scholar, Center for Internet and Society at Stanford Law School. LL.M., Harvard Law School; J.D., University of Southern California; LL.B., London School of Economics and Political Science. An earlier version of this Article was submitted in partial fulfillment of my LL.M degree, and I would like to thank Professor John Palfrey for his helpful advice throughout my research. I am also deeply indebted to Professor Daria Roithmayr for her invaluable guidance, and I would like to thank the faculty at Chicago-Kent College of Law, Alexander Rodney, Andrew Crocker, Andrew Tuch, Clemens Wackernagel, Eike Hosemann, Elettra Bietti, Gerard Kennedy, Ivar Hartmann, Jane Bestor, Matthew Becker, Matt Vitins, Nathan Lovejoy, Noam Noked, and Rodrigo Lavados for their thoughtful comments on presentations of an earlier version of this Article. This Article has also greatly benefited from Professor Urs Gasser's helpful input regarding interoperability in social networks and discussions of a related piece with Professor Herbert Burkert, Professor Jonathan Zittrain, Professor Yochai Benkler, and Ryan Budish. Finally, I want to thank the editors and staff of the *Harvard Journal of Law & Technology* for their excellent editing and comments.

I. INTRODUCTION

During the "Green Revolution" in 2009, the Iranian military posted photos from the protests on a website and invited citizens to identify twenty individual faces that were singled out in those photos.[1] They claimed to have arrested at least two of the individuals in the photos shortly after the protests.[2] According to some sources, the Iranian government tried to use face recognition technology to identify protesters, though its technology was still under development.[3] Imagine if

1. *See* Fred Petrossian, *Iranian Officials 'Crowd-Source' Protester Identities*, GLOBAL VOICES (June 27, 2009, 5:28 PM), http://globalvoicesonline.org/2009/06/27/iranian-officials-crowd-source-protester-identities-online/ (discussing the photos posted on http://www.gerdab.ir/fa/pages/?cid=407).

2. *Id.*

3. John Preston, *The Net Delusion by Evgeny Morozov: Review*, TELEGRAPH (Jan. 9, 2011), http://www.telegraph.co.uk/culture/books/8241377/The-Net-Delusion-by-Evgeny-

the government could simply match these faces against the hundreds of billions of photos available on Facebook. The matches could reveal not only the protesters' names,[4] but also their whereabouts, their contacts, their online conversations with other protesters, and potentially their future plans.

Faces are particularly good for identification purposes because they are distinctive and, in most cases, publicly visible. Other personal features that are in plain sight — like coats and haircuts — can easily be replaced, but significantly altering a face to make it unrecognizable is difficult. And yet most people can remain anonymous, even in public, because they have only a limited set of acquaintances that can recognize them. The use of face recognition technology in social networks shifts this paradigm. It can connect an otherwise anonymous face not only to a name — of which there can be several — but also to all the information in a social network profile.

Given the risks of face recognition technology when combined with the vast amount of personal information aggregated in social networks, this Article presents two central ideas. First, applying Professor Helen Nissenbaum's theory of contextual integrity,[5] I argue that face recognition technology in social networks needs to be carefully regulated because it transforms the information that users share (e.g., it transforms a simple photo into biometric data that automatically identifies users) and provides this personally identifying information to new recipients beyond the user's control. Second, I identify the deficiencies in the current law and argue that law alone cannot solve this problem. A blanket prohibition on automatic face recognition in social networks would stifle the development of these technologies, which are useful in their own right. At the same time, our traditional privacy framework of notice and consent cannot protect users who do not understand the automatic face recognition process and recklessly continue sharing their personal information due to strong network effects. Instead, I propose a multifaceted solution aimed at lowering the costs of switching between social networks and providing users with better information about how their data is used.[6]

Morozov-review.html (stating that the Iranian government "us[ed] face-recognition technology to identify people from pictures taken on mobile phones"); *see also In re Facebook and the Facial Identification of Users,* ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/facebook/facebook_and_facial_recognitio.html (last visited Dec. 22, 2012) ("Iranian researchers are working on developing and improving facial recognition technology to identify political dissidents.").

4. Facebook currently has a policy that requires users to provide their real names upon registration. Somini Sengupta, *Rushdie Runs Afoul of Web's Real-Name Police*, N.Y. TIMES (Nov. 14, 2011), http://www.nytimes.com/2011/11/15/technology/hiding-or-using-your-name-online-and-who-decides.html.

5. See *infra* Part III.B–C.

6. *See infra* Part V.

My argument is that once users are truly free to switch networks, they will be able to exercise their choice to demand that social networks respect their privacy expectations.

In Part II, this Article begins with a general overview of face recognition technology and how it is implemented on Facebook. Part III of the Article uses the theory of contextual integrity to examine how social networks may violate user privacy when they apply face recognition technology to user photos. It also explains why more traditional privacy theories — epitomized by Warren and Brandeis' right to be let alone — cannot address this problem because they are mostly concerned with the privacy of physical spaces and confidential information. Having identified how face recognition technology violates privacy in this context, Part III explains why a complete prohibition of face recognition technology or related data processing could prevent the development of useful technologies. This sets the stage for my multifaceted proposal. Part IV reviews current laws that could potentially apply to this problem and concludes that they do not offer sufficient privacy protection. Finally, Part V outlines a combination of legal, architectural, market, and norm-driven solutions that I believe could offer adequate privacy protection without unduly stifling innovation.[7]

My proposed *legal* solution aims to reform our current privacy laws of notice and consent to require adequately informative notice and true consent. This proposed law would require a social network to provide users with detailed — yet comprehensible — information about how it collects, stores, processes, and shares user biometric data. It would also be required to obtain opt-in consent from users before collecting their data or using it for a new purpose. These requirements would be part of a broader data protection law, enforced by a proactive agency that could investigate the complicated data practices in social networks. More importantly, my proposal recognizes that even an improved notice and consent model cannot, by itself, solve this problem unless users have a real choice to leave a network without adversely affecting their online social lives.[8]

To this end, the architectural and market solutions of my proposal are aimed at lowering the cost of switching between social networks to free users from the network effect that currently locks them into a social network. The *architectural* solutions would enable users to:

---

7. This proposal is structured along the "four modalities of regulation" articulated by Professor Lawrence Lessig. *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0 125 (2d. ed. 2006) (presenting the four modalities of regulating online (and offline) behavior: "[l]aws, norms, the market, and architectures").

8. *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS, no. 4, 2011, at 32, 35 (2011) (calling into question how much choice a user actually has not to participate in a social network) [hereinafter Nissenbaum, *Contextual Approach*].

(1) prevent a centralized social network from extracting biometric data by instead sharing photos with their friends through a distributed social network; (2) export their personal information to a platform that they trust, under data portability standards; (3) continue to communicate with friends that remain in a centralized social network under interoperability standards; and (4) protect their privacy when they are photographed in public places or upload photos to a public network. The *market* solutions would further allow users to subsidize their social network use to avoid the collection of particularly sensitive information — like their biometric data — and to negotiate their own data use terms when sharing photos in social networks.

Finally, increased transparency of social networks and widespread knowledge about their data use practices would empower users to demand that social networks conform to pre-existing privacy *norms*. Lest these companies fail to provide users with full information about their data use practices, the state should also provide public education on online privacy to children and adults. The combination of these various solutions is aimed at ensuring a fair quid pro quo whereby users give out a reasonable amount of information about themselves for advertising purposes in return for a valuable socializing tool. Users will know and evaluate the cost of their social connectivity; if they find the cost to be excessive, they will be able to take their data and go elsewhere. The advantage of this multifaceted proposal — as compared to a blanket prohibition on face recognition technology in social networks — is that it narrowly addresses privacy concerns without stifling innovation in the development of face recognition technology and social networks.

Though my proposal is intended to apply to all current and future uses of face recognition technology in social networks, the examples in this Article largely focus on the most prominent social network to apply this technology: Facebook.[9] I therefore want to acknowledge at the outset the important social function that Facebook has served. Indeed, the Council of Europe recently proclaimed that "[s]ocial networks [serve] as human rights enablers and catalysts for democracy."[10] They are particularly important for youth, who rely on social networks for the "development of their own personalit[ies] and identit[ies], and as part of their participation in debates and social activities."[11] In 2011, Facebook also demonstrated its potential as a vital

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

10. *Recommendation CM/Rec (2012) 4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services*, COUNCIL OF EUR. (Apr. 4, 2012), https://wcd.coe.int/ViewDoc.jsp?id=1929453 [hereinafter *Recommendation*, COUNCIL OF EUR.].

11. *Id.*

channel for political mobilization, both during the Arab Spring and in the Occupy Wall Street movement.[12] Facebook thus facilitates social interaction and political discourse, which are functions that we consider highly valuable — if not essential — to our society.[13] But precisely because of its important role, Facebook needs to be secure and respect its users' privacy. It must pay particular attention to how it uses photos and biometric data because there is nothing more personal or susceptible to identification than a person's face. A person exposes her facial features wherever she goes, but she cannot easily replace her face if she does not want to walk around with her entire Facebook profile effectively tattooed on her forehead.

II. FACE RECOGNITION TECHNOLOGY AND FACEBOOK[14]

A. Overview of Face Recognition Technology

Face recognition technology aims to combine the superior perception skills of humans with the immense processing power and memory capacity of computers. Humans recognize other individuals based on their appearance — focusing on facial features — and by using other senses, such as smell, hearing, and sometimes touch.[15] While recognition is a natural human skill, the human brain can only memorize a limited number of faces.[16] On the other hand, computers can process and remember a vast number of facial features to recognize many more people.[17] But qualitatively, the human brain does a more complete job of recognizing faces than computers because it is able to combine visual recognition with other human senses. Computers lack contextual knowledge of what clothes a person tends to wear or in whose company she may be found.[18] Nonetheless, computer vision borrows techniques from human perception. These techniques are

12. This may be because, as Ethan Zuckerman observed, censorship of general-purpose applications like Facebook risks galvanizing users who would not otherwise be politically active because they use the applications for non-political purposes — such as looking at pictures of cats online. Ethan Zuckerman, *The Connection Between Cute Cats and Web Censorship*, MY HEART'S IN ACCRA (July 16, 2007, 10:30 PM), http://www.ethanzuckerman.com/blog/2007/07/16/the-connection-between-cute-cats-and-web-censorship.

13. *See Recommendation*, COUNCIL OF EUR., *supra* note 10.

14. Portions of Part II duplicate my discussion of face recognition technology in another paper. *See* Yana Welinder, *Face Recognition Privacy in Social Networks under German Law*, 31 COMM. L. BULL., no. 1, 2012, at 5.

15. *See* FACE PROCESSING: ADVANCED MODELING AND METHODS 8–9 (Wenyi Zhao & Rama Chellappa eds., 2006).

16. *See id.*

17. *See id.*

18. *See id.*

identified through psychological studies of how humans pay attention to certain facial features when they recognize others.[19]

Generally, the automatic face recognition process begins with an analysis of "training images" of already known individuals and measurement of their facial features.[20] These measurements — which make up the individuals' unique biometric data — are compiled into a biometric database along with other known information about them.[21] Face recognition technology is then applied to a new photo to find faces and identify them.[22] If it detects any faces in that photo, it "normalizes" them, which involves transforming their scale, position, and lighting, and sometimes converting them into gray scale images so that they can more easily be compared to faces photographed under different conditions.[23] The technology then identifies and measures facial features in the normalized faces.[24] The resulting measurements are compared to biometric data in the previously compiled database to identify the faces detected in the new photo.[25]

The accuracy of this process depends upon factors such as the exact methodology applied, the number of available training images, the quality of the photos, and the visibility of the individual within those photos.[26] The face recognition process is improving: although early face detection technologies could barely recognize a single face from a frontal view, technologies have now been developed that can identify individuals from various angles and distinguish faces from cluttered backgrounds.[27] As a study conducted by researchers at Carnegie Mellon University shows, photos that are available on Facebook without logging in are sufficient to identify college students on a campus with a 31.18 percent success rate when using face recognition technology that was publicly available until it was recently acquired by Google.[28]

---

19. *See id.*

20. *See* STAN Z. LI & ANIL K. JAIN, HANDBOOK OF FACE RECOGNITION 2, 8 (2005). The description of the technology in this article is intended as a general overview of the face recognition process, but many different technologies have developed in the field. *See* Andrea F. Abate et al., *2D and 3D Face Recognition: A Survey*, 28 PATTERN RECOGNITION LETTERS 1885, 1898 (2007).

21. *See* LI & JAIN, *supra* note 20, at 2–3 (describing use of facial databases for face recognition): *see also* Abate et al., *supra* note 20, at 1886 (describing uses of biometric databases).

22. *See* LI & JAIN, *supra* note 20, at 2–3.

23. *Id.*

24. *Id.*

25. *Id.* at 2–3.

26. *See* FACE PROCESSING, *supra* note 15, at 10–11.

27. *See id.*

28. Alessandro Acquisti, Associate Professor of Information Technology and Public Policy, Heinz College at Carnegie Mellon University, BlackHat Webcast: Faces of Facebook: Privacy in the Age of Augmented Reality (Jan. 9, 2012), *available at* http://www.blackhat.

B. Information Processed by Facebook's Photo Tag Suggest

In December 2010, Facebook introduced a new feature — called "Photo Tag Suggest" — that uses previously labeled photos and face recognition technology to identify individuals in new photos that users can then tag.[29] Facebook collects and retains a great deal of information about its users. This information includes photos that are automatically tagged and training images — from which biometric data is extracted. It also includes all information displayed on a Facebook profile because, as explained below, by labeling a photo, the feature generates a hyperlink to the user's profile.[30] Though Facebook collects a vast amount of data, this Article will discuss only data that is related to face recognition technology.

The user supplies much of the information on a Facebook profile. Initially, Facebook requires a new user to provide her "name, email address, birthday, and gender."[31] Though not required, the user is also prompted to provide her religious beliefs, political views, and sexual orientation.[32] As the user goes through the process of "friending" other users — who may already be her friends, classmates, family, or colleagues offline — Facebook also retains a list of those "friends."[33] More recently, Facebook has begun asking users to describe their relationship to their friends.[34] A vast amount of communication between a user and her friends is also retained as a user makes "status updates," comments on friends' "walls," sends private messages, or chats in real time.[35]

Facebook further collects photos uploaded by users or their friends, as well as information about facial features when the users

---

com/docs/webcast/acquisti-face-BH-Webinar-2012-out.pdf; Leena Rao, *Google Acquires Facial Recognition Software Company PittPatt*, TECHCRUNCH (July 22, 2011), http://techcrunch.com/2011/07/22/google-acquires-facial-recognition-software-company-pittpatt.

29. Mitchell, *supra* note 9.

30. *See Facebook Data Use Policy: Information We Receive About You*, FACEBOOK, https://www.facebook.com/about/privacy/your-info#inforeceived (last visited Dec. 22, 2012) [hereinafter *Facebook Data Use Policy*]; *See also Hearing on What Facial Recognition Technology Means for Privacy and Civil Liberties Before the Subcomm. on Privacy, Tech., & the Law of the S. Comm. on the Judiciary,* 112th Cong. 3 (2012) (statement of Robert Sherman, Manager, Privacy and Public Policy, Facebook) (explaining that photo tagging "allows users to instantaneously link photos from birthdays, vacations, and other important events with the people who participated"), *available at* http://www.judiciary.senate.gov/pdf/12-7-18ShermanTestimony.pdf.

31. *Facebook Data Use Policy*, *supra* note 30.

32. *See* E. A. Vander Veer, FACEBOOK: THE MISSING MANUAL 13–14 (Dawn Mann and Nellie McKesson eds., 3rd ed. 2011).

33. *Id.* at 46.

34. Blake Ross, *Improved Friend Lists*, THE FACEBOOK BLOG (Sept. 13, 2011, 9:59AM), https://blog.facebook.com/blog.php?post=10150278932602131.

35. *See* Vander Veer, *supra* note 32 at 69–81.

identify ("tag") themselves or others in uploaded photos.[36] Facebook's photo collection contained around 220 billion photos by October 2012 and increases by up to 300 million photos per day.[37] These photos are further tagged at a rate of 100 million labels per day.[38] The sheer size of this massive annotated photo library cannot be overstated.

The uploaded photos may also provide Facebook with metadata, including the "time, date, and place" of a photo.[39] Moreover, if a user uploads a photo from a mobile phone, Facebook may also know the user's physical location at that instant.[40] Thus, if Photo Tag Suggest were applied to identify various individuals in photos uploaded from mobile phones, Facebook could effectively also have those individuals' physical locations.[41]

Some of the personal information retained by Facebook is displayed on a user's profile and is visible to other users by default, unless the user changes her privacy settings to specify whether the information should be visible to "friends only" or only to specific individuals.[42] The user may even limit access to certain information only to herself — for example, in order to create a private photo album online or to avoid sharing her email address, which she cannot delete from Facebook.[43] Many users, however, do not understand or use these privacy settings.[44]

Facebook's Photo Tag Suggest implicates all of the personal information in a user's profile because it connects facial features detected in newly uploaded photos to that user's profile with a hyperlink. Users manually tag a person in uploaded photos by marking a square around the person's face and providing the person's name.[45] Once a

---

36. *Facebook Data Use Policy*, *supra* note 30.

37. Robert Andrews, *Facebook has 220 Billion of Your Photos to Put on Ice*, GIGAOM, Oct. 17, 2012, http://gigaom.com/cloud/facebook-has-220-billion-of-your-photos-to-put-on-ice; *Hearing on What Facial Recognition Technology Means*, *supra* note 30.

38. Mitchell, *supra* note 9.

39. *Facebook Data Use Policy*, *supra* note 30.

40. *Id.* Facebook may get this information as a geotag uploaded with the photo, containing its exact latitude and longitude. Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES, Aug. 12, 2010 at B6.

41. *Id.*

42. *See Facebook Data Use Policy: Sharing and Finding You on Facebook*, FACEBOOK, https://www.facebook.com/about/privacy/your-info-on-fb#controlpost (last visited Dec. 22, 2012).

43. *See generally* FACEBOOK, www.facebook.com (Facebook's account settings do not permit a user to delete her primary email address from her account.).

44. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook* 12, Presented at Proceedings of Privacy Enhancing Technologies Workshop (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf ("[A]mong current members, 30% claim not to know whether [Facebook] grants any way to manage who can search for and find their profile, or think that they are given no such control.").

45. *See* Vander Veer, *supra* note 32, at 166–67.

person is tagged, her name appears when a user hovers with the mouse over the tagged face in the photo.[46] Photo Tag Suggest also lists the tagged person's name next to the photo as a hyperlink to the person's profile if she has a Facebook account.[47] That profile may contain personal information, including e-mail address, phone number, birthday, gender, religious beliefs, political views, sexual orientation, and countless personal status updates.[48] The information in a user's profile may or may not be visible to a person clicking on the hyperlink depending on the selected privacy settings.[49] And unless a user specifically opts out of being automatically identified in photos, Facebook uses tagged photos of that user as training images to identify the user in newly uploaded photos.[50] Having identified the user, Facebook then suggests to the person uploading the photo that she tag the identified user in the photo, which results in a new hyperlink to the identified user's profile.[51] Photo Tag Suggest leverages not only Facebook's vast database of photos, but also user willingness to label the photos for fun.

From Facebook's Data Use Policy, it appears that Facebook uses all tagged photos of an individual as training images without distinguishing photos that the user only makes available to certain friends through her privacy settings.[52] This means that if a user restricts access to a photo so that it is only visible to her family, Facebook may nevertheless extract biometric data from it and use it with Photo Tag Suggest to allow her other Facebook friends to identify her in new photos.

Photo Tag Suggest's alleged restriction that only a user's friends can use it to automatically identify her in photos does not necessarily protect the user from abuse by automatic face recognition. In authoritarian countries, in particular, commentators have reported instances of dissidents being tortured to disclose their social network passwords.[53] Government officials can then gain access to a dissident's Facebook account to interact with other dissidents and subsequently, tap into dissident plans. Even in democracies, users cannot trust their social network friends given that schools, colleges, and future employers have started demanding user passwords to screen future em-

46. *See id.*

47. Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (June 30, 2011, 8:16 PM), http://blog.facebook.com/blog.php?post=467145887130.

48. *Facebook Data Use Policy: Information We Receive About You*, *supra* note 30.

49. *Id.*

50. *See id.*

51. *See id.*

52. *See generally id.* (describing how Facebook uses data collected from users).

53. Adrian Blomfield, *Syria 'Tortures Activists to Access Their Facebook Pages,'* TELEGRAPH (May 9, 2011, 10:26 PM), http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8503797/Syria-tortures-activists-to-access-their-Facebook-pages.html.

ployees and monitor students.[54] And for users who have some social network friends that they do not personally know offline, there is a risk that those friends are actually "socialbots."[55] A socialbot is software that is designed to behave like a human user and connect with users to gather their personal information.[56] Thus, for example, if a socialbot operator can get access to hundreds of college student profiles, the operator could use face recognition technology to identify those students on campus and use elements of their offline and online activities to create elaborate identity theft schemes.[57] Although there are laws that already prohibit that type of identity theft,[58] users still

54. *See, e.g.*, *ACLU-MN Files Lawsuit Against Minnewaska Area Schools*, AMERICAN CIVIL LIBERTIES UNION OF MINNESOTA (Mar. 6, 2012), http://www.aclu-mn.org/news/2012/03/06/aclu-mn-files-lawsuit-against-minnewaska-area-schools (noting that a school in Minnesota forced student to disclose Facebook password); Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants' Facebook Passwords*, NBCNEWS.COM (Mar. 6, 2012, 6:13 AM), http://redtape.msnbc.msn.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords (stating that applicants for Maryland government positions were asked to log onto Facebook during interviews and show friends' private profile information); Jacqui Cheng, *Bozeman Apologizes, Backs Down over Facebook Login Request*, ARS TECHNICA (June 23, 2009, 5:32 PM), http://arstechnica.com/web/news/2009/06/bozeman-apologizes-backs-down-over-facebook-login-request.ars (stating that a Montana city required all applicants for city positions to provide their social network passwords). However, several states, including Maryland, California, and Illinois, have recently passed legislation prohibiting future employers and universities from demanding social network passwords. Md. Lab. & Empl. Code § 3–712; Cal. Lab. Code § 980; Cal. Ed. Code §§ 99120-99121; Ill. Public Act 097-0875.

55. *See* Yazan Boshmaf et al., *The Socialbot Network: When Bots Socialize for Fame and Money*, *in* PROC. OF THE 27TH ANN. COMPUTER SECURITY APPLICATIONS CONF. 2011 93, 93 (2011), http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1; *Cyber Threats*, NETWORKED SYSTEMS LABORATORY, http://netsyslab.ece.ubc.ca/wiki/index.php/Cyber_Threats (last modified July 13, 2012).

56. Boshmaf et al., *supra* note 55, at 93; John P. Mello Jr., *"Socialbots" Invade Facebook: Cull 250GB of Private Data*, PCWORLD (Nov. 2, 2011, 2:20 PM), http://www.pcworld.com/article/243055/socialbots_invade_facebook_cull_250gb_of_private_data.html.

57. *See* David D. Clark & Susan Landau, *Untangling Attribution*, *in* PROC. OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POL'Y 25, 29 (2010), *available at* http://www.cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf; *see also* Ashkan Soltani, *Face Palm*, ASHKANSOLTANI.ORG, http://ashkansoltani.org/docs/face_palm.html (last visited Dec. 22, 2012).

58. There are a number of state laws that specifically apply to identity fraud based on biometric data. *See, e.g.*, CAL. PENAL CODE §§ 530.5(a) & 530.55(b) (2011) ("Every person who willfully obtains personal identifying information, [including unique biometric data such as facial scan identifiers], and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense . . . ."); CONN. GEN. STAT. ANN. § 53a–129a (2011) ("A person commits identity theft when such person knowingly uses personal identifying information of another person [including unique biometric data] to obtain or attempt to obtain . . . money, credit, goods, services, property or medical information without the consent of such other person."); IOWA CODE § 715A.8 (2005) ("A person commits the offense of identity theft if the person, [including biometric identifier,] with the intent to obtain a benefit fraudulently obtains identification information of another person . . . ."); TENN. CODE § 39-14-150 (2012) ("A person commits the offense of identity

have the right to be put on notice of the added risks with face recognition technology so that they may take precautions. In practice, a person who uses Photo Tag Suggest may not actually know the Facebook user whom she identifies. There is a risk of misidentification that would attribute certain activities to the wrong user.[59] The misidentified user would not necessarily be put on notice of the misidentification — for example, if the other user does not complete the tagging process so that no hyperlink to the misidentified user's profile is generated. As a result, the misidentified user would not be able to correct the misidentification, while the other user may assume that the automatic identification is particularly accurate because there is no risk of human error.[60] But in fact, there *is* potential for human error given that identification uses tags previously generated by Facebook users.

C. From an Anonymous Face in the Street to a Facebook Profile

In 2011, privacy researchers at Carnegie Mellon University ("CMU") presented a study of face recognition technology that "show[s] that it is possible to start from an anonymous face in the street, and end up with very sensitive information about that person."[61] This study exemplifies how the vast amount of data in social networks can be misused to essentially place a nametag on each individual as she walks around in public — a nametag with a link to all her online activities no less. Much like in the above hypothetical on socialbots, the CMU researchers took three photos of college students on campus and matched them against Facebook photos.[62] However, they used only those photos that could be viewed on Facebook with-

---

theft who knowingly obtains, possesses, buys, or uses, the personal identifying information of another [including unique biometric data]: (A) With the intent to commit any unlawful act including, but not limited to, obtaining or attempting to obtain credit, goods, services or medical information in the name of such other person; and (B)(i) Without the consent of such other person; or (ii) Without the lawful authority to obtain, possess, buy or use that identifying information.").

59. Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology, A Survey of Policy and Implementation Issues*, CTR. FOR CATASTROPHE PREPAREDNESS AND RESPONSE AT N.Y.U. 15 (Apr. 8, 2009), *available at* http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf (discussing how one may determine "the social cost of misidentifying someone in a particular context or the financial costs of granting access based on misidentification" when using face recognition technology).

60. *Id.* at 41 (explaining how face recognition technology could "create a situation where system recognition risks (mistakes) are disproportionately experienced by a specific group based on gender, race, age, etc. [which becomes problematic] . . . . when the assumption is made, as it is often the case, that technology is neutral in its decision making process").

61. Alessandro Acquisti, Ralph Gross & Fred Stutzman, *Face Recognition Study — FAQ*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ (last visited Dec. 22, 2012).

62. *See* Acquisti, *supra* note 28, at 39.

out logging in.[63] They further did not use Facebook's Photo Tag Suggest, but instead applied publicly available face recognition technology.[64] When combining these two resources, they were able to identify nearly one out of three participants in only a few seconds.[65] The researchers could even identify one participant — who did not have a Facebook profile picture — because he was tagged in his friends' publicly available photos.[66]

The CMU study is basically "a proof-of-concept [of an] iPhone application that can snap a photo of a person and within seconds display their name, date of birth and social security number."[67] But on March 7, 2012, Face.com — the company that provided the technology behind Facebook's Photo Tag Suggest and recently was acquired by Facebook — released an iPhone application with similar capabilities.[68] This application, called "KLIK," identified users' friends in real time as users took photos of them with their camera phones.[69] KLIK automatically tagged the photos, which could then be uploaded to Facebook or just stored on the iPhone.[70] The application, however, had some security flaws that allowed anyone to hack other user accounts to be able to identify their Facebook friends in real time.[71] After Facebook acquired Face.com, KLIK was promptly withdrawn from the App Store.[72] But given that KLIK used data previously collected by Facebook, it showed the danger of mere collection and storage of personal information: even if the original collection may be harmless, the data always can be used later in a manner that is contrary to user expectations.[73]

---

63. *Id.* at 15, 44.

64. *See id.* at 5, 14, 27, 31.

65. *Id*. at 30.

66. *See id.*

67. David Goldman, *In the Future, Can You Remain Anonymous?*, CNN MONEY (Jan. 13, 2012, 6:22 AM), http://money.cnn.com/2012/01/13/technology/face_recognition/index.htm?iid=EL.

68. *See Awesome News — Facebook Acquires Face.com*, FACE.COM (June 18, 2012), http://face.com/blog/facebook-acquires-face-com/; David Goldman, *Real-time Face Recognition Comes to Your iPhone Camera*, CNN MONEY (Mar. 12, 2012, 11:13 AM), http://money.cnn.com/2012/03/12/technology/iPhone-face-recognition/index.htm.

69. *See* Goldman, *supra* note 68.

70. *Id.*

71. *See* Soltani, *supra* note 57 ("Face.com essentially allowed *anyone* to hijack a KLIK user's Facebook and Twitter accounts to get access to photos and social graph (which enables 'face prints'), even if that information isn't public." (emphasis in original)).

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

73. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 232 (2008) ("[P]eople might make rational decisions about sharing their personal information in the short term, but underestimate what might happen to that information as it is indexed, reused, and repurposed by strangers.").

III. THEORETICAL FOUNDATION FOR A FACE RECOGNITION PRIVACY LAW

My first inquiry is whether and how the use of face recognition technology in social networks threatens privacy. Looking only to various privacy laws will not address this issue because the law has not kept up with information flows in social networks and cutting-edge face recognition technology. Even if the law were up to speed with the current technologies, it may not tell us what privacy interests ought to be protected, as it tends to reflect various political compromises.[74] These compromises are particularly skewed in privacy laws because privacy is often balanced against interests that are much more concrete.[75] Furthermore, as I explain below when exploring state laws with respect to biometric data, sometimes even applicable laws do not effectively regulate behavior due to the lack of effective enforcement. Therefore, to assess whether the law adequately protects privacy in this context, we need to establish some frame of reference that is independent of the current law. We need a conceptual understanding of what privacy interests are at play.

I analyze the privacy implications of face recognition technology in social networks by applying Professor Helen Nissenbaum's theory of contextual integrity. In so doing, I break from several traditional conceptualizations of privacy.[76] These conceptualizations appear unsuitable for analyzing the technologies at issue. To show why Professor Nissenbaum's theory is particularly appropriate in this context, I begin this section with a brief survey of the five privacy theories that I find to be less applicable: namely, (1) the right to be let alone; (2) theories based on limited accessibility and secrecy; (3) the right to control personal information; (4) the individuality theory; and (5) the pragmatic approach to privacy. After discussing why these theories are ill-suited for my analysis, I outline the contextual integrity theory and apply it to the problem at hand to establish that face recognition technology in social networks in fact violates privacy. Finally, I counter the identified privacy concern with the interest in protecting the

---

74. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 39 (2008).

75. LESSIG, *supra* note 7, at 200–01 ("[W]ith privacy, the interests threatened are diffuse and disorganized, ... [while] the values on the other side of protection (security, the war against terrorism) *are* compelling and well understood." (emphasis in original)); *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 7 (2008) ("The interests on the other side [of privacy] — free speech, efficient consumer transactions, and security — are often much more readily articulated.") [hereinafter SOLOVE, UNDERSTANDING PRIVACY].

76. Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1095 (2002) (describing as "traditional" a number of privacy theories that have sought to "articulate what separates privacy from other things, what makes it unique, and what identifies it in its various manifestations") [hereinafter Solove, *Conceptualizing Privacy*].

flexible features of the Internet that invite innovation — something that I believe any protection of online privacy ought to take into account.

A. Only Bedrooms and Secrets Used To Be Private

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[77]

So wrote Samuel Warren and Louis Brandeis in 1890, clearly agonizing about the possible invasion into the "domestic life" in private homes — metaphorically described as "the closet." The "devices" they were worried about likely included inventions such as Kodak's 1884 handheld "snap cameras."[78] Marketed with the slogan "You press the button, we do the rest,"[79] these cameras were dubbed the "chief enemy of privacy in modern life" by one prominent commentator at the time.[80] In response to the rapid developments in norms and technology, Warren and Brandeis proposed a "right 'to be let alone,'" quoting Judge Thomas McIntyre Cooley.[81] Decades later, then-Justice Brandeis applied this right in Olmstead v. United States, dissenting from the majority view that wiretapping did not violate the Fourth Amendment because there was no physical invasion of the home.[82] Arguing that "[i]t is . . . immaterial where the physical connection with the telephone wires leading into the defendants' premises was made,"[83] Justice Brandeis wrote that:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought

77. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

78. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 57 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

79. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 108 (2007) [hereinafter SOLOVE, FUTURE OF REPUTATION].

80. *Id.* at 107–08 (quoting E. L. Godkin).

81. Warren & Brandeis, *supra* note 77, at 195.

82. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

83. *Id.* at 479.

> to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men.[84]

Justice Brandeis' dissent in Olmstead, as well as subsequent case law,[85] extended the scope of privacy protection beyond the four walls of the home. But the vague notion that privacy only protects truly "private spaces" remained.[86]

Over the years, courts and scholars have elaborated on the scope of the right to be let alone.[87] Nevertheless, Professor Ruth Gavison argues that the scope of the right remains frustratingly limited because it "excludes from the realm of privacy all claims that have nothing to do with [certain] highly personal decisions, such as an individual's unwillingness to have a file in a central data-bank," to pay taxes, or to join the army.[88] Nor would the right to be let alone cover those who do not want to be listed in a *biometric* database.

More problematically for our analysis, this right primarily applies "as against the government."[89] But privacy claims arising out of the use of face recognition technology in social networks would probably be invoked either against a social network or fellow users of that network. Certainly, in most cases, there would be no claims against the government.[90] Instead, we need a theory that can address widespread user sharing of photos with their friends — who may be a very large group of individuals dispersed around the world. Still more problematic, with social networks we primarily do not worry about information that is "whispered in the closet."

---

84. *Id.* at 478.

85. *See, e.g.*, Katz v. United States, 389 U.S. 347, 358–59 (1967) (holding that wiretapping violates an individual's reasonable expectation of privacy); Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (holding that the reasonable expectation of privacy precludes the use of a thermal imaging device to monitor the inside of a home from the outside).

86. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 110; *see also* LESSIG, *supra* note 7, at 201.

87. *See, e.g.*, Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 433, 436–38 (1980).

88. *Id.* at 437–38.

89. Olmstead v. U.S., 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

90. *See, e.g.*, Gavison, *supra* note 87, at 439 ("[T]he typical privacy claim is not a claim for noninterference by the state at all."); Ryan Budish, Note, *In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1873, 1881–82 (2007) (pointing out that "with the exception of Professor Jonathan Zittrain, legal scholars have missed the greatest threat to modern privacy: ourselves.").

1. The Accessibility and Secrecy Theories

While criticizing the right to be let alone, Professor Gavison advocates for another privacy theory, which can be described as "concern over our accessibility to others."[91] Though fairly similar to the right to be let alone, this accessibility theory is more specific in scope as it is based on the protection of three particular elements: "secrecy, anonymity, and solitude."[92] Professor Daniel Solove has criticized these elements as mostly inapplicable to the "collection, storage, and computerization of information."[93] If Solove were correct about this inapplicability, the theory would also not apply to issues involving biometric databases. But as I discuss below, the collection and aggregation of biometric data certainly affects our ability to remain anonymous in public — arguably implicating the anonymity element.[94] However, the accessibility theory is nevertheless problematic for face recognition technology in social networks because it only discusses collection and aggregation of *secret* information. It does not discuss aggregation of non-secret information to de-anonymize individuals.[95] In so doing, this theory adopts Judge Richard Posner's earlier conceptualization of privacy as secrecy and "concealment of information."[96] Like the accessibility theory, the secrecy theory also fails to encompass photos shared with hundreds of friends in a social network.

2. The Control Theory

Professor Charles Fried has further modified the secrecy theory by arguing that "[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the control we have over information about ourselves."[97] Control over the information that we share is essential to social relationships.[98] We establish intimate relationships of love and friendship by sharing our "actions, beliefs, or emotions" with particular individuals.[99] Broadly, this privacy theory could apply to the sharing of photos with a close circle of friends to establish a certain degree of intimacy. But writing decades before the first social networks — which have come to blur the public and pri-

91. Gavison, *supra* note 87, at 428–36.
92. *Id.* at 433.
93. Solove, *Conceptualizing Privacy*, *supra* note 76, at 1105 (arguing that "the collection, storage, and computerization of information . . . often do not reveal secrets, destroy anonymity, or thwart solitude." (internal quotations and citations omitted)).
94. *See supra* Part IV.E.
95. Gavison, *supra* note 87, at 429–31.
96. Richard Posner, THE ECONOMICS OF JUSTICE 231–33 (1983).
97. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (emphasis in original).
98. *Id.* at 485.
99. *Id.* at 484.

vate distinction — Professor Fried argued that "the control over privacy must be limited by the rights of others," and "the more one ventures into the outside . . . the more one must risk invasions of priprivacy."[100] This theory of privacy as "control over information" thus suggests that users who share photos in social networks venture so far out in public that they must accept the risk of losing control over the information in those photos, including their biometric data. Yet studies have shown that people consider the information they post in social networks as private in the sense that they may not want to share it with certain people.[101] Accordingly, we need a privacy theory that can address individual desire for privacy despite widespread sharing of information with friends. This very recent problem calls for a contemporary understanding of privacy.

3. The Individuality Theory

Perhaps least applicable to face recognition technology in social networks is Professor Edward Bloustein's conceptualization of privacy as protection of "individuality" and "personal dignity."[102] The Supreme Court has applied this theory in cases regarding "marriage, procreation, contraception, family relationships, and child rearing."[103] But the everyday posting of photos in social networks likely does not relate to this formulation of individuality, which appears to be more concerned about protecting an individual's life-defining choices.

4. The Pragmatic Theory

In contrast to the traditional privacy theories discussed above, Professor Solove has proposed a "pragmatic approach" to privacy that rejects the idea that privacy can be defined as a single concept suitable for diverse contexts.[104] Criticizing many other privacy theories for trying to analyze privacy in the abstract, he argues that it should be theorized "bottom up" by identifying an undesirable disruption of a socially valuable practice.[105] To Professor Solove, privacy does not

100. *Id.* at 486.

101. danah boyd, The Future of Privacy: How Privacy Norms Can Inform Regulation, Address at the International Conference of Data Protection Commissioners (Oct. 29, 2010) [hereinafter boyd, The Future of Privacy], *available at* http://www.danah.org/papers/talks/2010/PrivacyGenerations.html.

102. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 973 (1964).

103. Solove, *Conceptualizing Privacy*, *supra* note 76, at 1117.

104. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 10; Solove, *Conceptualizing Privacy*, *supra* note 76, at 1091–92.

105. *Id.* at 1091–92, 1129–30.

have an intrinsic value.[106] Rather, it serves to promote other values, such as "self-creation, independence, autonomy, creativity, imagination, counter-culture, freedom of thought, and reputation."[107] His theory is helpful for dealing with new technologies because it is not based on traditional theories of private space or secret information. Yet applying it to face recognition technology in social networks is nevertheless problematic because it requires us to make assumptions without a clear theoretical framework. Pursuant to the pragmatic theory, one could argue that face recognition technology violates privacy because it disrupts the socially valuable practice of online socializing. Arguably, the technology disrupts this practice by exposing users to various risks and by having a chilling effect on the sharing of experiences with friends. But this reasoning appears circular because in order to analyze whether there is a privacy violation, we need first to assume that social networks are valuable and face recognition technology is disruptive. The assumptions may seem intuitive, but how do we choose it over the inverse: that the technology is valuable (because it helps us to remember our contacts) and the social networks actually disrupt that practice by connecting an automatically generated tag to aggregated personal information on a user's profile?[108] The pragmatic approach does not yet seem to offer a clear formula for how we should make these underlying assumptions with respect to novel technologies.

B. "Traditional Privacy" Is Dead; Long Live "Contextual Integrity"

As I discuss in the previous section, applying traditional theories of privacy to social networks and other online platforms frequently results in a mismatch. Some theories seek to protect private spaces like one's home.[109] But there are no such spaces online. Other theories focus on secrets[110] — but in social networks individuals voluntarily share information with hundreds of friends every day, some of whom they have never met in person. Does this mean that privacy is dead or

106. *Id.* at 1145.

107. *Id.* at 1145–46.

108. *See, e.g.*, Budish, *supra* note 90, at 1874 ("Images flood the Web because it is so easy and cheap to publish photos, but it is the ability to sift through this sea of data that threatens to erase the boundary people so carefully construct between their public and private lives.").

109. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 110 (discussing Kyllo v. U.S., 533 U.S. 27 (2001), in which the United States Supreme Court concluded that the Fourth Amendment protected a person's home from unauthorized search from thermal imaging devices); *see also* LESSIG, *supra* note 7, at 201.

110. *See* SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 21–24.

simply taking a different form?[111] While sharing information online with hundreds of friends, an individual may have a sense that this information is, nevertheless, very personal. The individual may not want her employer to read it. She may not want it to be accessible to certain government entities. And she may not want a stranger to get a first impression of her solely based on this information.

Professor Nissenbaum addresses user online privacy practices in her theory of contextual integrity.[112] Departing from the traditional distinction between private and public information, she focuses instead on the context in which the information is shared and the norms governing that context.[113] She thus analyzes online flows of information, both private and public, by:

> (1) Determining the relevant "context" of the particular flow;
>
> (2) Identifying the parties to the flow, including the "sender," the "recipient," and the "subject" of the information;
>
> (3) Identifying the nature of the information, by considering the different information types involved in the flow;
>
> (4) Identifying the relevant "transmission principles";
>
> (5) Based on these factors, determining the applicable "informational norms" that have developed in an analogous context offline and applying the norms to the informational flow.[114]

This analysis relies on prescriptive norms of how information ought to flow, which individuals follow because of a sense of societal expectations.[115] An information flow that does not follow the norms for the relevant context violates contextual integrity, resulting in a

111. *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

112. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2009) [hereinafter NISSENBAUM, PRIVACY IN CONTEXT].

113. *See id.* at 125–6.

114. *Id.* at 149–150. Professor Nissenbaum writes about the nature of the information as "attributes" of the information. *Id.* at 149.

115. *Id.* at 138.

privacy violation.[116] In particular, a flow is presumed to violate privacy if it changes the nature of the information or its transmission principles or makes the information available to additional parties.[117] This presumption can be overruled only if the change is "morally or politically superior" to the old norms.[118] A change may be superior if it positively affects an important concern for the society, such as "autonomy and freedom[,] . . . power structures[,] . . . justice, fairness, equality, social hierarchy, [and] democracy."[119] And even if a change benefits some of these concerns, those benefits should be weighed against the interests of the relevant context.[120]

The introduction of the E-ZPass, for example, expanded the number of *recipients* of information about our travels from only the toll road personnel to E-ZPass employees at remote locations and the DMV.[121] E-ZPasses arguably also changed the *nature* of the information by recording a car's location, which could, for example, show that the car has been driving too fast.[122] For now, drivers still have the option to pay cash.[123] But were that option completely eliminated such that travel information had to be transmitted to the DMV and other third parties, that would change the rules for how the information is transmitted, which is what Professor Nissenbaum calls a change in "*transmission principles*."[124]

Given that a violating flow can pertain to information that would traditionally be considered public — such as a blog post — Professor Nissenbaum uses the term "privacy" only because it historically has been invoked to characterize disruptions of informational norms.[125] So, while privacy, as we once knew it, may be dead or outdated, it has been reincarnated as "contextual integrity."

It is also important to note that some online applications do not have a "brick-and-mortar precursor" that can provide the relevant informational norms for this contextual analysis.[126] This is the case with social networks, search engines, and other platforms that integrate products with user-generated content.[127] When there are no existing

116. *See id.* at 10 (discussing how the theory of contextual integrity can help determining whether particular technologies violate individuals' privacy).

117. *Id.* at 150 (noting that these changes should result in a "[r]ed flag").

118. *Id.* at 165.

119. *Id.* at 182.

120. *See id.*

121. *See* Ross Kenneth Urken, *Is The E-ZPass Box A Trojan Horse For Privacy Invasions?*, AOL (June 27, 2011), http://autos.aol.com/article/e-zpass-privacy-invasion.

122. *See id.*

123. *Id*.

124. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 149–50 (emphasis added).

125. *Id.* at 4.

126. Nissenbaum, *Contextual Approach*, *supra* note 8, at 39.

127. *Id.* at 39.

norms, Professor Nissenbaum suggests that we consider the "underlying standards, derived from general moral and political considerations as well as the ends, purposes, and values of respective contexts."[128] Social networks, for example, can be analyzed by considering their purposes — such as social interaction, political engagement, or professional networking.[129]

C. How the Use of Face Recognition Technology in Social Networks Violates Contextual Integrity

If we think of posting photos on Facebook primarily as social interaction, we could analogize this practice to someone showing a photo album from a recent trip to a few friends over coffee. Extraction of biometric data then would be analogous to one of my friends secretly snapping photos of my album with his camera and forwarding them to a third party, who in turn uses them to identify me in other contexts. When analogizing to an offline situation, we can see clearly that such behavior would violate the social norms governing my coffee session. I would be showing pictures only to share my travel experiences with my friends, but the information would be used to identify me in a completely different context without my knowledge.

The same is true in the online context. If I were to post a photo on my Facebook wall of myself from a recent trip, I could expect my friends to "like" it or maybe comment on it. But I would not expect them to share it with others in a private Facebook group in which I am not a member. I would also not expect them to share it on their walls and limit their privacy settings such that I could not see my own photo being shared. In other words, the social norms governing sharing photos with friends translate rather well into the online environment — at least as between social network users.

Assuming that the context of posting photos on Facebook can be analogized to sharing photos with friends, Facebook's Photo Tag Suggest can be said to violate the existing social norms because

> (1) Facebook changes the *nature of the information* from a photo that cannot necessarily be used to recognize the user in other photos to biometric data that allows someone who does not know that user to identify her with varying degrees of accuracy.

---

128. *Id.* at 40.

129. *Id.* at 43 (noting that "[t]ime spent on social networks, such as Facebook, is an amalgam of engagement with personal, social, intimate and home life, political association, and professional or work life.").

> (2) Facebook introduces *new recipients* to the information flow beyond the recipients that the user selects when posting a photo on Facebook. The user intends to share the photo with the limited number of friends that she specifies in her privacy settings for that particular photo, whereas Photo Tag Suggest extracts biometric data and makes it available to all of her Facebook contacts who may choose to automatically identify her in new photos.
>
> (3) Facebook changes the *transmission principle* from one where the user can delete all her photos and tags of her so that others cannot find her on Facebook to a situation where her personally identifiable information is stored in a biometric database beyond her control. In fact, the recent introduction of KLIK, which automatically identified users in real time, shows how little control users have over their biometric data in Facebook.[130]

By altering the nature of the information users share, the number of recipients that have access to this information, and the transmission principles governing the information, the Photo Tag Suggest presents "a prima facie violation of [users'] contextual integrity."[131] The stated value of the Photo Tag Suggest is to allow "users [to] more efficiently tag their friends in photos."[132] It does not appear to serve any of the important social concerns that can sometimes overcome a presumed contextual integrity violation.[133]

I apply Professor Nissenbaum's theory of contextual integrity only to identify the privacy violation that arises out of the combination of these technologies. According to her theory, the solution in most cases is to categorically avoid any violating flows.[134] While this solution is wise in many situations — particularly when dealing with strictly noncommercial online uses, like Wikipedia and OpenStreetMap — here, I offer a more nuanced solution tailored specifically to face recognition technology in social networks. As I explain below, I believe this multifaceted solution is appropriate to avoid unduly burdening the development of these technologies by prohibiting their use altogether. My analysis is consistent with Professor Nissen-

130. *Cf.* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 141–43, 149–50.
131. *Id.* at 150 (describing "a prima facie violation of contextual integrity").
132. *Hearing on What Facial Recognition Technology Means*, *supra* note 30.
133. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 182.
134. *See* Nissenbaum, *Contextual Approach*, *supra* note 8, at 45.

baum's theory because she has also suggested that specific solutions — such as a particular notice and consent model — may be more appropriate for face recognition technology that connects a face to other information in a database.[135]

D. Balancing Privacy Protection with Online Innovation

One salient aspect of privacy protection is that it tends to be balanced against other important interests such as national security, freedom of speech, and innovation.[136] Online innovation is the one interest mainly implicated when regulating social networks.[137] To give one example: a common privacy problem with social networks is that they constantly alter how they use personal information.[138] One day, user photo tags are mere annotations to photos. The next day, they are used to extract users' biometric data to find them in new photos. While this may be a disturbing development for users who feel that they have no control over their photos, it also reflects social networks' rapid innovation.[139] Mark Zuckerberg, Facebook's young CEO, considers this to be a feature of the "Hacker Way," which "is an approach to building that involves continuous improvement and iteration."[140] Given this building method, if privacy regulations were to require Facebook to provide notices of every change months in advance, it would probably severely limit Facebook's ability to develop new services in exchange for a limited benefit of greater predictability.[141]

The potential constraint on today's Facebook tells only half the story — privacy regulations could have a far more devastating effect on innovation in smaller companies. Much innovation in the information age comes not from already established companies, like Facebook or Google, but from small startups and other "outsiders" that do

---

135. *See* Introna & Nissenbaum, *supra* note 59, at 44; *see also* Nissenbaum, *Contextual Approach*, *supra* note 8, at 45 (after making "explicit" pre-existing social norms, "plenty of room would still remain to express personal preferences and to maintain a robust role for informed consent").

136. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 7–8.

137. As social networks are intermediaries, most of their material would not be considered to be their "speech." One court has even found that users' expression of opinion when "liking" something on Facebook does not qualify as "speech." Bland v. Roberts, No. 4:11cv45, 2012 WL 1428198, at *3 (E.D. Va. Apr. 24, 2012).

138. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1168–69 (2009).

139. *See id.* at 1145–46.

140. Facebook, Inc., Registration Statement (Form S-1), at 69 (Feb. 1, 2012), *available at* http://battellemedia.com/wp-content/uploads/2012/02/Facebook-S-1.pdf.

141. *Cf.* Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED, no. 7, 2010, at 155, 156, 161–62 (discussing how an stringent notice and consent requirements could have prevented Google's development of the Google Flu Trends), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp.

not get a paycheck to come up with new solutions.[142] Indeed, the most innovative aspects of Facebook as a socializing platform were implemented in its early days by a college student.[143] This is because the Internet offers a platform for projects that require very little capital investment — thus lowering the barriers to entry.[144] Developers can build their projects in the so-called "'application layer'" of the Internet, on top of its physical infrastructure, without complete comprehension of every aspect of the network.[145] And because it is an open platform, it encourages users to play with the technology, which in turn may lead to innovation.[146] Online innovators often do not have funds to defend against litigation and are therefore wary of particularly regulated markets where the threat of lawsuits is high.[147] In short, any privacy regulation needs to avoid creating a litigious environment that deters innovation and instead preserve the flexible qualities of the Internet that foster experimentation.[148]

I now turn to how regulation of face recognition technology could potentially impact innovation. Obviously, a blanket prohibition of face recognition technology would prevent the use and further development of an innovative technology. Cameras use automatic face recognition technology to focus lenses on a face.[149] With recent advancements in technology, users can now fully take advantage of the vast memory capacity of their digital cameras by taking countless photos and sorting them online.[150] The use of this technology in social networks further creates or strengthens social connections between friends. If I were to upload photos from a party and automatically find and tag my friends in those photos via Photo Tag Suggest,[151] they

142. *See* Jim Shimabukuro, *e-G8 — Lawrence Lessig: "Outsider Innovation Threatens the Incumbent,"* EDU. TECH. & CHANGE J. (June 8, 2011), http://etcjournal.com/2011/06/08/8927.

143. *See* Nicholas Carlson, *At Last — The Full Story of How Facebook Was Founded*, BUSINESS INSIDER (Mar. 5, 2010, 4:10 AM), http://www.businessinsider.com/how-facebook-was-founded-2010-3.

144. *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 6 (2006).

145. ZITTRAIN, *supra* note 73, at 67–68.

146. *See id.* at 2.

147. *See* Jason Kincaid, *imeem Founder Dalton Caldwell's Must-See Talk on the Challenges Facing Music Startups*, TECHCRUNCH (Oct. 16, 2010), http://techcrunch.com/2010/10/20/imeem-founder-dalton-caldwells-must-see-talk-on-the-challenges-facing-music-startups.

148. *See* Shimabukuro, *supra* note 142. With this Article, I do not intend to engage in the debate on the relative "innovative" potential of small startups as compared to established companies or small startups' relative impact on the economy. For the analysis in this Article, it is sufficient to observe that there is significant online innovation from smaller players, which stringent regulation could deter.

149. *See Face Detection*, SONY, http://www.sony.co.uk/hub/learnandenjoy/2/1 (last visited Dec. 22, 2012).

150. *See* Mitchell, *supra* note 9.

151. *See supra* Part II.B.

would be notified and could start chatting about the night and reliving their experiences. Also, regulating the flow of personal information in social networks could limit third-party innovation that uses social networks' open Application Programming Interface ("API") platforms.[152] To put this in context, by 2007, third-party developers had built some 5,000 applications using Facebook's API.[153] The third-party developers' ability to use the information gathered by a social network helps them offer new services without having to invest in developing their own social network. Finally, regulations could limit social networks' ability to provide new services because they are funded through advertising that relies on their users' data.[154] To avoid these and other restrictions on innovation, it is important to design regulations so that they do not completely prohibit any specific technologies or completely restrict the online flow of information.

This is the fine balance that my proposal in Part V tries to maintain. While requiring greater transparency of data use practices, my proposal would not prohibit social networks from sharing data with third-party developers and advertisers. Likewise, although I recognize that improved notice and consent requirements alone fail to offer sufficient protection, I do not invite more rigorous privacy laws. Instead, my proposal supplements the legal requirements with non-legal solutions that I believe will have a less stifling effect on innovation.[155] For example, by proposing greater reliance on data portability and network interoperability standards as well as distributed networks, my proposal gives users greater bargaining power with respect to data use. At the same time, these solutions could actually facilitate innovation.[156] The purpose here is not to exhaustively analyze whether this

---

152. Grimmelmann, *supra* note 138, at 1146–47 (discussing how Facebook's current ability to share information with third parties allows developers to create new applications on the Facebook Platform).

153. URS GASSER & JOHN PALFREY, BREAKING DOWN DIGITAL BARRIERS: WHEN AND HOW ICT INTEROPERABILITY DRIVES INNOVATION 7 (2007), *available at* http://cyber.law.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf.

154. *See* Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 3 (2009) ("[S]ome companies collect [personally identifying information], mine it for trends, and tailor marketing campaigns."); *see also* Larry Magid, *Zuckerberg Claims "We Don't Build Services to Make Money,"* FORBES (Feb. 1, 2012, 7:02 PM), http://www.forbes.com/sites/larrymagid/2012/02/01/zuckerberg-claims-we-dont-build-services-to-make-money (noting that Facebook's S1 filing states that "we don't build services to make money; we make money to build better services").

155. *See, e.g.*, Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law*, 41 GA. L. REV. 1, 11, 32, 64 (2006) (arguing that rather than applying "top-down regulation," "regulators need to develop strategies that will allow for the 'sustainable development' of the information economy" to "protect privacy without strangling technological innovation").

156. JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 90 (2012) [hereinafter PALFREY & GASSER, INTEROP].

proposal will burden innovation. Rather, it is to show why I have opted for a multifaceted regulatory model rather than proposing a legal reform that would either completely prohibit the use of face recognition technology in social networks or impose some other legal hurdles.

Of course, any privacy regulation — however well intentioned — could restrict innovation in completely unpredictable ways. Historically, heightened "regulability" of technologies has often provided platforms that limit innovative capacity.[157] Scholars have therefore warned against regulating "technolog[ies] in transition."[158] To be sure, leaving social networks completely unregulated could contribute to future innovation that we cannot even anticipate today, but it seems that the cost to privacy would be too high. Although "the Internet and Web generally thrive on lack of regulation," even the father of the Web acknowledges "some basic values have to be legally preserved."[159]

Another reason we should not leave social networks completely unregulated is that the lack of regulation could backfire if the technology were to hit a political nerve.[160] As Professors Jonathan Zittrain and Lawrence Lessig have argued, the Internet's openness and capacity for innovation can also be used for malevolent purposes.[161] If those harmful uses were to produce "the Internet's equivalent of 9/11," the political reaction would be something like the Patriot Act — an arguably drastic overreaction.[162] When it comes to privacy, the triggering event need not be quite as dramatic as 9/11 — as long as it hits close to home. For instance, after Justice Robert Bork's rather innocuous video rental records were leaked to the press during his Supreme Court nomination hearings in 1987, members of Congress realized that there was no legislation to protect them from suffering the same fate and swiftly passed the Video Privacy Protection Act ("VPPA").[163] While not nearly as disproportionate as the Patriot Act,

---

157. *See* ZITTRAIN, *supra* note 73, at 8.

158. LAWRENCE LESSIG, FREE CULTURE 303 (2004) (To avoid stifling innovation, "[w]e should instead be regulating to minimize the harm to interests affected by th[e] technological change, while enabling, and encouraging, the most efficient technology we can create.").

159. Tim Berners-Lee, *Long Live the Web: A Call for Continued Open Standards and Neutrality*, SCI. AM. (Nov. 22, 2010), *available at* http://www.scientificamerican.com/article.cfm?id=long-live-the-web; *see also* Budish, *supra* note 90, at 1891 (suggesting regulation of face recognition technology and noting that while the "fear that even the slightest intervention can have devastating impact . . . might have been justified for the Internet a decade ago, it is worth reconsidering today").

160. *See* LESSIG, *supra* note 7, at 74–80.

161. *Id.*

162. *Id.*

163. Yana Welinder, *Dodging the Thought Police: Privacy of Online Video and Other Content Under the "Bork Bill,"* HARV. J. L. & TECH. DIG. (Aug. 14, 2012, 6:11 PM), http://jolt.law.harvard.edu/digest/legislation/dodging-the-thought-police-privacy-of-online-

the VPPA is nevertheless ill conceived because it inexplicably singles out video rental records and does not protect records of library borrowing, media purchases, or other "intellectual vitamins."[164] Given that face recognition technology in social networks violates contextual integrity,[165] the combination of these technologies will continue to offend user notions of privacy. But the day the Photo Tag Suggest automatically identifies a politician's minor daughter being intimate with her boyfriend in a park, extreme legislation will likely follow. The legislative response could be a complete prohibition on face recognition technology or it could be more extreme. It will likely not be subject to a careful analysis to ensure that the resulting legislation does not unduly stifle innovation. Thus, rather than waiting for a privacy-geddon, we may want to prevent the problem with smaller trade-offs.[166]

IV. DOES AUTOMATIC FACE RECOGNITION VIOLATE CURRENT PRIVACY LAWS?

The discussion in Part III sought to illustrate the theoretical foundation for regulating face recognition technology in social networks to protect privacy. Here, I will survey existing laws to show why face recognition technology is not already sufficiently regulated. Specifically, I will review:

> (1) Section 5 of the Federal Trade Commission Act and the Children's Online Privacy Protection Act;
>
> (2) The Illinois Biometric Information Privacy Act;
>
> (3) Section 503.001 of the Texas Business and Commerce Code regulating "Capture and Use of Biometric Identifier";
>
> (4) Various bills that have been considered by the California legislature; and

---

video-and-other-content-under-the-bork-bill; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1442 (2001) [hereinafter Solove, *Privacy and Power*].

164. *See* Video Privacy Protection Act, 18 U.S.C. § 2710 (2006); *Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 and S. 2361 Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary and the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. 2 (1988) (statement of Alfred A. McCandless, California congressman) (arguing that "[b]ooks and films are the intellectual vitamins that fuel the growth of individual thought").

165. *See supra* Part III.C.

166. *See* LESSIG, *supra* note 7, at 76.

(5) The tort of seclusion.

I will show that these laws are deficient in addressing this problem. Their deficiencies will serve as the basis for my proposal in Part V.

A. Face Recognition as an Unfair and Deceptive Trade Practice Under the Federal Trade Commission Act and Children's Online Privacy Protection Act

Section 5 of the Federal Trade Commission ("FTC") Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[167] Central to this provision is the promotion of a fair and competitive market based on "informed consumer choice."[168] As I will explain, Facebook's Photo Tag Suggest may qualify as an unfair and deceptive trade practice based on the FTC's prior interpretations of Section 5. But the FTC Act generally does not provide sufficient clarity about what information and consent procedures are necessary to constitute informed consumer choice.

On June 10, 2011, the Electronic Privacy Information Center ("EPIC") asked the FTC to investigate and enjoin Facebook's face recognition technology.[169] It claimed that Facebook's online terms led users to upload photos with the expectation that they would continue to control those photos.[170] Yet Facebook then allegedly collected biometric data from user photos without their knowledge or consent and used this data to identify users in new photos.[171] EPIC argued that this was unfair and deceptive under Section 5 of the FTC Act.[172]

The FTC has previously found various Facebook practices to be unfair and deceptive.[173] For example, the FTC did not approve of changes to Facebook's site that made certain information about users publicly accessible without first getting their consent.[174] It also disap-

---

167. 15 U.S.C. § 45(a)(1) (2006).

168. *FTC Policy Statement on Unfairness*, FED. TRADE COMM'N. (1980), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

169. *See* Complaint, Facebook, Inc. and the Facial Identification of Users, No. C-4365 (Fed. Trade Comm'n June 10, 2011) [hereinafter Complaint, Facebook], *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_Complaint_06_10_11.pdf.

170. *Id.* at 32.

171. *Id.*

172. *Id.* at 1.

173. *See, e.g.*, Julia Angwin, Shayndi Raice & Spencer E. Ante, *Facebook Retreats on Privacy: Social Network Nears Settlement on Charges It Misled Users About Their Data*, WALL ST. J. (Nov. 11, 2011), http://online.wsj.com/article/SB10001424052970204224604577030383745515166.html.

174. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), http://www.ftc.gov/opa/2011/11/privacysettlement.shtm.

proved of Facebook giving third-party applications access to nearly all users' data after promising those users that it would only share the data that was needed to run the applications.[175] Facebook further acted unfairly when sharing user information with their friends' third-party applications after those users had specified that they wished that information to be shared with their "Friends Only."[176] Finally, Facebook could not share user personal information with advertisers after stating that it would not do so.[177]

As another example, the FTC has found that Google violated Section 5 when it used Gmail user contacts for its social networking tool, Google Buzz, without user consent.[178] The FTC found that, according to Google's representations, user information should only have been used to provide Gmail services.[179] As Google then used Gmail contacts to automatically generate connections in its new social networking site without user consent, the FTC found Google's representations to be a deceptive trade practice in violation of Section 5.[180]

Extracting biometric data from user photos without their consent is comparable to Facebook's past practices that the FTC found to violate Section 5. It is comparable to, if not more "deceptive" than, using Gmail user contacts in Google Buzz. While Gmail user contacts were still used as "contacts" in Google Buzz (albeit publicly visible contacts), users who uploaded photos to Facebook could not expect that years later those photos would be scanned for biometric data to identify them in other photos without their knowledge or consent.[181] In oth-

---

175. *Id.*

176. *Id.*

177. *Id.*

178. *See* Complaint, Google Inc., No. C-4336 (Aug. 8, 2012) [hereinafter Complaint, Google], *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf.

179. *Id.* at 5–6.

180. *Id.*

181. For example, Facebook's Privacy Policy from 2006 does not specifically mention processing photos submitted to Facebook to extract personally identifiable information. Instead, this early policy provides:

> Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings to enable you to connect with people on Facebook . . . . Profile information is used by Facebook primarily to be presented back to and edited by you when you access the service and to be presented to others permitted to view that information by your privacy settings. In some cases where your privacy settings permit it (e.g., posting to your wall), other Facebook users may be able to supplement your profile . . . . Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people at a school like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook.

Facebook Privacy Policy Version Recorded May 5, 2006, TOSBACK, http://www.tosback.org/version.php?vid=396 (last visited Dec. 22, 2012).

er words, the Photo Tag Suggest used personal information in an entirely new and unpredictable manner.

The problem is that "unfair or deceptive" is a very ambiguous standard.[182] A court may defer to the FTC's interpretation of the scope of Section 5.[183] But until the FTC takes a stand, a company does not have clear instructions for what is considered "deceptive" with respect to new technologies and what it needs to do to comply with Section 5. It is, for example, unclear whether extraction of biometric data from photos is a completely new use of information, or whether it can be encompassed within Facebook's broad statement about how it will use all information it receives "in connection with [its] services."[184] It is likewise unclear whether specific user consent is required or whether the ability to opt out is sufficient.[185] These ambiguities create a race to the bottom whereby online businesses narrowly interpret privacy laws in order to gain a competitive edge.

It could also be argued that Facebook's Photo Tag Suggest violates the Children's Online Privacy Protection Act ("COPPA")[186] by collecting biometric data from the 7.5 million Facebook users that are under the age of thirteen and linking new photos to those user profiles.[187] In essence, COPPA requires the FTC to make rules that require a website that is "targeted to children" or has "actual knowledge" that it collects information from children to notify them about how their information is collected, used, and disclosed and "obtain verifiable parental consent."[188] Implementing regulations "prohibit[] unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet."[189] The FTC can further litigate COPPA violations under the FTC Act.[190] Various problems with COPPA have been discussed at length elsewhere.[191] But most im-

182. *See* Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1326 (2001).

183. *See generally* Chevron USA Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984) (establishing that when a statute is ambiguous, courts must defer to agency interpretation if that interpretation is reasonable).

184. *Facebook Data Use Policy: Information We Receive About You*, *supra* note 30.

185. The FTC appeared to reject certain opt-out features when Facebook opened to the public user information that was previously only available to individuals specified in user privacy settings. It is, however, not clear whether this applies to opt-out features outside the narrow facts of that case. *See* Complaint, Facebook, *supra* note 169, at 6.

186. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2006).

187. Complaint, Facebook, *supra* note 169, at 24.

188. 15 U.S.C. § 6502.

189. 16 C.F.R. § 312.1 (2012).

190. *Id.* § 312.9.

191. *See, e.g.*, *How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective, Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. (2010) (statement of danah boyd et. al.), *available at* http://cyber.law.harvard.edu/publications/2010/COPPA_

portantly for our purposes, COPPA suffers from the same ambiguities as the FTC Act, in that it is unclear whether (and what) notice and parental consent is required for biometric data.[192]

B. Illinois Biometric Information Privacy Act

What appears to be missing from the FTC Act and COPPA, for the purposes of face recognition, are provisions identifying collection and use of biometric data as a new practice that requires specific and informed consent. Such provisions can be found in the Illinois Biometric Information Privacy Act.

In 2008, the Illinois legislature worried that "[m]ajor national corporations ha[d] selected the City of Chicago and other locations in th[e] State as pilot testing sites for new applications of biometric-facilitated financial transactions."[193] Illinois addressed this by requiring companies to notify an individual and obtain a written release before collecting the individual's biometric information, including "face geometry."[194] Crucially, individuals must know about the "purpose and length of term for which . . . biometric information is being collected, stored, and used."[195] Once a company has collected biometric data, it may not disclose it without individual consent, unless the law requires disclosure.[196]

The Illinois legislation avoids some of the pitfalls identified in the FTC Act and COPPA when dealing with automatic face recognition. It clearly specifies what type of information a company needs to provide to individuals before collecting their biometric data.[197] It also

---

Implemented_Is_Misinterpreted_by_Public.

192. One reason for this ambiguity is that it is unclear whether biometric data falls within COPPA's definition of "personal information," which includes:

> (A) a first and last name;
> (B) a home or other physical address including street name and name of a city or town;
> (C) an e-mail address;
> (D) a telephone number;
> (E) a Social Security number;
> (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
> (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

15 U.S.C. § 6501(8) (2006). Biometric data would seem to fall under subsections (F) and (G), but until the FTC acts to enforce these provisions with respect to face recognition technology, companies plainly cannot be certain of the scope of these provisions.

193. 740 ILL. COMP. STAT. ANN., § 14/5(b) (West 2012).

194. *Id.* §§ 14/10, 14/15(b)(1),(3).

195. *Id.* § 14/15(b)(2).

196. *Id.* § 14/15(d).

197. *Id.* § 14/15(b)(1)(2).

specifies that individual's need to opt in to the collection and use of biometric data — and that opt-out consent will not suffice.[198] What is unclear, however, is whether individuals are able to provide written release in electronic format to allow the collection and use of biometrics in social networks.[199]

This legislation also has a number of broader problems — the most obvious of which is that it only applies in Illinois or to transactions with sufficient nexus to the state.[200] Given the global scope of Internet companies such as Facebook, different state laws create a fragmented legislative landscape that is difficult on small businesses while not necessarily offering more protection to online users. Federal legislation is more desirable, though even that may be too limited in geography. The European Union members, for example, have sought to harmonize their national data protection laws into binding EU legislation to address today's global information flows.[201]

Second, it is questionable whether biometric-specific legislation provides protection for users. The Center for Democracy and Technology has cautioned, "if consumer profiling and tracking via facial recognition or other biometrics were curtailed, consumers would still be profiled and tracked through innumerable alternative methods."[202] It therefore encouraged Congress to adopt comprehensive data protection legislation rather than discretely addressing automatic face recognition.[203] Indeed, broader regulation is important given that individuals could be identified and connected to their online profiles even without biometric processing through geolocation in mobile phones or some yet unknown future technology.[204]

---

198. *See id.* § 14/15(b)(3).

199. *See id.*

200. Illinois courts would only have personal jurisdiction over a defendant that has "minimum contacts" with Illinois. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945). However, Illinois law may still be applied by another court if it determines the State of Illinois "has the greater interest in having its rule applied." CAT Internet Servs. v. Magazines.com, Inc., No. CIV.A. 00-2135, 2001 WL 8858, at *2 (E.D. Pa. Jan. 4, 2001).

201. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, COM (2012) 11 final, (Jan. 25, 2012) [hereinafter *General Data Protection Regulation*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

202. *Seeing Is ID'ing: Facial Recognition & Privacy*, CTR. FOR DEMOCRACY AND TECH. 13 (Dec. 6, 2011), https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-CDT_Comments_to_FTC_Workshop.pdf.

203. *Id.*

204. *See* Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES, Aug. 12, 2010, at B6.

Finally, unlike the FTC Act, the Illinois law is not enforced by an agency.[205] Instead, it creates a private right of action for aggrieved individuals.[206] This is particularly problematic for privacy in social networks, where users are often not fully apprised of how their biometric information is stored and used.[207] Even if individuals did have access to this information, they may not have the technical expertise to effectively evaluate the privacy practices.

C. Texas Regulation of Biometric Data

Similar to Illinois, Texas regulates the collection and use of biometric data, including "face geometry."[208] It prohibits the collection of an individual's biometric data for a commercial purpose without first informing that individual and obtaining her consent.[209] Once the data is collected, the company in possession must protect it from disclosure the same way it would protect any confidential information and must delete the biometric data within a year after it has served its purpose.[210] Texas further does not permit transfers of biometric data for any purpose other than: (1) to identify a deceased or missing individual if that individual previously consented to such identification; (2) for a transaction upon an individual's request or authorization; or (3) to disclose the data pursuant to a state or federal statute or for a law enforcement purpose pursuant to a warrant.[211]

Further, although this statute creates a private cause of action much like the Illinois law, it also allows the Texas Attorney General to bring an action for damages.[212] The Attorney General, however, may not have the relevant expertise and resources to bring such actions. This illustrates the greatest flaws of both the Illinois and the Texas laws: it is not enough to have laws on the books if they are not effectively enforced.[213] While these two statutes technically prohibit the conceptual privacy violation identified in Part III, they do not appear to be capable of preventing it. Here, "the States [of Illinois and

205. It did, however, establish a Biometric Information Privacy Study Committee to consider the use of biometric data by government agencies. 740 ILL. COMP. STAT. ANN. § 14/20–14/30 (West 2012).

206. *Id.* § 14/20.

207. *See* Solove, *Privacy and Power*, *supra* note 163, at 1433 (discussing privacy tort violation in the commercial uses of databases and noting that "[i]t would be difficult for a plaintiff even to discover that such sales or disclosures have been made").

208. TEX. BUS. & COM. CODE ANN. § 503.001(a) (Vernon 2012).

209. *Id.* § 503.001(b).

210. *Id.* § 503.001(c)(2)–(3).

211. *Id.* § 503.001(c)(1).

212. *Id.* § 503.001(d).

213. There does not appear to be a single case filed pursuant to these statutes in the years since they were passed.

Texas have] perform[ed] their role as laboratories for experimentation to devise various solutions where the best solution is far from clear."[214] The lesson learned from their experiments, I would argue, is that mere legislation is not sufficient to prevent privacy violations that arise from non-consensual extraction of biometric data from photos in social networks. Instead, a problem of this nature requires a multifaceted solution along the lines of the proposal in Part V.

D. California's Failed Attempts to Regulate the Use of Biometric Data

It is curious, perhaps, that while Illinois and Texas have statutes regulating the use of biometric data within their jurisdictions, the high technology hub in Silicon Valley has no such statutes. Being at the forefront of technological progress, Californians ostensibly worried about face recognition technology as early as 1998. Back then, the *Los Angeles Times* suggested that:

> Face-recognition technology . . . could be used by government or police agencies to literally identify faces in a crowd. Any face that had already been stored in a databank could be identified much more quickly and with far more accuracy than the FBI enjoyed while snapping photographs of Vietnam War protesters.[215]

This article was later cited before the California legislature, which has since considered a string of bills to protect biometric data — none of which were passed.[216] In 1998, the legislature considered Senate Bill 1622 to require a person's consent before collecting or sharing her biometric data and Assembly Bill 50 to require notice and consent to use such data to complete a transaction.[217] While both of these bills died in the legislative process, they were revived in the equally unsuccessful Senate Bill 71, which would have provided specific requirements for collecting and using biometric data as part of a California

---

214. United States v. Lopez, 514 U.S. 549, 581 (1995) (Kennedy, J., concurring).

215. Eric Slater, *Not All See Eye to Eye on Biometrics*, L.A. TIMES (Apr. 29, 1998), http://articles.latimes.com/1998/apr/29/news/mn-44246.

216. *See* S. RULES COMM., BILL ANALYSIS OF S.B. 129 (Aug. 28, 2000) (Conf. Rep. No. 1), *available at* http://www.leginfo.ca.gov/pub/99-00/bill/sen/sb_0101-0150/sb_129_cfa_20000829_124347_sen_floor.html.

217. S. 1622, 1997–1998 Sess. (Cal. 1998), *available at* http://www.leginfo.ca.gov/pub/97-98/bill/sen/sb_1601-1650/sb_1622_bill_19980706_amended_asm.html; Assemb. 50, 1997–1998 Sess., (Cal. 1998), *available at* http://www.leginfo.ca.gov/pub/97-98/bill/asm/ab_0001-0050/ab_50_bill_19980831_amended_sen.pdf.

Personal Information Privacy Bill of Rights.[218] In the following year, Senate Bill 129 was introduced to require consent before collection of biometric data, but it was subsequently amended to eliminate all provisions regarding biometrics.[219] In 2001, Senate Bill 169 was proposed to specifically regulate face recognition technology and require a "clear and conspicuous notice" before collection of biometric data as well as consent before such data could be shared.[220] Finally, a bill that did not pass by the end of the 2011-2012 legislative session would have required a company that collects or uses "sensitive information," including biometric data, to allow users to opt out of its collection, use, and storage.[221] Yet, because California houses numerous cutting-edge technology companies, there was loud opposition to this bill.[222] Some thirty companies and organizations, including Facebook, Google, AOL, Yahoo!, Time Warner Cable, and American Express came out against it, contending that "[p]rohibiting the collection and use of . . . data would severely harm future innovation in the state and harm consumers."[223]

The Silicon Valley lobby's rhetoric and the long history of failed legislation in California further show why mere legal reform would inadequately address this issue. The concern for innovation is particularly prevalent in that state. Excessive privacy regulation will deter experimentation by small startups, which do not have deep pockets to risk litigation.[224] To avoid this, we need to think outside the box to provide a flexible regulatory framework that prevents abusive collection and use of biometric data, while preserving the unregulated quali-

---

218. *See* S. 71, 1997–1998 Sess. (Cal. 1998), *available at* http://www.leginfo.ca.gov/pub/99-00/bill/sen/sb_0051-0100/sb_71_bill_20000828_amended_asm.pdf.

219. S. 129, 1999–2000 Sess. (Cal. 1999), *available at* http://www.leginfo.ca.gov/pub/99-00/bill/sen/sb_0101-0150/sb_129_bill_20000930_chaptered.html; *see also* S. RULES COMM., *supra* note 216.

220. S. 169, 2001–2002 Sess. (Cal. 2001), *available* at http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_0151-0200/sb_169_bill_20010914_amended_asm.html.

221. S. 761, 2011–2012 Sess. (Cal. 2012), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0751-0800/sb_761_bill_20110510_amended_sen_v95.html.

222. *See* Mathew Lasar, *Google, Facebook: "Do Not Track" Bill a Threat to California Economy*, ARS TECHNICA (May 6, 2011, 11:12 AM), http://arstechnica.com/tech-policy/news/2011/05/google-facebook-fight-california-do-not-track-law.

223. Letter from PFIC to The Honorable Alan Lowenthal, California State Senate (Apr. 27, 2011), *available at* http://static.arstechnica.com/oppositionletter.pdf.

224. *See* Darian M. Ibrahim, *How Do Start-Ups Obtain Their Legal Services?*, 2012 Wis. L. Rev. 333, 337–38 (discussing that "start-ups are notoriously cash-strapped. Expenses are heavily scrutinized and a start-up's main goal is to use its limited funds to develop or grow its product or service. As a result, legal and other needs may be seen as a luxury a start-up cannot afford."); *see also* Tim Wafa, *Global Internet Privacy Rights: A Pragmatic Approach*, 13 INTELL. PROP. L. BULL. 131, 144 (2009) (noting that small businesses "generally operate on thinner margins and lack the financial wherewithal to comply with multi-jurisdictional privacy requirements").

ties of the Internet that invite innovation.[225] This, I believe, warrants architectural and market solutions in addition to legal reform.[226]

E. Face Recognition as Intrusion upon Seclusion

Even if a state does not have legislation regulating face recognition technology, it seems reasonable that individuals harmed by this technology should have a cause of action in tort against social networks. Most privacy torts, however, would not apply to the mere collection and processing of biometric data because they require a *disclosure* of private information to third parties.[227] The most applicable tort therefore is intrusion upon seclusion,[228] which is generally described as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[229]

Given that this intrusion need not be physical, it could apply to a social network's processing of user photos to collect biometric data, provided that a user can establish that those photos were kept in "seclusion" and that these actions would be "highly offensive to a reasonable person."[230] Generally, information is in seclusion when it exists in "spheres from which an ordinary [person] in a plaintiff's position could reasonably expect that the particular defendant should be excluded."[231] The fact that a user shared her photos with friends would not necessarily mean that those photos were not in seclusion because courts have sometimes relied on a notion of reasonable expectation of limited privacy.[232] For example, a California court considered non-physical intrusion sufficient when a plaintiff was

---

225. *See* Hirsch, *supra* note 157, at 32, 64.

226. *See infra* Part V.

227. For example, the torts of disclosure of private facts and false light require a publication. SOLOVE, THE DIGITAL PERSON, *supra* note 78, at 59–60.

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

229. *Id.* § 652B.

230. *Id.*

231. Nader v. General Motors Corp., 25 N.E. 2d 765, 768 (N.Y. 1970) (citing Pearson v. Dodd, 410 F.2d 701 (D.C. Cir. 1969)).

232. Sanders v. American Broadcasting Cos., 978 P.2d 67, 72 (Cal. 1999).

videotaped with a "hat cam" while giving an interview.[233] The court noted that:

> Like "privacy," the concept of "seclusion" is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone.[234]

By analogy, even if I share a photo with my fifteen closest friends in a social network, it does not mean that the network may extract my biometric data from that photo and offer it to my 800 network contacts to automatically recognize me in other photos.

The main problem with applying this tort to face recognition technology is that courts may not view mere collection of information as "highly offensive."[235] As Professor Solove has noted, "[e]ach particular instance of collection is often small and innocuous; the danger is created by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time."[236] Professor Solove has also observed that "many parts of cyberspace may well be considered public places," where there can be no seclusion.[237] This view corresponds to the traditional privacy theories I discussed in Part III, which generally protect private spaces and secrets rather than the collection of information that flows in cyberspace. However, at least one court has suggested that "overzealous" information collection, even in public places, could sometimes constitute an intrusion upon seclusion.[238] In *Nader v. General Motors Corporation*, the court noted that:

> [T]he mere observation of the plaintiff in a public place does not amount to an invasion of his privacy.

---

233. *Id.* at 70.

234. *Id.* at 72 (internal quotations and citation omitted).

235. *See Nader*, 25 N.E. 2d at 567 ("It should be emphasized that the mere gathering of information about a particular individual does not give rise to a cause of action under this theory. Privacy is invaded only if the information sought is of a confidential nature and the defendant's conduct was unreasonably intrusive."); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

236. SOLOVE, THE DIGITAL PERSON, *supra* note 78, at 59 (noting that courts have dismissed "actions based on obtaining a person's unlisted phone number, selling the names of magazine subscribers to direct mail companies, and collecting and disclosing an individual's past insurance history").

237. *Id.*; *see also* Romano v. Steelcase Inc., 907 N.Y.S. 2d 650, 657 (Sup. Ct. 2010) (stating that a user "consented to the fact that her personal information would be shared with others [on Facebook and MySpace], notwithstanding her privacy settings" and therefore she "knew that her information may become publicly available").

238. *See Nader*, 25 N.E.2d at 570.

> But, under certain circumstances, surveillance may be so 'overzealous' as to render it actionable . . . . A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing.[239]

A person may expose her face when she is in a public place or publicly posts her picture in a social network, such that if friends see her or the picture, they may recognize her.[240] But she is not necessarily exposing her biometric data, which is not visible to the human eye. Arguably, much as a private person may not have the right to use binoculars to try to discover how much money a bank patron is withdrawing from across the bank office, so too Facebook likely cannot extract biometric data from a person's face even if the person shows her face in public.[241] Yet, even if courts could be persuaded that extraction of biometric data from public photos is a highly offensive intrusion upon seclusion, the policing of violations would again be left to individual users who lack relevant expertise and information about data practices in social networks.[242] As we saw with the Illinois and Texas laws, the mere existence of a law that prohibits the collection of biometric data without user consent does not actually prevent social networks from collecting this data because users cannot effectively enforce these laws. It seems, therefore, that to be effective, a regulatory solution needs to do more than merely prohibit certain activities. In the next Part, I outline what I believe could be a feasible solution to this problem.

V. A PROPOSAL FOR FACE RECOGNITION PRIVACY

The current legal landscape explains why social networks can collect and use biometric data in a manner that exposes user privacy. There are no comprehensive rules governing this practice. Instead, there is fragmented legislation on the state level, which is not sufficiently enforced against companies. Further, as users do not understand the automatic face recognition process, they do not exert pressure on social networks to improve their practices. Given both the

239. *Id.*

240. *See* Budish, *supra* note 90, at 1876 (intrusion upon seclusion is "inapplicable to those whose photos are taken in public spaces and then uploaded to the Internet").

241. *See* NANCY YUE LIU, BIO-PRIVACY, PRIVACY REGULATION AND THE CHALLENGE OF BIOMETRICS 177 (2012) ("While there may be no expectation of privacy in public places, there may still be an expectation of anonymity.").

242. *See generally* Solove, *Privacy and Power*, *supra* note 163.

technological and social complexity of this problem — including users' social need to share experiences with friends, and the overall benefits of new technology — it calls for solutions beyond mere legal reform.

In this Part, I suggest how face recognition technology in social networks could be regulated. My proposal relies on Professor Lawrence Lessig's famous articulation that online activities are regulated by the aggregate of four constraints — namely, "the law, social norms, the market, and architecture."[243] Most obviously, the law mandates certain behavior and imposes sanctions on deviate actions.[244] Social norms likewise impose sanctions when members of a community stray from commonly held expectations of proper behavior.[245] The market further tends to inflict a cost on certain actions, incentivizing market participants to modify their behavior.[246] Finally, architecture can mandate behavior in the most effective way, by making deviate behavior technically impossible or difficult.[247] For example, the law could directly prohibit posting of obscene content on an online forum.[248] But architecture and social norms may provide more effective sanctions by technologically filtering out certain words or by playing on users' fear of staining their good name or online identity if they post that kind of content.[249] If the obscene content is also unpopular, this market condition will encourage the forum provider to remove the content in order to attract more users and thereby boost ad revenues from the site.[250]

These four constraints on behavior are interdependent and can work together or against each other.[251] Adjusting only one of these constraints could therefore be counter-productive because the other constraints could correct for that adjustment and result in zero net regulation of the activity. Scholars have therefore noted that no single one of these constraints offers sufficient protection for online privacy.[252]

---

243. LESSIG, *supra* note 7, at 123. As Professor Lessig explains, these four constraints collectively regulate offline behavior. *Id.* For example, how fast you drive on a road may be constrained by the legal speed limit, architectural constraints such as road bumps and stop signs, whether the market price of car insurance increases if you receive a speeding ticket, and speed of other drivers, i.e. the social norms.

244. *Id.* at 124.

245. *Id.*

246. *Id.*

247. *See id.* at 124–26.

248. *See id.* at 124.

249. *See id.*

250. *See id.*

251. *Id.* at 123–24.

252. John G. Palfrey, *The Public and the Private at the Border*, 78 MISS. L.J. 241, 289 (2008) ("Though technology may help safeguard personally identifiable information to some extent in a digital age, the answer is not likely that privacy can be enhanced through

On the other hand, a regulatory proposal that includes adjustments to all four constraints could be more effective because the constraints could work together — while being less restrictive on innovation.[253] Relying on all four constraints may also have a broader effect than a mere legal reform because it would not be limited to the territorial boundaries of one jurisdiction.[254] If a social network were to adopt data portability and interoperability standards, those standards could apply globally. Further, because part of the solution is to allow users to enforce their own pre-existing privacy norms, the regulation would automatically adjust to cultural differences. Thus, for instance, if the Germans are particularly sensitive to face recognition technology, they can enforce their social norms to avoid it, while most Americans may consciously consent to it.[255] While these social norms and technical and market solutions would complement the legal solution, the law could still play an important role in mandating adjustments to all four constraints.[256]

A. Law — Better to Ask for Permission Than Forgiveness

There is much to be desired in privacy law. The current federal law lacks any regulations on the collection and use of biometrics. While such provisions currently exist in Illinois and Texas, the global scope of the Internet necessitates at least nationwide requirements, in the absence of easily enforceable international treaties. Further, given the lack of transparency in social networks, any requirements with respect to biometrics should be enforced by an agency rather than by

---

technology alone. The market can help, too, as firms compete to earn user trust, but it provides an imperfect solution at best. In addition, straight legal reform is unlikely to offer a complete answer."); *see also* Urs Gasser, Sandra Cortesi & John Palfrey, The Changing Role of the Individual for Privacy: The Example of Youth Online ("[H]ere is no silver-bullet solution to the various privacy-related problems and issues resulting from the current users of digital technology in general and the changed role of the individual in particular . . . Rather, a combination of approaches and instruments must be used to address the manifold privacy challenges") (unpublished article) (on file with author).

253. *See supra* text accompanying note 155.

254. *See* Jacqueline D. Lipton, *What Blogging Might Teach About CyberNorms*, 4 AKRON INTELL. PROP. J. 239, 244 (2010) [hereinafter Lipton, *Blogging*].

255. This hypothetical may even have some grain of truth as Facebook offered its Photo Tag Suggest in the United States for several months before rolling it out in Europe, where the Hamburg Data Protection Agency immediately investigated the technology and concluded that it violated users' privacy. Press Release, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Facebook's Biometric Database Continues to Be Unlawful (Nov. 10, 2011) [hereinafter FB Database Unlawful], *available at* http://www.datenschutz-hamburg.de/uploads/media/PressRelease-2011-11-10-Facebook_BiometricDatebase.pdf.

256. LESSIG, *supra* note 7, at 125 ("[The four constraints] are neither found in nature nor fixed by God. Each can be changed, though the mechanics of changing them is complex. Law can have a significant role in this mechanics . . . .").

aggrieved individuals through private actions. Finally, a face recognition privacy law should be one piece of a broader data protection law to avoid plugging the gap on face recognition technology while exposing users to other types of privacy violations. These observations suggest the need for the following components of a productive privacy law reform:

> (a) A comprehensive data protection law;
>
> (b) As part of the broader law, provisions that specifically identify collection and use of biometric data as a separate data use that gives rise to specific obligations;
>
> (c) Clear instructions about how companies need to inform users about their biometric data practices;
>
> (d) A requirement that companies get informed, written, and specific consent from users before collecting or processing their biometrics (to be accompanied by architectural solutions that ensure users' free choice when consenting); and
>
> (e) An agency tasked with enforcing the comprehensive data protection law, including the provisions with respect to biometrics.

The full scope of the comprehensive data protection law sweeps well beyond the scope of this Article, which focuses on the privacy concerns that arise out of social networks' collection and use of biometric data. However, the development of such comprehensive legislation is currently underway in the U.S. and in Europe.[257]

---

257. In 2011, Senators John Kerry and John McCain proposed a Privacy Bill of Rights Act to grant individuals the right to prevent the use of their personal information and require companies to obtain consent before collecting or sharing sensitive data. S. 799, 112th Cong. (2011). Further, the Obama administration has encouraged Congress to adopt a privacy bill of rights act and put pressure on companies to improve their privacy practices. Press Release, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights. The European Union is also strengthening its data protection laws with a proposed unified regulation that would apply directly to individuals and companies in the EU countries. Press Release, European Commission, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), *available at* http://europa.eu/rapid/press-release_IP-12-46_en.htm.

At this point, I should acknowledge that while there is a fierce debate over the overall efficiency of the notice and consent model; I do not intend this Article to engage in that debate.[258] This Article closely scrutinizes the narrow issue of face recognition technology in social networks and proposes a multifaceted solution to protect privacy — of which notice and consent is but one facet. Crucially, my proposed notice and consent requirements are tailored to the particular problem of face recognition technology in social networks, which even critics of the notice and consent model agree may be a successful strategy.[259] While providing solutions that focus on this narrow problem, the proposal may nevertheless shed light on how we can address other online problems that raise similar issues.

1. Specific Consent Before Collecting or Using Biometric Data

At this juncture in my analysis, it should be clear that I view biometric data as particularly sensitive information because of its power to de-anonymize a face (which we cannot easily hide or alter) and instantly connect it to all our online activities. This type of sensitive information should never be collected or used without a person's con-

258. *See* Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent (Oct. 2009) (unpublished position paper), *available at* http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf (analyzing the problem of getting true notice and consent in the context of "online behavioral advertising"); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 342 (Jane K. Winn ed., 2006) (arguing that "we have become so enamored with notice and choice that we have failed to develop better alternatives"); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1398 (2000) ("[T]he privacy-as-choice model assumes that data privacy can be valued using market measures. But monetary measures of value do not capture the very real incommensurabilities that the choice presents."); Grimmelmann, *supra* note 138, at 1181–84 (concluding that "the informed-choice model is completely unrealistic"); Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 779–80 (1999) (discussing why "notice and consent are not enough"); Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 782–83 (2000) (discussing how the notice and consent model "only present[s] take-it-or-leave-it terms — and ones that are frequently vague"); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 827–28 (1999–2000) (stating that "notice and consent alone are insufficient").

259. *See*, *e.g.*, Nissenbaum, *Contextual Approach*, *supra* note 8, at 35 ("I am not convinced that notice-and-consent, however refined, will result in better privacy online as long as it remains a procedural mechanism divorced from the particularities of relevant online activity."); *see also* Introna & Nissenbaum, *supra* note 59 (noting that a particular notice and consent model may be appropriate for face recognition that connects a face to other information in a database); NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 145 (discussing how sometimes notice and consent are the relevant transmission principles governing the flow of information).

sent.[260] The consent needs to be specific as to the collection or use of the data and be based on detailed information of the type that I outline in the next section. It must also be affirmative, and it must precede the collection or use of the information in question. From the user's perspective, however, the notice and consent model can only be effective if it is accompanied by freedom to withhold consent. For that reason, the architectural and market solutions below are intended to give users more choice by making social networks interoperable with distributed social networks and providing users with more autonomy over their data use. Once users understand how social networks use their biometric data and have realistic alternatives, they will be able to select only those data practices that they find acceptable. But if users fail to make a choice — either because they still do not understand the particular data process or because they have not had time to become informed — no new data should be collected and previously collected data should not be used in a new way.[261]

Privacy settings[262] that allow users to opt out of collection and use of biometric data simply cannot serve as consent — not least because by the time a user opts out, the data has already been collected and

260. *See Recommendation*, COUNCIL OF EUR., *supra* note 10 ("The use of techniques that may have a significant impact on users' privacy — where for instance processing involves sensitive or biometric data (such as facial recognition) — requires enhanced protection and should not be activated by default.").

261. The German Federal Data Protection Act, which implements the European Union Data Protection Directive, currently has a similar consent requirement with respect to the collection and processing of personally identifiable data. Moreover, the EU Article 29 Working Party has opined that "[c]onsent must be given prior to the start of processing activities or before any new use of the data" so that users can make "informed choice[s]." Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Dec. 20, 1990, Bundesgesetzblatt [BGBl. I] at 2954, as amended Sept. 14, 1994 [hereinafter "BDSG"], *available at* http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile (all subsequent quotations refer to an English translation of the Act); Press Release, Article 29 Data Protection Working Party, European Data Protection Authorities Clarify the Notion of Consent (July 14, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/press_release%20opinion_on_consent_14072011.pdf; *see Opinion of the Article 29 Data Protection Working Party on the Definition of Consent*, 2011 O.J. (C 1197), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf; *see also Recommendation*, COUNCIL OF EUR., *supra* note 10 ("Social networking services should seek the informed consent of users if they wish to process new data about them, share their data with other categories of people or companies and/or use their data in ways other than those necessary for the specified purposes they were originally collected for.").

262. Although privacy settings alone should not be used to satisfy a "consent" requirement, they can serve an important function to supplement opt-in consent to allow users to change their mind after consenting, to fine-tune their data use practices, or to simply review what exactly they have opted into. The overall value of privacy settings, however, is beyond the scope of this Article and has been extensively debated by scholars. *See, e.g.,* SOLOVE, FUTURE OF REPUTATION, *supra* note 80, at 200–01; Grimmelmann, *supra* note 138, at 1184–87.

potentially used to identify the person in new photos.[263] Professor James Grimmelmann has noted that opt-out consent is particularly insufficient when a new practice in a social network involves "a large cultural shift."[264] Collection and use of biometric data from photos previously shared with friends involves such a cultural shift because it uses technology that, for most users, is completely unimaginable. Further, opt-out consent is often designed so that users are not even aware of the change that they are accepting by default. But even if a social network were to actually notify a user that she can opt out if she does not want to have her friends automatically find her in new photos, the user would simply not understand the issue. This is because it would be presented in terms of trust vis-à-vis the users' friends — not the social network that will be collecting, storing, and using highly sensitive and personally identifiable information about that user. A user cannot be expected to take affirmative (and cumbersome) steps to object to something that she does not understand. As a result, specific opt-in consent should be solicited from users. One problematic aspect of consent with respect to face recognition technology is that in order to know whether an unidentified individual consents to automatic face recognition, you need to first extract and process her biometric data to compare it against a database of consenting individuals.[265] This could be addressed by allowing automatic face recognition for the limited purpose of determining consent and requiring immediate deletion of any data derived from the process if it turns out that there was no such consent.[266]

The consent also needs to be innovatively designed to ensure that users truly understand what they approve. In this respect, Google's opt-in notice for its face recognition technology, "Find My Face," is a good start, though not perfect. Google launched Find My Face in December 2011.[267] At that time, it used a cartoon to illustrate how Find

---

263. Indeed, one study suggests that "people who think they have already lost the ability to control private information — that privacy is not something they are endowed with [because a service collects data by default and users must opt-out of data collection] — may value privacy less as a result." Aleecia M. McDonald & Lorrie Faith Cranor, *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*, 38TH RES. CONF. ON COMM., INFO. & INTERNET POL'Y 26 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092.

264. Grimmelmann, *supra* note 138, at 1202.

265. Yana Welinder, *EU Weighs in on Privacy in Face Recognition Apps*, ELEC. FRONTIER FOUND. (Jun. 28, 2012), https://www.eff.org/deeplinks/2012/06/eu-recommendations-use-face-recognition-technology-online-and-mobile-applications.

266. *See Opinion of the Article 29 Data Protection Working Party*, 2012 O.J. (C 727), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.

267. Larry Magid, *Google+ Adds Find My Face Feature*, FORBES (Dec. 8, 2011, 1:59 PM), http://www.forbes.com/sites/larrymagid/2011/12/08/google-adds-find-my-face-feature.

My Face would "[h]elp people tag you in photos" and it provided the user's real name above a face in the cartoon to make the example feel realistic.[268] Users could then select to turn on the function. The problem was that the notice did not indicate that this function would use old photos to find users' faces in new photos. If users did not know how face recognition technology works — and most users do not — this notice did not tell them that it was asking for permission to collect and use their data in a new way. The notice had a link that users could click to "learn more," but given the small print that usually appears after clicking on links of this sort, by now most users have learned not to be too curious online.[269] Yet, while this notice failed to inform users of every relevant aspect of the face recognition process, it demonstrated Google's ability to communicate abstract information like automatic face recognition through a simple cartoon. Google is treading a narrow path here. On the one hand, it tries to live up to its motto, "Don't be evil."[270] On the other hand, it does not want to provide more information than its competitors so as not to overwhelm the users. But if Google had clearer instructions about what information it needed to present, and the same requirements applied to its competitors, it could have designed a notice to obtain adequate consent from its users.

2. Notice Regarding the Collection and Processing of Biometrics

What sort of information should companies provide before collecting or using biometric data? At the very least, users should know specifically what biometric data is collected and from which photos. They should also know how long the data will be stored and who will have access to it in the meantime. Companies need to explain in detail how they will use the data and who will have access to the end results of that use, i.e., once the data has been aggregated or processed in some way. Users should also know how they can delete biometric data — as it is not clear that deleting a photo necessarily deletes the biometric data collected from that photo.[271]

---

268. *See id.*

269. Zev J. Eigen & Florencia Marotta-Wurgler, *What if Consumers Could Change the Terms of Online Contracts?* OWOCKI DOT COM (Nov. 29, 2011), http://owocki.com/wp-content/uploads/2011/11/Eigen_Marotta_Wurgler_TOSAmend.pdf (describing how users tend to tick the box agreeing to all "Terms & Conditions" without actually clicking on a link leading to those terms).

270. *Code of Conduct*, GOOGLE, http://investor.google.com/corporate/code-of-conduct.html (last visited Dec. 22, 2012).

271. *See,* e.g., Budish, *supra* note 90, at 1884–85 (suggesting that deletion of names from a biometric database would allow "citizens [to] secure their privacy without hiring attorneys or clogging the judicial system"); *see also Facebook Data Use Policy, supra* note 30 (stat-

The current lack of information leads users to make erroneous assumptions about how social networks use their photos. Users may, for example, mistakenly believe that biometric data will not be collected from photos to which they restrict access through their privacy settings. Most users probably think that if they opt out of automatic face recognition their biometric data will never be collected. But as a function of the opt-out consent, chances are that a social network collects biometrics when it rolls out a service, which then resides in a database even after a user opts out of automatic face recognition. These issues should be no mystery to users whose information is collected.

Companies should further have an incentive to think creatively about how they can present this information to users in an accessible way. Crucially, this information cannot just be buried in a privacy policy full of "legalese" and "tech-speak,"[272] which no one reads.[273] Some scholars are very skeptical about whether information about privacy practices can ever be effectively communicated to users.[274] Professor Nissenbaum argues that attempts to concisely communicate this information in plain language present a "transparency paradox."[275] Thorough information overwhelms users, while concise notices contain general provisions and do not describe the details that differentiate between good and bad practices.[276] I am more optimistic about companies' ability to concisely present this information if they have the right incentives. Work in infographics has shown that it is possible to explain incredibly complex information, such as geography or medical information, with graphs and charts that can easily be understood by non-experts.[277] The recent start-up trend of creating

---

ing that "some information may remain in backup copies and logs for up to 90 days" after an account is deleted).

272. Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 70 (2007).

273. While privacy policies are intended to inform users about how their personal data is collected, used, and shared, studies have shown that very few users read and understand them. *See, e.g.*, JOSEPH TUROW, AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 3–4 (2003), http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf; *Zogby Poll: Most Americans Worry About Identity Theft*, ZOGBY INT'L (Apr. 3, 2007), http://www.zogby.com/news/2007/04/03/zogby-poll-most-americans-worry-about-identity-theft.

274. *See, e.g.*, Cohen, *supra* note 258, at 1398; Grimmelmann, *supra* note 138, at 1181–84; Nissenbaum, *Contextual Approach*, *supra* note 8, at 35–36; Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, *supra* note 258, at 779–80; Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, *supra* note 258, at 782–83; Schwartz, *Internet Privacy and the State*, *supra* note 258, at 827–28; Barocas & Nissenbaum, *On Notice: The Trouble with Notice and Consent*, *supra* note 258.

275. Nissenbaum, *Contextual Approach*, *supra* note 8, at 36.

276. *Id.*

277. *See* THOMAS GOETZ, THE DECISION TREE: TAKING CONTROL OF YOUR HEALTH IN THE NEW ERA OF PERSONALIZED MEDICINE xiii (2010); NATHAN YAU, VISUALIZE THIS: THE FLOWINGDATA GUIDE TO DESIGN, VISUALIZATION, AND STATISTICS xvi (2011).

"demo" videos to communicate often very complex online business models to users and investors in only a few minutes is another example of this capability.[278] Emerging research in user experience design further suggests that websites can be designed to notify users of the data collection in real time and show how it will be used.[279] Indeed, social networks already spend most of their time thinking about how to present our intricate social relationships, correspondence, and social lives in a clear and accessible manner so that the platforms can be used by children and grandparents alike.[280] Organizing information about data practices is in fact a very similar task that they have the resources to handle.[281] The cartoon in the Google Plus notice — though not perfect — is a good example of how social networks can communicate very detailed information through a simple picture.[282] Another example is Facebook's Interactive Tools that allow a user to browse her own profile as if she was another person to experience what that particular individual can learn about her.[283] Were comprehensible information in non-traditional form incentivized by legal requirements and user expectations, these companies could extend their innovative solutions to provide simple and informative notice about biometric data collection and processing.

278. *See, e.g.*, MICTROTASK, http://www.microtask.com (last visited Dec. 22, 2012); *Personal Videos*, PERSONAL, https://www.personal.com/videos (last visited Dec. 22, 2012); SOLVE MEDIA, http://www.solvemedia.com (last visited Dec. 22, 2012); *Vimeo PRO*, VIMEO, http://vimeo.com/pro (last visited Dec. 22, 2012).

279. *See* M. Ryan Calo, *Against Notice Skepticism In Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033–34, 1041 (2012) (suggesting that privacy notices be designed based on users' "familiarity" with older technologies and their "psychological responses" to certain elements, as well as by "demonstrating the result of company [data] practices"); Deirdre K. Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1019 (2012) (arguing that "[p]rivacy by design . . . should aim to identify contextually-bound understandings of privacy, and, to design system architectures, interfaces, default settings as well as corporate policies that reflect them"); Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635, 1653 (2011) ("A growing body of literature in the field of human-computer interaction has focused on what are known as 'privacy indicators' — designs such as logos, icons, settings, and seals used to intuitively convey a website's policy regarding collection and use of personal information.").

280. *See* Mulligan, *supra* note 279, at 1026 (noting that "[g]iven that Facebook, Google, Apple, Microsoft, Twitter, and other companies employ significant numbers of HCI researchers, it is likely that [their] privacy failures can be attributed to both lack of adoption of HCI methods and disregard for HCI-based insight when in tension with other business goals").

281. *See id.*

282. *See supra* Part V.A.1.

283. *Interactive Tools*, FACEBOOK, https://www.facebook.com/about/privacy/tools (last visited Dec. 22, 2012).

3. Not-So-Secret Agents with a License to Investigate Data Practices

As with any regulation, the requirements discussed up to this point require an effective enforcement mechanism.[284] Users are not good at policing social networks because they do not know about the networks' internal operations. This is particularly true for highly technical processes like face recognition technology, which explains why we have not seen more lawsuits pursuant to the Illinois and Texas statutes or users trying to establish that the collection of biometric data is an intrusion upon their seclusion.[285] It seems, therefore, that this calls for an agency with technical expertise to investigate these processes. That agency should not passively wait until it gets complaints from aggrieved individuals or concerned organizations. Rather, it should regularly monitor the relevant activities, assess the risks of various practices, and provide informal guidance to social networks when their practices expose personal information. Its broad powers would be justified due to the vast amount of information that social networks collect from users — including children — while those users are under the impression that they are just sharing their experiences with their friends. Indeed, even if social networks were fully transparent, users would still not have a complete grasp of the situation because they use these services while socializing — when they feel like they can relax because they are among friends.[286] Given the amount and type of information that users relinquish in this intimate setting, an agency needs to step in and make sure that social networks do not take advantage of their users.[287] The agency's role would be to make sure that there is a fair quid pro quo whereby users provide some acceptable amount and type of information in return for a free socializing tool.

Here, the work of the European data protection agencies is instructive. The European Union member states have sought to harmonize their national privacy protection laws by adopting an EU Data

284. *See, e.g.*, Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, *in* WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION 13, 21 (Adam Thierer & Clyde Wayne Crews, Jr. eds., 2003).

285. *See supra* Part IV.

286. boyd, The Future of Privacy, *supra* note 101 ("You can think of these technologies as the equivalent of the mall or the cafe or the park when you were growing up. Teens go to them because all of their friends are there. They use them as public spaces where they can gather, socialize, gossip, flirt, and hang out.").

287. *See* Neil M. Richards, *The Perils of Social Reading*, 101 GEO. L.J. 1, 42 (forthcoming 2013) (suggesting that certain Internet service providers need to be regulated as "fiduciaries of our information"), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031307.

Protection Directive ("Directive").[288] This Directive required the member states to enact legislation to *transpose* (i.e., implement) the Directive's procedural requirements for the automatic processing of "personal data."[289] It further required the member states to establish at least one data protection agency to monitor the application of the transposing legislation within its territory.[290] In establishing these agencies, member states were to vest them with broad powers to:

1. Scrutinize data processes and demand information in the course of their investigations;[291]
2. Order "the blocking, erasure or destruction of data" and issue restraining orders on the processing of data;[292]
3. Refer cases to political bodies;[293]
4. Bring actions before appropriate courts;[294]
5. Consider personal claims regarding the violation of individual privacy rights;[295] and
6. Work with other member states' data protection agencies.[296]

As one example of national legislation implementing the Directive, the German Federal Data Protection Act provides for several data protection agencies.[297] It tasks a Federal Data Protection Agency with monitoring the data practices of *public* entities.[298] It further requires local governments for its various states to establish data protection agencies to monitor data practices in the *private* sector.[299] Thus, the Hamburg Data Protection Agency ("Hamburg DPA") — established pursuant to Section 24 of the Hamburg Data Protection Act — has the power to investigate and initiate action against companies within its jurisdiction.[300] As Facebook's German office is located in Hamburg, the Hamburg DPA obtained specific information from Fa-

---

288. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Recital 3, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF. It should be noted that this Directive is in the course of being superseded by an EU Data Protection Regulation, which if adopted will be directly binding in all EU states.

289. *Id.* art. 3 and 4.

290. *Id.* art. 28(1).

291. *Id.* art. 28(3).

292. *Id.*

293. *Id.*

294. *Id.*

295. *Id.* art. 28(4).

296. *Id.* art. 28(6).

297. BDSG, *supra* note 261, § 38.

298. *See id.* §§ 38(6), 27(1).

299. *See id.* § 38(6).

300. Hamburgisches Datenschutzgesetz [HmbDSG] [Hamburg Data Protection Act], July 5, 1990, HAMBURGISCHES GESETZ-UND VERORDNUNGSBLATT [HMB GVBL.] 24 (Hamburg) (Ger.), *available at* http://www.datenschutz-hamburg.de/uploads/media/Hamburgisches_Datenschutzgesetz__HmbDSG_.pdf.

cebook to investigate its face recognition technology.[301] It concluded that the technology violated the German Federal Data Protection Act and was preparing to file an action when Facebook voluntarily agreed to suspend its use of the technology in all EU countries.[302] In contrast to the events in Europe, Texas and Illinois residents do not have any procedure to obtain information from Facebook to determine if its face recognition technology complies with their state laws.[303]

There has been some debate over whether the FTC should function as a data protection agency. Almost a decade ago, Professor Joel Reidenberg argued that this privacy enforcement role sits uneasily with the FTC's "antitrust" and "consumer protection" roles.[304] Since then, the FTC has already assumed significant responsibility for privacy protection.[305] Thus, simply expanding and clarifying its functions may be preferable to creating a brand new agency. Indeed, a new agency may simply not be politically feasible given the current fear of "big government."[306]

B. Architecture — Unlocking the Walled Gardens

The notice and consent solution outlined above assumes that users have free choice regarding their participation in social networks. Yet, the use of social networks is driven by a "network effect" whereby their appeal depends on their number of existing users.[307] If most of one's friends use one network, it may be difficult to resist joining it, particularly if it has taken over many functions that traditionally took

---

301. *See* Press Release, Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Gesichtserkennungsfunktion von Facebook verstößt gegen europäisches und deutsches Datenschutzrecht (Aug. 2, 2011), *available at* http://www.datenschutz-hamburg.de/news/detail/article/gesichtserkennungsfunktion-von-facebook-verstoesst-gegen-europaeisches-und-deutsches-datenschutzrech.html?tx_ttnews%5BbackPid%5D=170&cHash=b9607e92ef91d779f308acd01b7dd639 (last visited Dec. 22, 2012); *see also* BDSG, *supra* note 261, §§ 38(3)–38(4).

302. *See* FB Database Unlawful, *supra* note 255; Somini Sengupta and Kevin J. O'Brien, *Facebook Can ID Faces, but Using Them Grows Tricky*, N.Y. TIMES, Sept. 21, 2012, at A1, *available at* http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html.

303. *See supra* Part IV.B–C.

304. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 887–88 (2003).

305. Steven Hetcher, *The* De Facto *Federal Privacy Commission*, 19 J. MARSHALL J. COMPUTER & INFO. L. 109, 130–31 (2000).

306. Elizabeth Mendes, *In U.S., Fear of Big Government at Near-Record Level*, GALLUP (Dec. 12, 2011), http://www.gallup.com/poll/151490/fear-big-government-near-record-level.aspx.

307. Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 483 (1998) ("'Network effects' refers to a group of theories clustered around the question whether and to what extent standard economic theory must be altered in cases in which 'the [u]tility that a user derives from consumption of a good increases with the number of other agents consuming the good.'" (citations omitted)).

place offline, like planning events and sharing everyday experiences with friends.[308] By the same token, switching to a different platform is problematic because a user would need to persuade all her friends to join her.[309] Given that most social networks do not allow users to move the profiles they built up over the years, a user's friends are not likely to be persuaded to start over with entering all of their information and establishing a new online identity.[310] The psychological impact of the network effect should not be underestimated. By way of illustration, Facebook's deactivation page — which shows photos of a user's closest friends and tells her that these friends will miss her if she deactivates her account — has apparently kept one million users per year from completing the deactivation.[311] To add to the confusion, Facebook has two separate procedures for deactivating and deleting accounts.[312] Moreover, if users leave due to privacy concerns, they have no guarantee that their information will actually be deleted from the network's database.[313] In short, users are locked into beautiful "walled gardens" along with all their friends.[314] As users are not free to leave, they cannot exert pressure on social networks to respect their privacy, and social networks have no incentive to improve their data use practices to compete with other networks. Their only incentive is to increase the network effect and make it more difficult for users to defect.

The centralized control in these "walled gardens" is a product of certain design choices, and users can be given more control by de-

---

308. Grimmelmann, *supra* note 138, at 1202; boyd, The Future of Privacy, *supra* note 101 ("Opting out of social media, opting out of online communities is quickly becoming akin to opting out of society."); *see also* Russell Bennett, *The Economics of Interoperability*, NO JITTER (Oct. 3, 2011), http://www.nojitter.com/post/231700141/the-economics-of-interoperability.

309. *See* Jeffrey Jarosch, *Novel "Neutrality" Claims Against Internet Platforms: A Reasonable Framework for Initial Scrutiny*, 59 CLEV. ST. L. REV. 537, 561 (2011).

310. Grimmelmann, *supra* note 138, at 1192–93; *cf.* SHERRY TURKLE, ALONE TOGETHER: WHY WE EXPECT MORE FROM TECHNOLOGY AND LESS FROM EACH OTHER 192 (2011) (quoting a social media user who sees Facebook as a part of her identity).

311. Luke Wroblewski, *Web App Masters: Design Lessons from 350 Million*, LUKEW (Mar. 23, 2010), http://www.lukew.com/ff/entry.asp?1033.

312. *Deactivating, Deleting, and Memorializing Accounts*, FACEBOOK, www.facebook.com/help/?page=185698814812082 (last visited Dec. 22, 2012).

313. Grimmelmann, *supra* note 138, at 1199; *see also Deactivating, Deleting, and Memorializing Accounts*, *supra* note 312 (explaining that some photos and notes may remain in Facebook's database even after a user permanently deletes her account); *see also Facebook Data Use Policy*, *supra* note 30 (stating that "some information may remain in backup copies and logs for up to 90 days" after an account is deleted).

314. Berners-Lee, *supra* note 159; *see also* ZITTRAIN, *supra* note 73, at 165 (warning that more controlled alternatives to the open Internet "block . . . the ability of outsiders to offer code and services to users, and the corresponding opportunity of users and producers to influence the future without . . . permission" from the party controlling this "[g]ated communit[y]").

sign.[315] The networks could be unlocked to reduce the network effect that currently ties users to them. New network designs could supplement the legal solution outlined above to give users more freedom to make choices with respect to their personal data. While many different solutions are currently being developed to address this problem, here I propose a combination of five architectural solutions that would allow users to:

> (1) Store their personal information locally and communicate with their friends directly through a distributed social network;
>
> (2) Export their personal information to a platform that they trust pursuant to data portability standards;
>
> (3) Continue communicating with their friends who remain in a centralized network pursuant to interoperability standards;
>
> (4) Protect their privacy when photos of them are taken in public places; and
>
> (5) For the users who elect to stay in a centralized social network, upload photos in a manner that prevents extraction of biometric data.

Though this Article addresses the specific problem of the use of face recognition technology in social networks, this architectural proposal has far broader applications. It can be extrapolated as a solution to other privacy problems caused by social networks and other online platforms that accumulate personal data. Web users could also apply this proposal to get more control over personal data to use it in novel ways for their own benefit.[316] More broadly, the undertaking to open up social networks and make them more transparent and interoperable could address Tim Berners-Lee's concern that these networks threaten to fragment the Web.[317] He has urged for public policy to preserve the "egalitarian principles" that transformed the Web from the one-site project he launched on his computer in 1990 into a global and indis-

315. Cohen, *supra* note 258, at 1436–37.

316. *See* Ian Katz, *Tim Berners-Lee: Demand Your Data from Google and Facebook*, GUARDIAN (Apr. 18, 2012), http://www.guardian.co.uk/technology/2012/apr/18/tim-berners-lee-google-facebook.

317. Berners-Lee, *supra* note 159.

pensable public resource.[318] This proposal presents one step in that direction.

1. Distributed Social Networks Directly Between PCs and Smartphones

The key problem with social networks is that they are designed to have users communicate with their friends through a third party, which is not bound by the social norms governing their friendships. Yet, most users do not experience their interaction on Facebook as public because, as danah boyd observed, the network has "differentiated itself by being private."[319] Instead, they think of this interaction as casual conversations with friends, and do not realize that everything they say is saved to their digital profile — information that can then be aggregated, searched, or used beyond their control in the far future. Professor Nissenbaum has expressed hope that social networks will eventually become more responsive to the norms that govern user expectations.[320] At the same time, she predicted that the discrepancy between social networks' practices and user privacy expectations will ultimately lead users to other networks that respect the established privacy norms.[321]

In the meantime, the Mobile and Social Computing Research Group at Stanford is developing such an alternative network with Musubi — an open and decentralized social network that allows sharing of status updates or photos without an intermediary.[322] Musubi thus enables users to share photos with their friends without channeling them through a third party that can extract biometric data from those photos and use that data for unauthorized purposes. The problem, however, is to make sure that users can move their data to these decentralized platforms and to give them an opportunity to continue communicating with their friends that stay behind.

2. Portability of Personal Data

While Musubi is an example of how users could interact with each other online without giving a third party control over their personal data, as a matter of fact, users have already gathered much of their data in social networking sites. These sites hold their profile in-

318. *Id.*; *see also* Katz, *supra* note 316.

319. danah boyd, *SNS Visibility Norms (A Response to Scoble)*, APOPHENIA (Sept. 9, 2007), http://www.zephoria.org/thoughts/archives/2007/09/09/sns_visibility.html.

320. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 228.

321. *Id.* at 229.

322. T. J. Purtell et al., *A Mobile Social Network on ESP: an Egocentric Social Platform*, MOBISOCIAL (Feb. 2012), http://mobisocial.stanford.edu/papers/pets12.pdf.

formation, photo albums, contacts, and various materials they have shared through status updates over the years. Facebook now allows users to get a copy of this data in HTML format, but so far users are not able to use their data in other platforms.[323] The threat of losing the online identities that users have built up over the years further contributes to user lock-in.[324] This could be remedied if social networks were subject to data portability standards that would allow users to export their data in a format that they could use in another network or in distributed social networks.[325]

Such standards have, for example, been incorporated into a new data protection regulation that has been proposed in the EU.[326] This regulation would allow users to export their data in a "format which is commonly used and allows for further use" or to have it transferred directly to another platform.[327] While the regulation does not specify any particular data portability standard, it provides that the European Commission may establish a standard format and mode of transmission between services.[328] Once a user obtains or transfers a copy of her personal data pursuant to this regulation, she should also be able to delete it from the original source, as the data will no longer serve the purpose for which it was originally collected.[329]

The use of data portability as a privacy solution is not uncontroversial. Professor Grimmelmann, for example, has argued that, because user profiles in social networks are highly intertwined, the ability to transfer one user's profile will violate her friends' privacy because it will inevitably drag along portions of their profiles.[330] There is certainly a question whether data in social networks belongs

---

323. *See, e.g.*, *Step for Step: "Complaint Against the Irish Authority in Brussels,"* EUROPE-V-FACEBOOK.ORG, http://www.europe-v-facebook.org/EN/Get_your_Data_/File_a_Comlaint/file_a_comlaint.html (last visited Dec. 22, 2012); *see also* Chris Saad, *Facebook's Claims About Data Portability Are False*, READWRITE (May 28, 2010), http://readwrite.com/2010/05/28/chris_saad_facebooks_claims_about_data_portability_are_false.

324. Grimmelmann, *supra* note 138, at 1192.

325. While some definitions of data portability also include the ability to automatically update users' information in several services, I discuss this requirement separately as "network interoperability" below. *See, e.g.*, Elias Bizannes, *Vision and Mission*, DATAPORTABILITY PROJECT, http://wiki.dataportability.org/pages/viewpage.action?pageId=3440714 (last modified Mar. 19, 2009) (login required) (describing "data portability" to include functions also known as "interoperability"); *see also* text accompanying note 336, *infra*; *cf. Recommendation*, COUNCIL OF EUR., *supra* note 10 (adopting a more limited working definition of data portability when stating that "[b]efore terminating their account, users should be able to easily and freely move the data they have uploaded to another service or device, in a usable format").

326. General Data Protection Regulation, *supra* note 201.

327. *Id.* at 53.

328. *Id.*

329. *Id.* at 51.

330. Grimmelmann, *supra* note 138, at 1194.

to the person uploading it or the person the data identifies.[331] In other words, if a friend uploads a photo of me, which of us has the right to export it?

While not an easy problem, it seems that data portability and third parties' privacy can be reconciled. You could, for example, be able to export all the photos that you uploaded to the network, but not tags of your friends in those photos — unless those friends allow you to export that additional information. You could further be able to export copies of photos of you that others have uploaded, but you would not be able to delete those photos (although you could delete your own tags). Likewise, you could be able to export your own status updates, but not your friends' likes or comments on those updates. Generally, the data portability standards could by default be based on the expectation that the person who provided the information to a social network likely already has her own copy of that information and, regardless, should have the right to take it back. It could further reflect the norm that social network users have been able to delete tags and other personally identifiable information about themselves even when others originally provided that information. Social networks are best suited to work out the technical details for these standards. Yet, they could be required to seek public comment and final approval from an agency of the type discussed in Part V.A.3 *supra*. They could do so through an electronic procedure to speed up the process. To provide more autonomy, sophisticated users may also be allowed to control how data portability is applied to their personal information through their privacy settings. In short, data portability standards can be structured to protect privacy.

3. Horizontal Interoperability Between Social Networks

While the ability to communicate through distributed social networks and to export personal data to such networks gives users some freedom, it does not completely liberate them from the network effect as all their friends continue to communicate within one closed centralized social network. The network effect would be weaker if the centralized network were interoperable with distributed and other social networks such that users could continue to selectively communicate with their friends even after they chose to leave the network.[332] Given

331. Ed Felten, *Scoble/Facebook Incident: It's Not About Data Ownership*, FREEDOM TO TINKER (Jan. 8, 2008), https://freedom-to-tinker.com/blog/felten/scoblefacebook-incident-its-not-about-data-ownership.

332. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 101 (discussing how "the vicious cycle of network effects" can make a "non-interoperable system that seem to be more to [to] actually become more popular for that very reason."); *see also* JOHN G. BRESLIN ET AL., THE SOCIAL SEMANTIC WEB 11–17 (2009).

that interoperability of social networks is a highly technical matter, it should not be micromanaged by the state.[333] Even so, the state could require social networks to be interoperable to allow seamless communication and leave them to develop the technical details.[334]

Interoperability would bring the promise of more user autonomy in social networks — which so far are only interoperable with third party applications. Professors Urs Gasser and John Palfrey have sought to define the somewhat nebulous term "interoperability" based on three case studies within information and communications technologies as well as relevant publications.[335] They conclude that while interoperability is a rather context-specific term, it generally can be conceptualized as "the ability to transfer and *render useful* data and other information across systems . . . , applications, or components."[336] The "ability . . . to render useful data" is of course the operative words for the discussion here, which focuses on users' ability to communicate between social networks.[337] From Professors Gasser and Palfrey's case studies — which were all in areas with strong network effects[338] — they concluded that increased interoperability generally provides users with greater "user choice and autonomy."[339] Their findings could be applied to social networks, which currently do not allow users to render their data useful. Despite being open for outside developers ("vertical interoperability"), social networks yield little opportunity for users to communicate between networks ("horizontal interoperability").[340]

The specific interoperability standards could be developed based on interoperable features that already exist in some social networks and be extended to other features and networks to allow users to communicate seamlessly with non-users outside their networks. Face-

---

333. PALFREY & GASSER, INTEROP, *supra* note 156, at 14.

334. *Id.* at 203 (stating that "the government's role is not to choose a specific technology but, rather, to ensure that data are able to flow between and among systems and that people are able to work better together across institutions, in the interests of the public at large").

335. GASSER & PALFREY, BREAKING DOWN DIGITAL BARRIERS, *supra* note 153, at 4.

336. *Id.* at 4 (emphasis added).

337. As mentioned in note 325 above, there is some overlap in the definitions of "data portability" and "interoperability," which often are discussed as subsets of each other. Separating these concepts in the narrow context of this Article helps to illuminate the nuances of which particular practices in social networks need to be refined in order to provide users with greater choice. Specifically, it shows that social networks currently provide some data portability, but the exportable data is not in a useful format. It further shows that while these networks are somewhat interoperable (primarily with third party apps), they are not horizontally interoperable with each other or other types of networks.

338. *See* GASSER & PALFREY, BREAKING DOWN DIGITAL BARRIERS, *supra* note 153, at 9.

339. *Id.* at 15.

340. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 70–71; Dana Petcu, *Portability and Interoperability Between Clouds: Challenges and Case Study*, 6994 TOWARDS A SERVICE-BASED INTERNET 62, 64 (2011).

book already allows users to continue receiving messages from their Facebook friends after they deactivate their accounts.[341] Facebook users can also receive messages from non-users on their Facebook e-mail accounts.[342] This allows users and non-users to share photos and links that can be attached to a message. However, Facebook users cannot friend non-users or share their status updates with them. Google Plus users, on the other hand, can add non-user e-mail addresses to their circles and share status updates, photos, and links with them.[343] Because Google Plus accounts are connected to a user's Gmail account, non-users can essentially also send messages to users. However, while the two networks are very similar and have roughly the same features, there is no interoperability between Facebook and Google Plus accounts that would permit users to view status updates from their friends in different networks or to share and tag photos. Nor will such interoperability likely develop without state intervention given the rivalry between the two companies.[344]

Social networks may resist interoperability on the argument that it could compromise user security, as they cannot authenticate users on other platforms. Leaving aside the fact that these platforms currently do not effectively authenticate their own users,[345] authentication between platforms could be achieved through open standards such as OpenID or OAuth.[346]

Interestingly, interoperability has often been described as a privacy problem rather than a solution.[347] But in fact, privacy problems

---

341. Marshall Kirkpatrick, *What Happens When You Deactivate Your Facebook Account*, READWRITE (May 6, 2010), http://readwrite.com/2010/05/06/what_happens_when_you_deactivate_your_facebook_acc (reporting that Facebook's deactivation notice states that "[e]ven after you deactivate, your friends can still invite you to events, tag you in photos, or ask you to join groups. If you opt out, you will NOT receive these email invitations and notifications from your friends"). Given that the forwarding of messages is enabled by default when users deactivate their accounts, this has not been a popular feature as users perceive that Facebook will not release them, even after deactivation. *See id.*

342. *How Does Email Work with Messages?*, FACEBOOK, https://www.facebook.com/help/?faq=212136965485956#How-does-email-work-with-messages? (last visited Dec. 22, 2012).

343. Mike Elgan, *How to Get Your Family and Friends on Google+*, DATAMATION, (Feb. 1, 2012) *available at* http://www.datamation.com/networks/how-to-get-your-family-and-friends-on-google-1.html (explaining that "Google+ lets you share posts with both users and non-users via e-mail") (last visited Dec. 22, 2012).

344. GASSER & PALFREY, BREAKING DOWN DIGITAL BARRIERS, *supra* note 153, at 10 (describing the rivalry that started when "Google lost the bidding war for a partnership with Facebook to Microsoft").

345. Ho B. Chang & Klaus G. Schroeter, *Creating Safe and Trusted Social Networks with Biometric User Authentication*, 6005 ETHICS AND POLICY OF BIOMETRICS 89, 91 (2011), *available at* http://www.bioid.com/assets/files/BioID-Creating-Safe-and-Trusted-Social-Networks-with-Biometric-User-Authentication-20100126.pdf.

346. BRESLIN, *supra* note 332, at 17 (citations omitted).

347. Gasser, Cortesi, & Palfrey, *supra* note 252; *see* PALFREY & GASSER, INTEROP, *supra* note 156, at 75.

related to interoperability often arise because of particular implementations that expose personal data to a greater number of parties.[348] Social networks, in particular, have focused on interoperability vis-à-vis third party developers who have been allowed to build on their open APIs.[349] This vertical implementation of interoperability, while beneficial for innovation, gives third parties access to user information, while chipping away at user control.[350] But interoperability also involves "seamless data transmission and easy extension and integration of data sources by *users*."[351] Thus, if network interoperability were implemented to allow users to keep their aggregated personal information on a platform that they trust and only send limited information to centralized networks to communicate with their friends, it should protect rather than expose their personal information.[352] Moreover, unlike cases where interoperability has contributed to privacy violations, here it would allow users to consciously send particular sets of data from one social network to another.[353] When choosing to communicate with friends in a centralized network, users would know that this particular information would be available to an intermediary. Thus, user data would flow within the context of selected social networks, with predictable recipients and transmission norms.[354]

Interoperability is also beneficial for innovation.[355] If networks were truly open to other networks at the users' choice (as opposed to interoperable with only a handful of companies), we might see more innovation in the development of new networks.[356] A healthy competition between social networks could also push for development of new features, which due to the required transparency and opt-in con-

348. GASSER & PALFREY, BREAKING DOWN DIGITAL BARRIERS, *supra* note 153, at 16.

349. *Id.* at 7.

350. In a recent incident, an app aggregated public Facebook profiles and location data from Foursquare to show information about female Facebook users who were geographically close to the person using the app. Erik Kain, *The Problem With The "Girls Around Me" App Isn't That Women Are Lazy About Privacy*, FORBES (Apr. 6, 2012, 2:15 PM), http://www.forbes.com/sites/erikkain/2012/04/06/the-problem-with-the-girls-around-me-app-isnt-that-women-are-lazy-about-privacy.

351. Gasser & Palfrey, *Breaking Down Digital Barriers*, *supra* note 155, at 5 (emphasis added).

352. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 81 (arguing "[o]ne might even be able to imagine interoperable systems with privacy-enhancing qualities").

353. For example, interoperability between Google products resulted in a privacy violation when personal contacts were automatically transferred from users' Gmail accounts to a new social network called Buzz. But in that instance, users did not select to transfer the data, and it travelled from one context (private e-mail contacts) to another context (public social network contacts). *Id.* at 82–84.

354. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 238–39.

355. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 111–29.

356. *See* Berners-Lee, *supra* note 159; *see also* PALFREY & GASSER, INTEROP, *supra* note 156, at 90.

sent may be based on privacy by design.[357] If successful, this could align the often-competing goals of privacy and innovation.

4. Privacy in Public

So far, I have outlined how social networks could be designed to allow users to opt out of data collection without foregoing their online social interaction. But even if a user were to successfully delete all her social network accounts, she may not completely avoid face recognition technology in social networks. Other users could continue uploading photos of her and tagging her. They could also upload other information about her and mention her in their status updates.[358] While social networks currently do not appear to apply face recognition technology to this type of non-user information, there is no nationwide legislation preventing this practice in the United States. The Council of Europe has asked its member states to provide guidance to social networks so that non-users can get an "effective means of exercising their rights without having to become a member of the service in question."[359] At the same time, U.S. legislators have already started thinking about how privacy in public can be protected from ubiquitous cameras in cell phones.[360] But collection of biometric information, in particular, may violate non-users' privacy because while a person may not have a privacy interest in her face that she exposes in public, she may nevertheless have a privacy interest in her biometric data that cannot be observed with a human eye.[361]

In this section, I discuss two technologies that individuals could use to protect themselves against unwanted photographing, which in turn would protect against extraction of biometric data. These two technologies provide different degrees of control and thus may be suitable for different purposes. It should be noted that unlike the other architectural solutions that I discuss in the previous Parts — which seek to enable users to communicate more freely online — the architectural solutions in this and the next Part operate as constraints on behavior to protect user privacy. As these architectural solutions restrict rather than enable behavior, they need to be limited in scope to avoid impeding innovation, creativity, and free speech.

---

357. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 228–29.

358. boyd, The Future of Privacy, *supra* note 101 (discussing that users participate in Facebook "regardless of [their] personal choices").

359. *Recommendation*, COUNCIL OF EUR., *supra* note 10.

360. Calo, *supra* note 279, at 1037 & n.54 (discussing how Congress considered the Camera Predator Alert Act of 2009 to require cell phones to make an analog camera sound when taking photos).

361. *See supra* Part IV.

The first technology is an anti-paparazzi device that emits a flash when it senses a camera lens, thereby ruining the image.[362] While it is highly effective in preventing photographing — and therefore provides a strong protection against extraction of biometric data — it may be too drastic under most circumstances. If these devices became cheap enough for daily use, photographers would not be able to take artistic photos of public places, and journalists would not capture newsworthy events. Excessive use of this device would thus hamper creativity and news reporting.[363] On the other hand, there may be situations when individuals truly need this protection. Domestic violence victims and individuals in victim protection programs, for example, may need to avoid today's ubiquitous camera phones with direct connection to social networks. Other individuals may get by without this protection on a daily basis, but may need it to stay anonymous during risky activities, such as protests against authoritarian regimes.

The second technology would allow an individual to convey a message to the photographer and is therefore less drastic.[364] This technology is a camera phone patented by Apple in 2011.[365] The design of the phone would allow it to receive messages via infrared light.[366] One such message could for example read: "Please do not collect my biometric data."[367] While that message would not guarantee that biometric data would not be extracted, people are often happy to comply with simple requests.[368] Of course, it would only work for the cameras containing the relevant technology, which could be mandated by law once it became sufficiently cheap and portable.[369] One could also imagine legislation prohibiting extraction of biometric data against a person's will.[370] The person's lack of consent could then be

---

362. *See* Shwetak N. Patel et al., *BlindSpot: Creating Capture-Resistant Spaces*, *in* PROTECTING PRIVACY IN VIDEO SURVEILLANCE 185, 187–88 (Andrew Senior ed., 2009) (describing a method for detecting the "retro-reflective" surfaces of camera lenses and emitting an infra-red light beam to blind detected lenses).

363. Ironically, it would also require the person who is trying to avoid photographing to constantly carry a camera to detect other camera lenses.

364. *Apple Working on a Sophisticated Infrared System for iOS Cameras*, PATENTLY APPLE (June 2, 2011), http://www.patentlyapple.com/patently-apple/2011/06/apple-working-on-a-sophisticated-infrared-system-for-ios-cameras.html.

365. *Id.*

366. *Id.*

367. *See* Jennifer Halbleib, *FOI Topics and Links of the Week*, THE FUTURE OF THE INTERNET (Jun. 6, 2011), http://futureoftheinternet.org/foi-topics-and-links-of-the-week-16.

368. Jonathan Zittrain, Harvard Law Professor, Jonathan Zittrain: The Web as Random Acts of Kindness, (July 22, 2009), *available at* http://www.ted.com/talks/jonathan_zittrain_the_web_is_a_random_act_of_kindness.html.

369. For example, Congress has considered a Camera Predator Alert Act of 2009 to require cell phones to emit an analog camera sound when taking photos. Calo, *supra* note 279, at 1037 & n.54.

370. This would be similar to pending "Do Not Track" bills that would allow users to make changes to their browser settings to avoid tracking cookies for advertising. *See, e.g.*,

evidenced by such a message. These messages would not interfere with photographer creativity by spoiling their photos and thus could be used far more widely than the anti-paparazzi device discussed above.

The value of these two technologies is to allow users more control over photos taken of them in public without resorting to restrictive legislation. By way of comparison: French law sometimes requires a person's consent before she is photographed in public.[371] Needless to say, such a law could hamper creativity and news reporting far more drastically than the occasional use of an anti-paparazzi device.

5. Privacy by Design in Photos

At this point, I need to acknowledge that, even if we equip users with distributed social networks and data portability and interoperability standards, realistically many users will still take the path of least resistance and stay in centralized social networks despite distrusting their privacy practices. But the very purpose of equipping users with the architectural solutions outlined above is to put pressure on social networks to respond to privacy concerns in order to keep users. The idea is that the combination of free choice to leave the network and legal requirements for transparency and opt-in consent will make privacy a primary concern for social networks.

But users who stay in centralized social networks — albeit with improved privacy practices — may still need some self-help remedies to control their personal information. As danah boyd and Alice Marwick's studies have shown, some social network users have already come up with their own alternative protection measures; one teenage girl that Marwick interviewed deactivated her Facebook account every night to prevent online activities beyond her control.[372] Similarly, users may need methods to protect themselves against unwanted collection of biometric data when they share photos with their friends.

A rather straightforward solution is to share only photos that cannot be subjected to face recognition technology. Some users already do this by only sharing only photos where they look away or wear ski

---

Mark Hachman, *"Do Not Track" Legislation is on the Move*, PCMAG.COM (May 6, 2011, 7:55 PM), http://www.pcmag.com/article2/0,2817,2385045,00.asp.

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

372. danah boyd & Alice Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies 20 (May 9, 2011) (unpublished symposium draft), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

goggles.[373] More sophisticated make-up and hairstyles that avoid face recognition are also being developed with CV Dazzle, which is "camouflage from computer vision."[374] While a user may easily recognize a friend wearing the CV Dazzle make-up, the current face recognition technology in social networks cannot even *detect* a camouflaged face in a photo — much less *recognize* it.[375] Thus, just like fashion has previously evolved in response to other social changes, it could now evolve to protect user privacy against technology.[376] Admittedly, it could also become a cat and mouse game whereby technology then evolves to detect and recognize camouflaged faces.

Another solution is to allow users to redact photos that they share to make them useless for automatic face recognition, while still serving the social function for which they are shared. While a blurred or pixelated face in a photo may sometimes avoid automatic face recognition, it would also defeat the purpose of sharing the photo because it would look strange and may not communicate the person's emotions.[377] Furthermore, if the blurring or pixelation is only slight, it may not be sufficient to trick the face recognition technology.[378] Instead of trying to blur her face, a user could cover it with a "computer generated face" that would "hid[e her] . . . identity yet preserv[e] the gaze direction and expression."[379] It would allow the user to share her experiences with friends without exposing her biometric data. As her friends have contextual knowledge about her, they may still recognize her from her body shape, clothes, and other items in the photo.[380] This would protect not only against face recognition technology within social networks, but also from third parties who may illicitly down-

373. J. Birgitta Martinkauppi et al., *Skin Color in Face Analysis*, *in* HANDBOOK OF FACE RECOGNITION, *supra* note 20, at 250 (noting that "[b]eards, eyeglasses, or jewelry may obscure facial features"); *see also* Doc Searls, *Clothing is a Privacy System*, DOC SEARLS WEBLOG (Mar. 15, 2012), http://blogs.law.harvard.edu/doc/2012/03/15/clothing-is-a-privacy-system.

374. Adam Harvey, *CV Dazzle: Camouflage from Computer Vision*, CV DAZZLE (Sept. 9, 2012), http://www.cvdazzle.com.

375. Adam Harvey, *CV Dazzle vs PhotoTagger*, VIMEO, http://vimeo.com/12308527 (last visited Dec. 22, 2012).

376. *See* Minh-Ha T. Pham, *If the Clothes Fit: A Feminist Takes on Fashion*, MS MAGAZINE (Jan. 17, 2012), http://msmagazine.com/blog/blog/2012/01/17/if-the-clothes-fit-a-feminist-takes-on-fashion (discussing how "in the 1980s, women appropriated men's styles of dress in an attempt to access the social and economic capital that lay on the other side of the glass ceiling"); *see also* Searls, *supra* note 373 ("[C]lothing gives us a means for doing what techies call selective disclosure . . . while just as selectively keeping some things undisclosed. Or, therefore, private.").

377. Andrew W. Senior & Sharathchandra Pankanti, *Privacy Protection and Face Recognition*, *in* HANDBOOK OF FACE RECOGNITION 682 (Stan Z. Li & Anil K. Jain eds., 2005).

378. *Id.*

379. *Id.*

380. *See* FACE PROCESSING, *supra* note 15, at 8–9.

load photos from a network using socialbots,[381] or other means, to apply their own face recognition technology to those photos. The problem would be to communicate to friends that the face in the photo is computer-generated to avoid confusion. This could turn out to be a minor problem given that many users already shield their identities by taking on pseudonyms that sound like real names without much reaction from social network friends who also know them offline.[382] Another problem is that friends may still upload photos of that user,[383] although this may fairly easily be addressed by privacy settings that prohibit tagging without user consent.

C. Market — Pay or Play

The architectural solutions outlined above are intended to complement the legal notice and consent requirements to give users free choice with respect to social network privacy practices. But users could also have more economic choice *within* the networks if they were structured as "freemiums."[384] Users could then elect to use a social network free of charge or subsidize their use by paying the lost advertising revenue for particular chunks of personal data that they do not wish to be collected or used. They could also prevent any use of their data by paying the full price of the service as a monthly fee. This would allow users to choose how much privacy they want to maintain based on their own personal circumstances and sensibilities. It would also indicate to social networks when certain data use is universally unwelcome because many users would pay to avoid it. If many users were to pay to avoid the collection of their biometric data, social networks may ultimately remove the face recognition feature because they would not have sufficient biometric data to keep it running. One social network has already implemented a similar business model — allowing users to decide when they want to give out their personal information to advertisers in exchange for discounts.[385]

---

381. *See supra* Part II.B.

382. *See* danah boyd, *"Real Names" Policies Are an Abuse of Power*, APOPHENIA (Aug. 4, 2011), http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html.

383. *See, e.g.*, boyd, The Future of Privacy, *supra* note 101 ("Even if you opt out, people can still write about you . . . . You become part of the network regardless of your personal choices.").

384. *See, e.g.*, Geoff Duncan, *Facebook Highlights: The Beginning of Paid Social Networking?*, DIGITAL TRENDS (Mar. 11, 2012), http://www.digitaltrends.com/mobile/facebook-highlights-the-beginning-of-paid-social-networking; *see also* Jason Kincaid, *Startup School: Wired Editor Chris Anderson on Freemium Business Models*, TECHCRUNCH (Oct. 24, 2009), http://techcrunch.com/2009/10/24/startup-school-wired-editor-chris-anderson-on-freemium-business-models.

385. *See* PERSONAL, *supra* note 278; *see also* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. TIMES (Feb. 13, 2012),

In theory, this would not cause social networks to lose any revenue, allowing them to continue provide social networking services and to innovate. In practice, however, increased transparency regarding how much personal data social networks aggregate — and how they benefit from it — could drive away some of the users, which is probably why social networks have not already adopted freemium models.[386] But this signals a market failure where social networks consciously keep users in the dark to make higher profits. Normally, such market failures call for regulators to step in to correct the information asymmetry.[387]

More problematically, the freemium model may force individuals to sacrifice their privacy if they cannot afford to pay. This becomes a bigger problem if we consider that social networks are international, and a few dollars may equate to a much higher price in other countries. Many users in developing countries may not have credit cards or may be unwilling to enter credit card information online.[388] From a United States perspective, however, a freemium model closely mirrors commercial norms that have evolved offline. It is, for example, not uncommon for stores to have customer value cards that collect information about customers' purchases in exchange for a discount.[389] Customers can elect not to have that information collected in exchange for paying a higher price for products. But to the extent that these offline norms are unsatisfactory — because we may want the online world to be a better and fairer place — we could also imagine a social network built on a freemium model that does not involve any sharing of personal information.[390] Indeed, one former Facebook executive is developing a social network that offers basic social network functions for free — and without using personal information — and

---

http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

386. Turow, *supra* note 273, at 3 ("When offered a choice to get content from a valued site [that tracks and shares user data] or pay for the site and not have it collect information, 54% of adults who go online at home said that they would rather [not use the service at all].").

387. *See* 15 U.S.C.§ 45(a)(1) (2006) (prohibiting "deceptive acts or practices").

388. Japhet E. Lawrence & Usman A. Tar, *Barriers to Ecommerce in Developing Countries*, 3 INFO., SOC'Y & JUST. 23, 26, 29 (2010), *available at* http://www.londonmet.ac.uk/fms/MRSite/acad/dass/ISJ%20Journal/V3N1/03_Barriers%20to%20E-commerce%20in%20developing%20countries_Lawrence&Tar.pdf.

389. *See Face Facts: A Forum on Facial Recognition Technology* (Fed. Trade Comm'n audio recording Dec. 8, 2011) (transcript available at http://htc-01.media.qualitytech.com/COMP008760MOD1/ftc_web/transcripts/120811_FTC_sess3.pdf) (discussing how supermarket loyalty cards present "an easy method of tracking people").

390. *See* Berners-Lee, *supra* note 159 ("We create the Web, by designing computer protocols and software; this process is completely under our control. We choose what properties we want it to have and not have.").

instead charges users for optional advanced features.[391] Additionally, the architectural solutions that I outline above could correct for the unfairness of the freemium model. Thus, if a user were to disagree with a data use practice and could not afford to pay to avoid it, she could export her data and continue communicating with her friends through a free distributed social network relying on the interoperability standards.

While these freemium models would require cooperation from social networks or a legal mandate, we can also imagine structural changes brought about by user activism. One example of this is TOSAmend, which is a plug-in that allows users to substitute their unconditional agreement to a website's terms and conditions with a rejection of those terms before entering into an online transaction.[392] Professors Zev Eigen and Florencia Marotta-Wurgler have opined that if an online company were informed that a customer rejected its click wrap terms and nevertheless delivered a product or service to that customer, the conflicting provisions would cancel each other out and leave intact only the undisputed terms of the agreement.[393] Awareness of an employee does not appear to be necessary as Section 14 of the Uniform Electronic Transactions Act allows "electronic agents" to enter into an agreement even without direct supervision of its human masters.[394] One could imagine a similar plug-in that would allow users to attach terms restricting data use when they share photos in social networks. While these data use terms would likely not be binding on a social network until they are recognized by courts, users would have a good argument because typed terms tend to prevail over preprinted terms when the two are in conflict.[395] A company could, of

391. *See About*, PATH, https://path.com/about (last visited Dec. 22, 2012); *see also* Geoffrey A. Fowler, *Path Gets "FriendRank" and a Revenue Stream*, WALL ST. J. (Mar. 11, 2011, 6:30 AM), http://blogs.wsj.com/digits/2011/03/11/path-gets-friendrank-and-a-revenue-stream.

392. Kevin Owocki, *#occupytheweb with Us: Change the Terms of Online Contracts*, OWOCKI DOT COM (Dec. 3, 2011), http://owocki.com/2011/12/03/occupytheweb-change-the-terms-of-online-agreements.

393. Eigen & Marotta-Wurgler, *supra* note 269.

394. UNIF. ELEC. TRANSACTIONS ACT § 14(1) ("A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements."). The Uniform Electronic Transactions Act has been adopted by 47 states. *Uniform Electronic Transactions Act*, NATIONAL CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/uniform-electronic-transactions-acts.aspx (last visited Dec. 22, 2012). It defines "Electronic agent" to mean "a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual." UNIF. ELEC. TRANSACTIONS ACT § 2(6).

395. *See, e.g.*, Bluewaters, Inc. v. Boag, 320 F.2d 833, 835 n.4 (1st Cir. 1963) (noting that "[it is well established that] typewritten additions normally prevail if there is a conflict with printed provisions").

course, make it difficult to change its privacy policy by including a clause that prevents any modifications of the terms. But Professors Eigen and Marotta-Wurgler hypothesize that courts may find such a clause unconscionable.[396]

D. Norms — Pushing for a Race to the Top

When looking at face recognition technology in social networks, it is essential to consider whether there are norms to address this privacy problem. Norms can play a powerful role by constraining behavior that the law lacks resources or motivation to regulate.[397] They can be external, such as encouragement or social disapproval in response to undesirable behavior.[398] But they can also become internalized such that they prevent a person from doing something out of "guilt or shame."[399] Internalized norms tend to be more effective because rather than punishing behavior after the fact, they can prevent it altogether.[400] Indeed, most of our privacy protections come not from laws or technological constraints, but from norms that evolve gradually in response to various changes in the society.[401] It is social privacy norms that stop your colleagues from clustering outside your office door to eavesdrop on a private phone conversation with your spouse. It is also mostly norms that keep women out of the men's room when there is an endless line to the ladies' room. And it is norms that prevent fellow subway passengers from reading e-mails on your smartphone over your shoulder during a morning commute.

Yet, the practice of sharing personal and intimate information in social networks has sometimes led to the conclusion that strong offline privacy norms do not apply online.[402] Worse still, some commentators argue that the use of technology has changed overall privacy norms such that people now generally have less of an expectation of privacy.[403] Even "though we often trade convenience for control," Internet users frequently agonize over new technologies that

396. Eigen & Marotta-Wurgler, *supra* note 269.

397. *See* Lipton, *Blogging*, *supra* note 254, at 241; *see also* LESSIG, *supra* note 7, at 122.

398. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 75, at 94.

399. *Id.*

400. *See* Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2030 (1996).

401. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 3. *But see* Lipton, *Blogging*, *supra* note 254, at 244 ("[N]orms can develop quickly with few formalities, unlike laws which require a combination of political will and congressional effort to come into being.").

402. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 106.

403. *See id.* at 106–07. Indeed, scholars have observed that new norms are developing online, such as norms regulating the hijacking of blogs. *See* Lipton, *Blogging*, *supra* note 254, at 247–48.

they experience as privacy violations.[404] And yet, privacy skeptics dismiss these complaints, arguing that user actions speak louder than their demand for privacy.[405] Privacy proponents, on the other hand, argue that user behavior in social networks does not indicate an erosion of privacy norms because studies show that users are not sufficiently informed about online privacy practices.[406] For example, research at CMU suggests that clearer privacy notices lead users to select privacy protective services.[407] Moreover, users may simply not have an alternative avenue for socializing with many of their friends, who have mostly abandoned telephones and other casual means of communication.[408] Network effects therefore force users to communicate via these services even though they violate user privacy expectations.[409] If so, there appears to be a discrepancy between privacy norms and practices.

Conceptually there is a difference between "descriptive" and "prescriptive" norms.[410] Descriptive norms represent "behavioral regularities, habits, or common practices, with no underlying expectation."[411] Conversely, prescriptive norms, as the name suggests, "prescribe, mandate, or require that certain actions be performed."[412] User desire for greater privacy in social networks, matching their offline privacy expectations, can be characterized as prescriptive norms. User acquiescence to the current state of affairs — where they have little control over their personal information — are merely descriptive norms.

I submit that if users were more informed about privacy practices in social networks and had more choice with respect to their online

404. Berkman Center, *John Palfrey on Legal Design for Delineating Public and Private*, BERKMAN CENTER FOR INTERNET & SOC'Y (Jun. 22, 2011), http://cyber.law.harvard.edu/node/6930; *see also* Ian Paul, *Girls Around Me App Voluntarily Pulled After Privacy Backlash*, PCWorld (Apr. 2, 2012, 5:25 AM), http://www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html.

405. *See* NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 105.

406. *Id.* at 106–07.

407. Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 254 (2011) ("[This] study indicates that when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."), *available at* http://www.guanotronic.com/~serge/papers/isr10.pdf. However, a recent European study showed that while people generally prefer sites with better privacy practices, they prefer cheaper online services even if these services compromise their privacy. DR. NICOLA JENTZSCH ET AL., EUROPEAN NETWORK AND INFO. SEC. AGENCY, STUDY ON MONETISING PRIVACY — AN ECONOMIC MODEL FOR PRICING PERSONAL INFORMATION 37 (2012), *available at* www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport.

408. *See, e.g.*, Turkle, *supra* note 310, at 197–98.

409. *See supra* text accompanying notes 307–14.

410. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 112, at 138–39.

411. *Id.* at 138.

412. *Id.*

socializing, they would exert pressure on social networks to conform to their prescriptive privacy norms. In that sense, the legal, architectural, and market solutions outlined above would bolster the existing privacy norms.[413] As part of the legal solution, the transparency requirement would allow users to see how their biometric data is extracted and used.[414] The opt-in consent and the architectural and market alternatives would give users more bargaining power in social networks.[415] Together, these solutions would allow users to compare social network practices against their own privacy expectations and to socially sanction violations of privacy norms by going elsewhere. This proposal would not seek to change the existing privacy norms. Rather, it would simply create a landscape where these norms can better control behavior.

In addition to the secondary effects of the legal, architectural, and market solutions discussed above, we can also think of solutions that directly allow users to police violations of social norms. Schools, for example, could educate children about how social networks use personal data.[416] While hundreds of millions of people use social network sites,[417] their business model is a mystery to many adults — not to mention children. Online companies have already started providing this type of education,[418] which is commendable. But given that schools are largely responsible for preparing children to become responsible citizens,[419] they should make sure that pupils get a complete and unbiased view of social network privacy practices. And to the extent that schools do not have expertise to teach online privacy to children, universities could step in to provide educational material that

413. *See* LESSIG, *supra* note 7, at 123.

414. *See supra* Part V.A.1–2.

415. *See supra* Part V.B–C.

416. *See* Gasser, Cortesi, & Palfrey, *supra* note 252, at 32, 35 ("[T]eachers play a crucial role in educating young people about privacy."); *see also* Jacqueline D. Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 979–80 (2009) [hereinafter Lipton, *Paparazzi*]; McDonald & Cranor, *supra* note 263, at 27 ("One younger participant said in frustration that she did not learn about how to protect her online privacy in school, she was just taught typing."); Urmee Khan, *Seven in 10 Parents Demand Compulsory Online Privacy Lessons*, GUARDIAN (Nov. 30, 2009), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/6684533/Seven-in-10-parents-demand-compulsory-online-privacy-lessons.html.

417. *See* Emil Protalinski, *Facebook Has over 845 Million Users,* ZDNET (Feb. 1, 2012, 6:13 AM), http://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332.

418. *See, e.g.*, *Good to Know*, GOOGLE, http://www.google.com/goodtoknow (last visited Dec. 22, 2012); MICROSOFT SAFETY & SEC'Y CTR., http://www.microsoft.com/security/default.aspx (last visited Dec. 22, 2012); THINKB4U, http://www.thinkb4u.com (last visited Dec. 22, 2012).

419. *See, e.g.*, LESSIG, *supra* note 7, at 129.

schools can use and build upon.[420] Various non-profit organizations have already started educating children and adults about the privacy risks of technology.[421] As this knowledge becomes more widespread, user privacy norms will likely gain more prominence.

The purpose of relying on existing social norms rather than proposing additional legislation is to strike a better balance between privacy and innovation. Strict legislation can deter new businesses that do not have the resources to defend against lawsuits. Norms, on the other hand, have a different constraining effect. Users cannot sue a company for violating a social norm. Instead, users will sanction a company by going to a competitor and by voicing their disappointment online.[422] It would therefore be in a company's interest to abide by social norms when designing a new platform. And while most companies would seek to comply with social norms to make a profit, startup companies would not have to fear excessive litigation costs that may come with a legal solution.

At this point, one may wonder why existing norms belong in a proposed regulatory solution. If these privacy norms already exist, is it not just a matter of time before Internet users will adjust how much they share so that their personal information cannot be misused in violation of these norms?[423] That would be true if learning how to share information online were like learning how to ride a bike. Cycling for the first time, you may fall down and bruise your knees, but then hop back on again. Eventually, the bruises heal and you will have learned how to balance. But when using the Internet, it is not obvious when you are doing something wrong — you do not fall to the ground or bruise when a company secretly extracts sensitive information from your photos. Yet, the virtual bruises may never heal; the personal in-

420. *See* ZITTRAIN, *supra* note 73, at 245 (arguing that "[o]ur Universities are in a position to take a leadership role in the Net's future" and they should see the Internet "as central to their mission of teaching their students and bringing knowledge to the world"); Lipton, *Paparazzi*, *supra* note 416, at 982 ("Academic institutions are another set of nonprofit organizations that can play a public-education role. They can assist in developing statements of best practices about online privacy, as well as disseminating information to the public about these issues.").

421. *See, e.g.*, *Consumer Privacy*, CTR. FOR DEMOCRACY & TECH., https://www.cdt.org/issue/behavioral-advertising (last visited Dec. 22, 2012) (explaining the process of behavioral advertising); *Scope & Sequence*, COMMON SENSE MEDIA, http://www.commonsensemedia.org/educators/scope-and-sequence (last visited Dec. 22, 2012) (providing educational resources for online privacy and security); *Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/privacy (last visited Dec. 22, 2012) (outlining how novel technologies can be used to collect private information); GETNETWISE, http://www.getnetwise.org (last visited Dec. 22, 2012) (information on privacy, security, spam for children and adults); *Computer and Internet Security*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/privacy-rights-fact-sheets (last visited Dec. 22, 2012) (providing fact sheets on various privacy issues).

422. *See, e.g.*, Paul, *supra* note 404.

423. *See* Lipton, *Paparazzi*, *supra* note 416, at 983.

formation can be aggregated, transferred to other companies, archived, searched, and taken out of context decades later.[424] It could, for example, be used in an embarrassing public campaign against the user, or secretly relied upon in an employment decision without giving the user an opportunity to respond. Children, in particular, could fall victim to data use practices, not least because they will be the first generation to have "digital dossiers" compiled over their entire life span.[425] Though in the short term, children may not necessarily be worse off than adults or the elderly, who may have different misconceptions about how the Internet operates based on their lifelong experiences in the offline world. All these users must be educated and empowered to enforce their existing privacy norms in cyberspace so that they, in the words of Professor Solove, can act as the "norm police."[426]

E. No Secret Laws — Transparency in Privacy Regulation

Though I believe this multifaceted proposal would be more effective than a mere legal reform, its non-legal aspects would need to be implemented with care to expose their underlying policies to the public in order to avoid effectively adopting secret quasi-laws. While sometimes less effective, legal reform has the advantage of going through a democratic legislative process that provides opportunity for debate and public comment. Even when agencies articulate legal rules, there are administrative law requirements that fetter agency power and make their decision-making process more transparent.[427] By seeking non-legal solutions, my proposal raises at least two transparency issues that must be addressed: first, regulation by architecture can create the illusion that the state is not making policy choices; and second, regulation by norms does not provide a clear opportunity for public comment in the legislative process.

While most of the non-legal solutions outlined above could be implemented by extra-legal efforts and cooperation, to be really effective they need to be mandated by law.[428] For example, privacy terms submitted through a plug-in like TOSAmend could be upheld by a court, making them legally binding on social networks. Likewise, the legislature could mandate data portability and interoperability stand-

---

424. *See id.*

425. JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 47, 53–54, 62 (2008); SOLOVE, THE DIGITAL PERSON, *supra* note 78, at 1–3.

426. SOLOVE, FUTURE OF REPUTATION, *supra* note 80, at 6.

427. *See* Nat'l Petrol. Refiners Ass'n v. FTC, 482 F.2d 672, 683 (D.C. Cir. 1983), *cert. denied*, 415 U.S. 951 (1974).

428. *See* LESSIG, *supra* note 7, at 132.

ards to make it easier for users to switch between social networks. This type of "indirect" legal regulation can sometime be more effective than "direct" legislation.[429]

However, to the extent that law is used to mandate the architectural and market solutions, it needs to be transparent. Otherwise, the government is allowed to take advantage of non-legal constraints to regulate behavior "at no political cost."[430] This is mainly a problem when the indirect regulation seeks to do something the government has no right to do by direct regulation.[431] But indirect regulation is perfectly fine if it is used for legitimate purposes and is transparent.[432] Transparency is particularly important when, like here, the regulation seeks to strike a fine balance between two important interests, which are sometimes in conflict.[433] Thus, if indirect regulation is introduced to mandate the architectural and market solutions outlined above, it should be explicit about the privacy interests that it seeks to protect so that its effect on innovation and other interests can be openly evaluated. The key is that indirect regulation should not "interfere with the ordinary democratic process by which we hold regulators accountable."[434]

The second transparency issue with my regulatory proposal is that it largely relies on norms to address privacy problems, whereas the process for developing social norms is rather obscure. Unlike legal rules that are produced through highly structured legislative or judicial processes, norms often evolve organically without any debate or clear opportunity to provide public comment.[435] This has led scholars to conclude that the policy justifications for norms are less apparent.[436] However, this overlooks the fact that norms can only develop and be maintained if there is overall consensus among the participants for the policies that those norms promote.[437] It is thus very different from laws, which can be passed solely by dint of powerful lobbying groups

---

429. *See id.* Lessig describes regulation as "direct" when "it tells individuals how to behave and threatens punishment if they deviate from that behavior." *Id.* "Indirect" regulation, by contrast, mandates changes to the market, architecture, or norms, which in turn regulate behavior. *Id.*

430. *Id.* at 135–38 (emphasizing that "[c]ode-based regulation — especially of people who are not themselves technically expert — risks making regulation invisible").

431. *See id.* at 135.

432. *See id.*

433. However, horizontal interoperability between social networks may align interests in privacy and innovation because it can protect users' privacy and lower the barrier to entry for new social networks. *See supra* Part V.B.3.

434. LESSIG, *supra* note 7, at 138.

435. *See* Lipton, *Blogging*, *supra* note 254, at 244.

436. *See, e.g.*, *id.*

437. *See* Alex Geisinger, *A Group Identity Theory of Social Norms and Its Implications*, 78 TUL. L. REV. 605, 612 (2004) (noting that norms "are simply a reflection of the behavioral preferences of the majority of group members").

and then apply universally until the law is amended or overruled in court.[438] So if there were no support for privacy norms protecting against the extraction of biometric data from photos in social networks, users would simply not object to these practices when learning about them and instead would consent to the continued collection of their biometric data. Whether this is the case remains to be seen once we have mandated transparency and facilitated choice — both of which will serve as mechanisms for establishing what privacy norms Internet users truly support.

VI. CONCLUSION

In an information-driven globalized world, social networks provide an invaluable communication tool. They organize our social lives in a portal that allows us to stay in touch with family and friends, with a relatively small time commitment and regardless of where in the world we find ourselves. Long gone are the days of handwritten love letters and printed telegrams. Even phone calls and e-mails are now less commonly used for casual communication.[439] Instead, people use online status updates to ask their friends "Who else is going to Coachella?" or download the BirthWatch app to have their friends follow the progress of their pregnancy. But because users do not pay for their social network use, they literally are the "product" being sold![440] Social networks have a commercial interest in aggregating user personal information to sell advertising.[441] Face recognition technology, in particular, serves this function by making it easier to upload and tag many more photos than before.[442] But as social networks apply face recognition technology to photos that users share with their friends, social networks alter the nature of the shared information and share it with additional recipients — thus violating the user's privacy.[443] Users, however, do not fully understand this process and so do not seek to protect themselves by legal action — even in states that have specific legislation with respect to biometric data. Users further cannot freely exercise their consumer choice because they are locked into the social network that their friends use and cannot meaningfully

438. *See, e.g.*, LAWRENCE LESSIG, REPUBLIC, LOST: HOW MONEY CORRUPTS CONGRESS — AND A PLAN TO STOP IT 45–48 (2011).

439. *See* TURKLE, *supra* note 310, at 197–98.

440. Jonathan Zittrain, *Meme Patrol: "When Something Online Is Free, You're Not the Customer, You're the Product,"* THE FUTURE OF THE INTERNET (May 21, 2012), http://futureoftheinternet.org/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product.

441. *See Ballmer: They Paid How Much for That?*, BLOOMBERG BUSINESSWEEK (Oct. 22, 2006), http://www.businessweek.com/magazine/content/06_43/b4006066.htm.

442. Mitchell, *supra* note 9.

443. *See supra* text accompanying notes 169–72.

export the personal data that they have been uploading to this network for years.[444] If users were to leave, the network could still abuse their personal data, and users would be cut off from their online social spheres. That is a sad state of affairs.

This Article makes two main contributions. First, applying the contextual integrity theory, it argues that face recognition technology in social networks needs to be regulated because it connects an otherwise anonymous face to a range of personal information online. Second, it proposes a combination of legal, architectural, market, and norm-driven solutions that could protect user privacy with respect to face recognition technology in social networks. Most of these solutions are interdependent and thus must be implemented concurrently to solve this problem. However, a couple of the solutions are intended only to protect particularly vulnerable users and are not essential to the overall effectiveness of this proposal. Similarly to previous work, this Article offers improvements to our current privacy model that require more informative notice to users and specific opt-in consent before collecting and using personal information. More importantly, notice and consent, however improved, will never solve this problem so long as the network effect locks users into one social network. The main contribution of this Article, therefore, is to offer solutions to reduce the network effect in centralized social networks, complementing the legal notice and consent requirement. Accordingly, the architectural and market solutions of this proposal are aimed at lowering the switching costs between social networks by allowing users to take their data and go to a network that they trust, while continuing to communicate with their friends who remain in the centralized social network. Once users are truly free to leave, they will be able to exercise the improved notice and consent framework in a meaningful way to demand that social networks respect their expectations of privacy.

To achieve this, many players need to be mobilized. The state will need to pass baseline privacy regulations that include more specific notice and consent requirements, as well as mandates for data portability and interoperability. The state will also need to introduce public education programs to inform children and adults about online privacy. The state's role will be to make policy decisions ensuring the right mix of legal, architectural, market, and norm-driven solutions. The technical implementation of the notice and consent and the data portability and interoperability standards will then be left to companies.[445] The stick will be more stringent laws and rigorous enforcement, while

444. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 101; *see also* LESSIG, *supra* note 7, at 232 (stating that "[t]he power of commerce is not behind [protecting privacy] . . . . Laissez-faire will not cut it.").

445. *See* PALFREY & GASSER, INTEROP, *supra* note 156, at 14.

the carrot will be that, as society becomes more informed and concerned about online privacy, users might favor companies that take the lead on this issue.[446] Armed with more choice due to lower switching costs between social networks and with information about what happens with their data, users will have the power to enforce the privacy norms that already govern their offline activities. I realize that this is an ambitious call to action, but if all these pieces were to fall into place, it could be a game-changer for online privacy. Even if the full proposal could not be implemented at this point, this Article is intended to start a conversation about how online privacy can be protected by creating a landscape where users have better choices.

Face recognition technology and online privacy, more generally, have recently been getting a lot of attention from media and regulators. The Subcommittee on Privacy, Technology and the Law of the Senate Committee on the Judiciary recently conducted a hearing on the privacy implications of face recognition technology.[447] The FTC is further considering possible legislative responses to this technology.[448] While addressing only the narrower issue of face recognition technology in social networks, this Article seeks to show that mere regulatory responses are insufficient. Rather, the law must be supplemented by education and availability of viable alternatives to monopolistic social networks.[449] The mixed proposal presented in this Article is designed to allow people to choose whether they want their face to serve as a barcode to their entire social network profiles when they meet new people, or sit in a hospital waiting room, or generally go about their day.

---

446. *See* Tsai, *supra* note 407, at 265 (noting that research has shown that when "people were provided with salient privacy information, they chose sites they considered privacy protective").

447. *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012), *available at* http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220.

448. *Face Facts: A Forum on Facial Recognition Technology*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/workshops/facefacts/ (last visited Dec. 22, 2012).

449. *See* Berners-Lee, supra note 159 ("A . . . danger is that one social-networking site . . . gets so big that it becomes a monopoly, which tends to limit innovation. As has been the case since the Web began, continued grassroots innovation may be the best check and balance against any one company or government that tries to undermine universality.").