PUTTING ONLINE PRIVACY ABOVE THE FOLD: BUILDING A SOCIAL MOVEMENT AND CREATING CORPORATE CHANGE

NICOLE A. OZER[†]

ABSTRACT

Online privacy issues are now "above the fold," both literally and figuratively. Consumers, companies, and policymakers increasingly think about collection and control of personal information, and the media prominently highlights these issues. But there is very little scholarship that reflects on the factors that have contributed to this recent increase in attention. And there is a dearth of scholarship that specifically analyzes how privacy advocates have started to face and overcome the challenges typical to building and sustaining any type of social movement, as well as challenges that make collective action around privacy issues particularly difficult, such as informational disparities and behavioral tendencies. This article provides a behind-the-scenes analysis of how recent factors have enabled the privacy community to create the climate necessary for a social movement to start to coalesce—a movement that can keep issues of online privacy above the fold in sustained ways and support real online privacy reform. The article assesses two recent privacy incidents, and it highlights how the privacy community has been able to mobilize—based on these incidents—to move beyond piecemeal responses and start to build a social movement and influence corporate change. Finally, the article identifies remaining obstacles that must be overcome for the movement to be successful and suggests a focus for legal and policy work to meet these challenges.

[†] Nicole A. Ozer is the Technology and Civil Liberties Policy Director at the ACLU of Northern California (ACLU-NC), where she developed the organization's Demand Your dotRights online privacy campaign. To learn more about her work and the campaign, please visit http://aclunc.org/tech and http://dotRights.org. The opinions expressed in this article are the author's own and should not be attributed to the ACLU-NC. The author wishes to particularly thank Technology and Civil Liberties Policy Attorney Chris Conley, interns Ariana Green, Alexander Reicher, and Dennys Antonialli, and Policy Program Assistants Caitlin O'Neill and Anna Salem for their thoughts and contributions to this article.

I.
INTRODUCTION

Online privacy is a hot topic. National print, television, and radio outlets have joined online media channels in regularly running stories about online privacy. Members of Congress, regulatory agencies, and the White House have convened hearings and roundtables and have initiated multi-stakeholder processes about data privacy. Enforcement actions by regulatory agencies and numerous class actions have targeted online privacy issues. Dozens of pieces of legislation concerning data privacy have been introduced in Congress and state legislatures. Public opinion polls show that consumers are increasingly concerned about how companies collect, retain, use, and share their personal information.[1] Companies are shifting from lengthy privacy policies filled with legal jargon to putting their privacy settings and protections front and center. Many companies have also hired high-level privacy officers and additional lawyers and policy counsel to focus on privacy issues, and some companies have withdrawn or changed products that drew fire for violating user privacy. To the casual observer or average consumer, all of the increased attention around online privacy issues since 2009 may seem like a spontaneous phenomenon. I can

1. *See infra* Section II.A.

assure you that it is not.

In this article, I provide a behind-the-scenes look at how recent factors have enabled the privacy community to create the climate necessary for a social movement to finally start to coalesce in support of real change in this area and keep issues of online privacy above the fold in a sustained way. While much has been written in the press about online privacy issues in recent years, and while there has been a wide range of academic scholarship about particular legal issues, this article fills what I see as a significant void. Very little scholarship assesses the growth of online privacy as a social movement and analyzes how the privacy community has successfully started to address the challenges typical to building and sustaining any type of social movement, as well as the specific challenges that make collective action about privacy issues particularly difficult. This article also highlights obstacles that still must be overcome for the movement to be ultimately successful.

This article builds on Andrew Clement and Christie Hurrell's *Information/Communication Rights as a New Environmentalism?* and Colin Bennett's *The Privacy Advocates*: *Resisting the Spread of Surveillance.*[2] In Clement and Hurrell's study of groups involved in computerization movements like information privacy,[3] the authors compared the privacy movement in 2005 to the early years of the environmental movement.[4] The authors characterized the information privacy movement as "fledgling"[5] and contended that the emergence of an overarching social movement would require several additional steps, including the development of a more widespread understanding of the data ecosystem, framing that connects privacy issues to an individual's daily life, and a shared concern for information and communication rights.[6] In Bennett's 2008 work, which traces the evolution of the privacy advocacy community and assesses the state of the movement, several members of the privacy community also analogized to the environmental movement and expressed optimism about the future growth of a privacy movement. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center ("EPIC"), predicted that "[p]rivacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the

2. Andrew Clement & Christie Hurrell, *Information/Communication Rights as a New Environmentalism?* 5 (Can. Research Alliance for Cmty. Innovation and Networking, Working Paper No. 3, 2005), *available at* http://archive.iprp.ischool.utoronto.ca/cracin/publications/pdfs/WorkingPapers/CRACIN%20Working%20Paper%20No%203.pdf; COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE 200 (2008)

3. Clement and Hurrell define computerization movements as social movements in which "both individuals and organizations . . . 'focus on computer-based systems as instruments to bring about a new social order.'" Clement & Hurrell, *supra* note 2, at 3 (citing "the call for participation for this workshop").

4. *Id.* at 4.

5. *Id.*

6. *Id.* at 16–17.

20th century."[7] Ari Schwartz, who is now Internet Policy Advisor at the National Institute of Standards and Technology ("NIST"), noted, "I see the potential for a larger movement . . . . With privacy you can look back and say that we are at the point where the environmental movement was in the 1960s, and expand from there."[8]

In his 2008 work, Bennett stated that "[t]he privacy advocacy network has never been regarded as a 'social movement' either by those within it, or by those observing from the outside."[9] Despite the emergence, greater communication, and increased coordination of privacy advocates, efforts had not yet been able to achieve the characteristics identified by political scientists like Sidney Tarrow that mark a social movement. These characteristics include (1) a collective challenge that serves as a focal point for both initial supporters and related constituencies; (2) a common purpose that provides focus; (3) solidarity and collective identity that allow the movement to become self-defining; and (4) the ability to sustain collective action and move beyond episodic contentions to create long-term change.[10] While Bennett explores mounting collective challenges through traditional and creative advocacy tactics, he points out that the concept of privacy still appears flexible and vague as a common purpose,[11] and that solidarity still remains fragile.[12] He also questions whether a broad concept such as privacy can generate sustained social activism, citing research suggesting that the "'answer is almost certainly 'no' if one looks backward, but very possibly 'yes' if one looks forward and extrapolates current trends.'"[13]

This article endeavors to pick up where Clement and Hurrell's work and Bennett's work concluded, tracing the crucial changes that have occurred since 2009 that I believe have modified the online privacy climate, have provided new resources to overcome the challenges identified with building a social movement for online privacy, and have altered attitudes about online privacy and its potential as the focus of a social movement. Part II of this article identifies the challenges faced by privacy advocates attempting to build a social movement around information privacy and examines how these challenges initially limited the success of such efforts. Part III discusses how a variety of factors have combined in recent years to launch online privacy onto center stage and to create

7. BENNETT, *supra* note 2, at 199 (quoting Marc Rotenberg, Director, Electronic Privacy Information Center).

8. *Id.* at 218–19 (quoting interview with Ari Schwartz, (May 5, 2006)). At the time of the interview, Schwartz was the vice president and chief operating officer of the Center for Democracy and Technology.

9. BENNETT, *supra* note 2, at 200.

10. *Id.* at 201–07 (citing SIDNEY TARROW, POWER IN MOVEMENT: SOCIAL MOVEMENTS AND CONTENTIOUS POLITICS 5–6 (1998)).

11. *Id.* at 203.

12. *Id.* at 205.

13. *Id.* at 206 (citing Milton Mueller, Christiane Page & Brenden Kuerbis, *Civil Society and the Shaping of Communication-Information Policy: Four Decades of Advocacy*, 20 INFO. SOC'Y 169, 182 (2004)).

an environment conducive to the growth of a privacy social movement. Specifically, this section examines how the widespread adoption of common new products and services like iPhones and Facebook, changing market conditions, the emergence of tech-savvy traditional and alternative media outlets, increased resources for privacy advocacy in academic and non-profit institutions, and building pressure to address privacy concerns through federal law and regulation, have combined to create a climate conducive to change. Part IV explores how privacy advocates have created "virtuous cycles" by leveraging specific incidents to reinforce these environmental factors. The privacy community has moved beyond piecemeal responses to specific incidents to proactive, multidisciplinary campaigns like the ACLU's online privacy campaign, Demand Your dotRights, and encouraged the development of a sustainable social movement around privacy.[14] The article concludes with a discussion, drawing from my experience as the Technology and Civil Liberties Policy Director at the ACLU of Northern California ("ACLU-NC") since 2004, and in developing and managing the organization's Demand Your dotRights online privacy campaign since 2008,[15] of what steps need to be taken to strengthen the movement and some areas of policy focus that will help to sustain momentum and create lasting change that ensures proper safeguards for consumer privacy.

II.
WHY DIDN'T ONLINE PRIVACY GENERATE A SOCIAL MOVEMENT YEARS AGO?

For many years, scholars who have analyzed privacy work in the United States have noted the lack of an organized social movement in the privacy arena.[16] Despite evidence demonstrating that consumers care deeply about privacy, a social movement for better privacy protections has remained "nascent" at best.[17] The specific challenges of information privacy, particularly the informational asymmetry between users and providers and common behavioral tendencies to underestimate long-term risk, have made it more difficult to form a cohesive social movement around the concept of online privacy. Until recently, the privacy community was largely unable to surmount these challenges.

A. Consumers Do Care About Privacy

Surveys performed over the past decade have consistently shown that a

14. ACLU OF N. CAL. DOTRIGHTS, www.dotrights.org (last visited Apr. 3, 2012).

15. More information about Demand Your dotRights online privacy campaign is available at ACLU OF N. CAL. DOTRIGHTS, www.dotrights.org.

16. *See, e.g.*, BENNETT, *supra* note 2, at 200 (stating that "[s]o far, the analysis has tended to support" arguments that privacy will not become a "political 'hot button' issue") (quoting DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE 135 (2001)).

17. Clement & Hurrell, *supra* note 2, at 5.

large percentage of the American public is concerned about their online privacy. In a 2000 study, 94 percent of respondents said that having their security and privacy protected when they were online was "very important."[18] A 2004 Carnegie Mellon/Berkman Fund study found that more than 87 percent of respondents felt that they did not have enough privacy in today's society.[19] By 2005, 52 percent of Americans believed that their right to privacy was "under serious threat."[20] In recent years, consumer concern has further escalated, both in the United States and around the world. A 2010 survey found that nearly eight in ten global consumers were concerned about unauthorized access to their personal information. That figure emerged consistently across age groups and regions and represented a 6 to 8 percent increase since 2008.[21] Among European consumers, there is a growing awareness and sensitivity about the use and misuse of personal data by third parties. Eighty-five percent of European consumers consider data privacy to be very important.[22]

The growth in consumer concern regarding online privacy has become particularly marked in select sectors, including targeted advertising, social networking, and mobile services.

1. Targeted Advertising

Studies have consistently shown that consumers are concerned about the privacy impact of targeted advertising. As early as 2000, 68 percent of consumers said they were "not at all comfortable" with companies that create profiles linking browsing and shopping habits to identity, and that 82 percent were "not at all comfortable" when profiles include additional personal information such as income, driver's license numbers, credit data, or medical

18. *See id.* at 15.

19. Additionally, 60 percent of respondents said that online privacy was "very important" to them, and 65 percent reported that their concern had increased in the past two years. Alessandro Acquisti, *Privacy, Economics, and Immediate Gratification: Why Protecting Privacy Is Easy, But Selling It Is Not*, PowerPoint presentation, slides 50, 53–55 (2004), http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-acquisti.pdf.

20. Joel Roberts, *Poll: Privacy Rights Under Attack*, CBS NEWS (Feb. 11, 2009, 7:06 PM), http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml.

21. KPMG CONSUMERS AND CONVERGENCE IV, CONVERGENCE GOES MAINSTREAM: CONVENIENCE EDGES OUT CONSUMER CONCERNS OVER PRIVACY AND SECURITY 6 (2010), *available at* http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/consumers-and-convergence/Documents/Consumers-Convergence-IV-july-2010.pdf.

22. A data privacy survey commissioned by Nokia Siemens Networks reveals growing sensitivity about personal data among European consumers. As Nokia Siemens Networks reports, "The survey of more than 5,000 people across five countries in Europe in 2010 shows a significant increase in awareness about the use and misuse of personal data by third parties compared to the level of awareness in 2009." *Consumers Concerned About Privacy, but Willing to Share Information with Trusted Telecoms Operators*, NOKIA SIEMENS NETWORKS (Feb. 4, 2011), http://www.nokiasiemensnetworks.com/news-events/press-room/press-releases/consumers-concerned-about-privacy-but-willing-to-share-informa.

status.[23] By the fall of 2008, when online targeted advertising had become more widespread, a Consumers Union study found that "[t]he vast majority of consumers want more control over their personal information online and want the ability to stop internet companies from tracking and profiling them." Ninety-three percent of respondents stated that Internet companies should always ask for permission before using personal information, and 72 percent stated that they want the right to opt out when companies track their online behavior.[24] A 2009 study by the University of Pennsylvania and University of California-Berkeley produced similar results, finding that 66 percent of Americans did not want marketers to tailor advertisements to their interests, and even higher percentages would refuse such advertising after receiving explanations about common methods of data collection.[25] In fact, 87 percent of respondents indicated that they "definitely" or "probably" would not allow tracking of their web browsing activity even if guaranteed that they would remain anonymous.[26] Young people were also concerned about targeted advertising, with 55 percent of 18- to 24-year-olds rejecting tailored advertising.[27] A December 2010 USA Today/Gallup poll found that 67 percent of Americans did not want advertisers to use their online browsing history to target advertisements.[28] A February 2012 Pew Internet & American Life poll revealed that concern had continued to grow, with 68 percent of respondents saying, "I'm NOT OKAY with targeted advertising because I don't like having my online behavior tracked and analyzed."[29]

2. Social Networking

As consumers increasingly share information about themselves on social networks, they are becoming increasingly concerned about the privacy of that information. A 2010 Forrester Research report found that 36 percent of adults were "very concerned" about their privacy on social networking sites in 2010, up from 30 percent the previous year.[30] A similar study released by Edison

23. *Business Week/Harris Poll: A Growing Threat*, BUSINESSWEEK ONLINE (Mar. 20, 2000), http://www.businessweek.com/2000/00_12/b3673010.htm.

24. Joel Kelsey & Michael McCauley, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMERS UNION (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

25. Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, & Michael Hennessy, *Americans Reject Tailored Advertising and Three Activities that Enable It* 3 (Working Paper, Sept. 2009), *available at* http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=1478214.

26. *Id.*

27. *Id.*

28. Lymari Morales, *U.S. Internet Users Ready to Limit Online Tracking for Ads: However, Many Are Amenable to Tracking by Advertisers They Choose*, GALLUP (Dec. 21, 2010), http://www.gallup.com/poll/145337/Internet-users-ready-limit-onlinetracking-ads.aspx.

29. Kristen Purcell, Joanna Brenner, & Lee Rainie, *Search Engine Use 2012: Summary of Findings*, PEW INTERNET (Mar. 9, 2012), http://pewinternet.org/ Reports/2012/Search-Engine-Use-2012/Summary-of-findings.aspx.

30. Jennifer Valentino-DeVries, *Concern About Social-Networking Privacy Jumps*, WSJ.com (Nov. 12, 2010, 7:48 p.m.), http://blogs.wsj.com/digits/2010/11/12/concern-about-social-

Research in May 2011 found that 58 percent of social network users were concerned about privacy on social networks.[31] In addition, Facebook was ranked as the ninth-worst company on the American Customer Satisfaction Index in November 2010, based in part on complaints about privacy and personal information protection.[32]

3. Location Privacy

With the emergence of smartphones and other mobile devices, location privacy has become another area of growing consumer concern. A 2010 survey found that 55 percent of users of location-based services were concerned about privacy,[33] and a 2011 Nielsen study found that 59 percent of women and 54 percent of men who download apps had privacy concerns related to sharing their location.[34] In fact, in a February 2011 study, 38 percent of mobile users listed privacy as their most significant concern about their device.[35]

B. Forces that Deter Privacy-Protective Actions

While a large percentage of consumers have expressed unresolved concerns over online privacy for many years, the public's use of the Internet, social networks, and mobile devices continues to grow. Some members of the business community have pointed to this apparent inconsistency between expressed concern and the lack of backlash to contend that since "people are voting against their own interests on privacy and security . . . that suggests that either they don't care, or they're making a calculated choice about it."[36] According to Facebook CEO Mark Zuckerberg, an increased willingness to share personal information and decreased concern about privacy is simply a new "social norm."[37] Scholars

---

networking-privacy-jumps/.

31. *See* Kenneth Rapoza, *Socially Networked: 52% of Americans on Facebook, Similar Sites*, FORBES (June 1, 2011, 10:52 PM), http://blogs.forbes.com/kenrapoza/2011/06/01/socially-networked-52-of-americans-on-facebook-similar-sites/.

32. Gus Lubin, *The 18 Worst Companies in America: #9 Facebook*, BUSINESS INSIDER (Nov. 14, 2010, 8:05 AM), http://www.businessinsider.com/the-18-worst-companies-in-america-2010-11#9-facebook-10.

33. *Webroot Survey Finds Geolocation Apps Prevalent Amongst Mobile Device Users, But 55% Concerned About Loss of Privacy*, WEBROOT (July 13, 2010), http://pr.webroot.com/threat-research/cons/social-networks-mobile-security-071310.html.

34. *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location*, NIELSEN WIRE (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/.

35. Kristina Knight, *Mobile Consumers Most Concerned About Privacy*, BIZREPORT (Apr. 27, 2011), http://www.bizreport.com/2011/04/survey-mobile-consumers-most-concerned-about-privacy.html.

36. Joe Mullin, *On Privacy, What Consumers Say Isn't What They Do*, PAIDCONTENT (May 19, 2011, 4:25 PM), http://paidcontent.org/article/419-on-privacy-what-consumers-say-isnt-what-they-do/.

37. Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over*, READWRITEWEB (Jan. 9, 2010, 9:25 PM), http://www.readwriteweb.com/archives/

such as Calvin Gotlieb have also asserted that "most people, when other interests are at stake, do not care enough about privacy to value it."[38]

However, commonly-heard arguments such as these do not adequately explain why a social movement has lagged behind consumer concerns about privacy. Rather, studies suggest that privacy-protective individual actions—and the rise of a privacy social movement—have been stunted by inefficiencies in the marketplace. These inefficiencies include informational asymmetry and incomplete information, common behavioral tendencies that influence consumers to overvalue "free" products and services, and societal pressure that discourages consumers from expressing a personal desire for privacy. If consumers do not understand how their personal information is being used, do not realize the costs of online services and the potential risks to their personal interest, are concerned that expressing a desire for privacy implies that they have "something to hide," and are therefore unwilling or unable to take individual steps to protect their personal interest, why would they come together in a social movement to collectively push for change?

1. Information Asymmetry and Incomplete Information

It is now widely recognized that consumers understand very little about how the technology and services they use every day really function or how these services' privacy practices apply to their own personal information. This lack of understanding affects the ability of consumers to take actions that are consistent with their stated desire to control their personal information and safeguard their privacy—as well as to organize and fight for change.

Recent research demonstrates that consumers have very little understanding of the actual privacy practices of the services that they use or the legal constraints on these practices. A 2010 study conducted by researchers at Berkeley and the University of Pennsylvania posed five true/false questions about online privacy, and 75 percent of online adults answered two or fewer of these questions correctly.[39] A 2008 Consumers Union study showed a similar lack of knowledge among consumers, finding that 57 percent incorrectly believed that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations. Forty-eight percent incorrectly believed their consent is required for companies

facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php. According to Zuckerberg, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."

38. Calvin C. Gotlieb, *Privacy: A Concept Whose Time Has Come and Gone*, *in* COMPUTERS, SURVEILLANCE, AND PRIVACY 156, 156 (David Lyon & Elia Zuriek eds., 1996).

39. Chris Jay Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* 17–19 (Working Paper, Apr. 2010) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864. Young adults fared even worse in the survey, with 88 percent of respondents aged 18 to 24 answering two or fewer questions correctly.

to use the personal information they collect from online activities, and 43 percent incorrectly believed a court order is required to monitor activities online.[40] It is not surprising that consumers do not fully understand the privacy practices of companies when research has shown that it would take the average consumer up to 293 hours per year just to skim the privacy policy at each website they visited and up to 304 hours to actually read them.[41] Because this information is so hard to find and understand, when privacy is left to an individual calculation, "people are less likely to make choices that protect their privacy unless these choices are relatively easy, obvious, and low cost."[42] A 2012 Pew study revealed that only 38 percent of Internet users are generally aware of ways they can limit how much of their information is collected by a website.[43]

A series of privacy roundtables held by the Federal Trade Commission ("FTC") in 2009 and 2010 also illuminated concerns that consumers are poorly equipped to make informed decisions about privacy. Summarizing the initial roundtable discussions, the FTC noted that, "consumers generally lack full understanding of the nature and extent of [data collected by third parties]."[44] The FTC cited largely invisible data collection practices and long and confusing privacy policies as contributing factors to this problem.[45]

Company leaders have also admitted that the technology industry has not done enough to educate consumers about how products and services work or their impact on consumer privacy. In 2011, Steve Jobs—the late co-founder, chairman, and CEO of Apple—told an interviewer, "As new technology comes into the society there is a period of adjustment and education. We haven't—as an industry—done a very good job educating people, I think, as to some of the more subtle things going on here."[46]

Experiments conducted by researchers at Carnegie Mellon University demonstrate the impact that this information asymmetry has on the ability of individuals to make privacy-protective decisions.[47] Researchers found that if

40. Kelsey & McCauley, *supra* note 24.

41. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 17 (2008), *quoted in* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 297 (2011).

42. Priscilla M. Regan, *Privacy as a Common Good in the Digital World*, 5(3) INFO., COMM. AND SOC'Y 382, 401 (2002).

43. Purcell, Brenner, & Rainie, *supra* note 29.

44. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012) [hereinafter RAPID CHANGE], *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

45. *Id.* at 2, 61.

46. Ina Fried, *Interview: Apple CEO Steve Jobs on How the iPhone Does and Doesn't Use Location Information*, ALL THINGS D (Apr. 27, 2011, 9:55 AM), http://allthingsd.com/20110427/exclusive-apple-ceo-steve-jobs-on-how-the-iphone-does-and-doesnt-use-location-information/.

47. Janice Tsai, Serge Egelman, Lorrie Cranor & Alessandro Acquisti 7, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, ICIS 2007 PROC. (2007), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf

privacy information was made more visible, people would indeed tend to make more privacy-protective actions.[48] Participants with more access to information about the privacy practices of companies chose to purchase from merchants that offer more privacy protection and were willing to pay a premium to purchase from such merchants.[49] The researchers concluded that "once people were provided with salient privacy information, they chose sites they considered privacy protective."[50]

2. Behavioral Tendencies

Common behavioral tendencies also influence consumers' ability to make privacy-protective choices and to come together to fight for collective privacy change. Social psychology research has long shown that individuals tend to discount future costs and underinsure against future risks. As Alessandro Acquisti writes, "[P]eople may genuinely want to protect themselves, but because of self-control bias, they will not actually take those steps, and [will] opt for immediate gratification instead."[51] Issues of online privacy may be particularly susceptible to these common behavioral tendencies for several reasons: the tendency to prefer products that are marketed as "free," the difficulty in valuing personal information, and the fact that harm from privacy invasions is often delayed and is hard to trace back to a particular cause. With these factors at play, it becomes understandable that people may be apt to act against their own interests when making decisions about their personal privacy.[52]

a. "Free" Services and the Zero Price Effect

Many online services market themselves as "free," which has a significant impact on the lack of privacy-protective choices made by individuals. The "zero price effect" undermines a consumer's rational behavior in considering the loss involved in the transaction. When an item is marketed as "free," individuals perceive that item as immensely more valuable than it actually is.[53] Researchers

(pre-publication version).

48. *Id.* at 24–25.

49. *Id.* at 25.

50. *Id.* at 31.

51. Acquisti, *supra* note 19, at 4.

52. *See id.* at 3–7 (listing and modeling "rationality and psychological distortions" in privacy).

53. *See* Kristina Shampanier, Nina Mazar, & Dan Ariely, *Zero as a Special Price: The True Value of Free Products*, 26 MARKETING SCIENCE 742 (2007), *available at* http://duke.edu/~dandan/Papers/zerofree.pdf (describing this effect and finding that affect emerges as the most likely account for it); Kristina Shampanier & Dan Ariely, *How Small is Zero Price? The True Value of Free Products* (Fed. Reserve Bank of Bos., Working Paper No. 06-16, 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=951742; Mario Vellandi, *Predictably Irrational, by Dan Ariely*, MELODIESINMARKETING.COM (Jan. 8, 2011), http://www.melodiesinmarketing.com/2011/01/08/predictably-irrational-book-dan-ariely-outline-

at Duke and MIT conducted experiments using chocolate to test this "zero price effect" theory. In one experiment, 73 percent of individuals were willing to pay 14 cents for a truffle instead of 1 cent for a Hershey's Kiss, but 69 percent chose the Kiss when the truffle was 13 cents and the Kiss was free.[54] Similarly, when Amazon introduced free "Super Saver" shipping, it saw sales increases worldwide—except in France, where the French division charged a single franc (approximately 10 cents) for shipping.[55]

The impact of the "zero price effect" may be particularly marked in the online privacy space because so many services that generate revenue through advertising or otherwise monetizing user data are marketed as "free." For example, at the top of its homepage, Facebook touts, "Sign up. It's free and always will be."[56] The Google Apps page prominently states, "Get started with Google Apps for free."[57] The Zynga Poker homepage also advertises the free factor, stating, "Zynga Poker . . . is the largest free-to-play online poker game in the world."[58]

The reality, however, is that users do pay for these "free" services: They pay with data about themselves. In some cases, as with Facebook, the data that consumers intentionally create and post is repurposed for revenue generation by the company.[59] In other cases, data collection is a less obvious part of the transaction. For example, if a consumer plays a "free" Zynga game through a platform like Facebook or MySpace, Zynga may collect and store a vast amount of personal information, including first and last name, profile picture, user ID number, email login, physical location where you logged in, your gender, and birthday.[60] When a consumer plays a Zynga game on Facebook, the company will also ask if it can access information about that consumer's Facebook friends as well. So, while this game costs no money to play, consumers share a treasure trove of personal information about themselves and potentially their friends that

---

summary.

54. Shampanier & Ariely, *How Small is Zero Price?*, *supra* note 53, at 25–26.

55. *Id.* at 31. When shipping in France was eventually reduced to free, France saw the same sales increases. DAN ARIELY, PREDICTABLY IRRATIONAL 65 (2009).

56. FACEBOOK, www.facebook.com (last visited Jan. 7, 2012).

57. *Google Apps*, GOOGLE, http://www.google.com/apps/intl/en/group/index.html (last visited Jan. 7, 2012).

58. ZYNGA POKER, http://company.zynga.com/node/859, (last visited Jan. 7, 2012).

59. *See How we use the information we receive,* FACEBOOK, http://www.facebook.com/about/privacy/your-info#howweuse (last visited Apr. 27, 2012) ("We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use."); *Personalized ads*, FACEBOOK, http://www.facebook.com/about/privacy/advertising#personalizedads (last visited Apr. 27, 2012) ("When an advertiser creates an ad on Facebook, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users.").

60. *Information We Collect*, Zynga, http://company.zynga.com/about/privacy-center/privacy-policy/#information-collect (last visited Apr. 14, 2012).

the company uses to sell targeted advertising.[61] And this information has real value: in February 2011, Zynga and its portfolio of "free" games were valued at $7 billion to $9 billion.[62] Facebook's "free to use" social network was valued at between $66.5 billion and $82.4 billion.[63]

When online services are advertised as free, consumers may fail to consider the tradeoffs implicit in using the service. For consumers to adequately assess the risk to their privacy and make an informed choice based on that assessment, they must first be aware that they are paying for these "free" services with access to their personal information.

b. Difficulty Assessing the Risk of Privacy Harm

It is also difficult for an individual to evaluate the costs of disclosing personal information because privacy harms can be hard to foresee.[64] Privacy harms are often intangible; independently innocuous data points can be aggregated in revealing ways; data that was originally not intended to point back to any given individual can be "de-anonymized"; and data shared today can end up being retained and used in different ways in the future. All these factors make it difficult for individuals to make an informed assessment of the risks of sharing data.

In his taxonomy of privacy, Professor Daniel Solove notes that the law, and courts in particular, have frequently had difficulty grappling with privacy harm because it often does not result in physical, financial, or reputational harm, but results instead in "feelings of emotional distress, humiliation, and outrage."[65] Privacy relates to "people's feelings,"[66] and individuals do not always anticipate how they will feel. As one researcher puts it, "It is a deceiving aspect of privacy that its value is truly appreciated only after privacy itself is lost."[67]

It becomes even harder for individuals to properly assess the risk of sharing

---

61. *Id.*

62. *See* Alexia Tsotsis, *Zynga's Reported $7-$10 Billion Valuation Surpasses That of EA*, TECHCRUNCH (Feb. 14, 2011), http://techcrunch.com/2011/02/14/zynga/. Zynga's total valuation exceeded that of one of the major developers of video games, Electronic Arts, which sells games ranging from $19.99 to $79.99 per copy. *Id.*

63. *See* Luisa Kroll, *Are Facebook Shares Losing Value?*, FORBES (Aug. 15, 2011, 5:15 PM), http://blogs.forbes.com/luisakroll/?p=1321.

64. In fact, privacy harms are even difficult to define. Scholars have taken a variety of approaches in defining "privacy harm." *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 174–79 (2008) [hereinafter SOLOVE, UNDERSTANDING PRIVACY]; M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011).

65. SOLOVE, UNDERSTANDING PRIVACY, *supra* note 64, at 174–79. Professor Solove identifies eight types of harms related to privacy problems: physical injuries, financial losses and property harms, reputational harms, emotional and psychological harms, relationship harms, vulnerability harms, chilling effects, and power imbalances. *Id.*

66. *Id.* at 176, *quoting* Paul Sieghart, *quoted in* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 28 (1992).

67. Acquisti, *supra* note 19, at 6.

personal information where they lack adequate knowledge of how it could be combined with other data in the future. In *United States v. Maynard*, the D.C. Circuit held that a warrant was required to install a GPS device on a car and track it for twenty-eight days, and observed that aggregated data can disclose far more than the sum of its parts:

> What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene. . . . [A] single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[68]

A research project called "Gaydar," developed by students at MIT and published in 2009, also demonstrates the power of aggregated data. The students demonstrated that individuals who had consciously chosen not to share their sexual orientation on a social network could nonetheless be "outed" solely by analyzing the gender and sexual orientation of their connections on the network.[69] As such techniques continue to develop, it may become even more difficult for individual consumers to understand the future privacy ramifications of sharing small amounts of seemingly innocent information today.

In addition, researchers have repeatedly demonstrated in recent years that "anonymous" data frequently can be reassembled to identify the persons whose records have been disclosed.[70] In 2000, using public anonymous data from the United States census, Professor Latanya Sweeney showed that 87 percent of the population in the United States could be uniquely identified simply by combining their five-digit ZIP code with their sex and date of birth.[71] In 2006, *New York Times* reporters were able to identify an individual and her search queries from a data set that AOL thought it had properly anonymized prior to its release for research purposes.[72] In 2007, consumers were surprised when

---

68. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 671 (U.S. 2010), *and cert. granted sub nom* United States v. Jones, 131 S. Ct. 3064 (U.S. 2011) (internal citations and quotation marks omitted).

69. Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14(10) FIRST MONDAY (Oct. 5, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2611/2302. *See also* Stan Schroeder, *GAYDAR: Your Facebook Friends Can Reveal Your Sexual Orientation*, MASHABLE (Sept. 21, 2009), http://mashable.com/2009/09/21/facebook-friends-sexual-orientation/.

70. For extensive discussion of failures of anonymity, see Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

71. Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 16 (Carnegie Mellon University, Data Privacy Working Paper No. 3, 2000).

72. *See* Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1. By correlating queries such as "landscapers in Lilburn,

University of Texas researchers were also able to de-anonymize data released by Netflix about customer movie rankings by cross referencing this data set with the public rankings and timestamps from the Internet Movie Database.[73] They were able to identify users and movies viewed by them that revealed information about politics, religious views, and attitudes about sexual orientation.[74]

The fact that data may resurface years later, be re-identified, or be combined in ways that individuals did not intend or envision, makes it very difficult for individuals to make privacy-protective decisions. In some cases, "data mining" tools that allow this kind of analysis may not have even existed when a user first entered a search string on AOL, rated a movie on Netflix, or decided to accept a friend request on Facebook. Moreover, even when a privacy harm occurs, it may be difficult to identify it as such—much less to track it back to the original source. Thus, unsurprisingly, the recent European Commission study on the economic benefits of privacy-enhancing technologies identified "the weak link between actions (the disclosure of personal data) and consequences (e.g., nuisance mail, fraud, theft, profiling etc.)" as "the most important" behavioral bias "that can explain the lack of a demand response to privacy incidents."[75]

3. *Valuing Privacy If You Have "Nothing to Hide"*

Another factor that makes it difficult for individuals to make privacy-protective choices is the mantra that privacy does not matter for those who have "nothing to hide"—that people who are not doing anything wrong will not be harmed if their information is disclosed, and that those who are doing something wrong have no legitimate right to conceal that fact from society. This argument requires the consumer to justify her own desire to keep her information private rather than forcing third parties to justify obtaining and using her private information. This burden-shifting can discourage individuals from pursuing privacy-protective options that they might otherwise desire and from identifying themselves as interested in personal privacy.

Ga," searches for several people with the last name Arnold, and "homes sold in shadow lake subdivision gwinnett county georgia," the reporters tracked down Thelma Arnold, a sixty-two-year-old widow from Lilburn, Georgia. In addition to these searches, she admitted that she also was responsible for other searches, which included some queries about health conditions like "numb fingers" and other personal information like her interest in meeting "60 single men."

73. Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* PROC. 2008 IEEE SYMP. ON SECURITY & PRIVACY 111, 121 (2008). *See* Bruce Schneier, *Anonymity and the Netflix Dataset*, SCHNEIER ON SECURITY (Dec. 18, 2007), http://www.schneier.com/blog/archives/2007/12/anonymity_and_t_2.html.

74. Narayanan & Shmatikov, *supra* note 73, at 123. The authors listed movies viewed by one user that suggested facts about his or her politics ("Fahrenheit 9/11"), religious views ("Jesus of Nazareth"), and attitudes toward gay people and homosexuality ("Queer as Folk").

75. LONDON ECON., STUDY ON THE ECONOMIC BENEFITS OF PRIVACY-ENHANCING TECHNOLOGIES (PETS), at executive summary, page x (2010), *available at* http://ec.europa.eu/justice/policies/ privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

This "nothing to hide" argument is not new.[76] In recent years, governments have regularly cited it to justify surveillance activities. For example, the United Kingdom promoted a program of widespread video surveillance by asserting, "If you've got nothing to hide, you've got nothing to fear."[77] Judge Richard Posner has written extensively about this issue, equating one's desire for privacy with wanting to "conceal discreditable facts about himself," and positing that "when people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."[78] Professor Daniel Solove has also written an entire book in an endeavor to debunk the "nothing to hide" argument and demonstrate that this line of reasoning creates a false tradeoff between privacy and security.[79] But nonetheless, the "nothing to hide" mantra—"privacy is about hiding bad things"[80]—endures.

C. *Missing Elements of a Privacy Social Movement and Why a Movement Matters*

The foregoing analysis of the impact of informational asymmetry, behavioral tendencies, and societal factors helps to demonstrate why, even if consumers express a preference for online privacy in anonymous surveys, it may be difficult for them to make independent decisions that protect their own privacy. But these forces have also affected the ability of the privacy community to assemble a coherent social movement to advocate for greater privacy protections. But why does having a coherent social movement related to online privacy matter? How would consumer privacy rights be different if this work coalesced into a real social movement?

Academic literature discusses varying definitions and characteristics of a social movement. But at their most general, social movements are defined as "organized collective endeavors to solve social problems."[81] They are "collective challenges, based on common purposes and social solidarities, in sustained interaction with elites, opponents and authorities."[82] Building a social

76. *See, e.g.*, Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 749 (2007), *quoting* HENRY JAMES, THE REVERBERATOR 62 (1888), reprinted in NOVELS 1886–1880, at 555, 687 (1989) ("[I]f these people had done bad things they ought to be ashamed of themselves and he couldn't pity them, and if they hadn't done them there was no need of making such a rumpus about other people knowing.")).

77. *Id.* at 748 (quoting JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 36 (2004)).

78. *Id.* at 751 (quoting RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983)).

79. DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

80. Solove, *supra* note 76, at 764.

81. Hayagreeva Rao, Calvin Morrill & Mayer N. Zald, *Power Plays: How Social Movements and Collective Action Create New Organizational Forms*, 22 RES. IN ORGANIZATIONAL BEHAV. 237, 242 (2000).

82. BENNETT, *supra* note 2, at 202 (citing TARROW, *supra* note 10, at 4).

movement for online privacy matters because the ability of activists to bring about lasting change depends upon the ability to "transform . . . initial challenges into permanent access to power and leave lasting networks of activists behind" that "can reappear after the cycle is over and new opportunities appear."[83] According to scholars, "The emerging consensus in the social movement literature is that the ability of institutional entrepreneurs/activists to bring about change depends upon framing processes, mobilizing structures, and political opportunities."[84] In sum, an online privacy social movement would transcend activism around a specific issue and serve as a consistent counterforce against pressures to compromise online privacy.

Existing studies of privacy work in 2005 and 2008 concluded that a social movement had not coalesced. In 2005, Andrew Clement and Christie Hurrell contended that an overarching information privacy social movement would not coalesce without more widespread understanding of the data ecosystem, framing that enables individuals to connect privacy issues to their daily life, and communication of shared concerns among individuals within the community.[85] In 2008, Colin Bennett assessed the online privacy community based on the characteristics of a social movement developed by Sidney Tarrow. Bennett found that advocacy regarding online privacy had not yet cohered into a movement, as it lacked (1) the collective challenge marked by "interrupting, obstructing, or rendering uncertain the activities of others" that serves as a focal point for both initial supporters and related constituencies; (2) a common purpose that provides focus; (3) the "solidarity and collective identity" that allows the movement to become self-defining; and (4) the ability to "sustain[. . .] collective action against antagonists" to move beyond a single "contentious episode" and become capable of creating long-term change.[86] These identified limitations are not surprising considering the relevant informational asymmetries, behavioral tendencies, and societal factors that deter privacy-protective actions. Meeting these challenges to social movement growth and building a sustainable movement can be particularly difficult if consumers do not understand how their personal information is being used, do not realize the costs of online services and the potential risks, and are concerned that expressing a desire for privacy implies that they have "something to hide." These difficulties challenge the online privacy movement and have a real impact on the movement's ability to create change.

However, despite these challenges to the growth of a social movement, since 2009, the privacy community has experienced greater success in building momentum for better consumer online privacy. Why? A series of factors, including widespread adoption of new products and services like iPhones and

83. TARROW, *supra* note 10, at 172.

84. Rao, Morrill & Zald, *supra* note 81, at 242.

85. *See* Clement & Hurrell, *supra* note 2, at 16–17.

86. BENNETT, *supra* note 2 at 201–07 (citing TARROW, *supra* note 10, at 5–6).

Facebook, changing market conditions, the emergence of tech-savvy traditional and alternative media outlets, increased resources for privacy work in academic and non-profit institutions, and building pressure to address privacy concerns through federal law and regulation, have combined in recent years to create a climate more conducive to change.[87] Part II of this article analyzes these changes and discusses how they provide an environment suitable for the growth of a privacy social movement. Part III examines how advocates have leveraged and reinforced these changes in the context of specific privacy-related incidents to further encourage the development of a sustainable social movement.

III.
WHY NOW? FACTORS THAT HAVE CONTRIBUTED TO THE GROWTH OF A PRIVACY SOCIAL MOVEMENT

A variety of factors have combined in recent years to launch privacy issues onto center stage and create a climate ripe for building a privacy social movement. This section highlights the following factors: (1) the nearly universal adoption of the Internet, Facebook, and mobile phones among all segments of society, including lawmakers and regulators; (2) economic factors that have placed competing pressures on companies to both monetize personal information and build user trust; (3) growing media coverage of technology issues; (4) increased resources for privacy advocacy, privacy research, and collaboration; (5) the increased attention of domestic and international regulators and lawmakers to issues of online privacy.

A. Widespread Technology Adoption Makes Privacy Issues Personal and Common to a Growing Number of Consumers

One significant factor contributing to the increase in attention paid to online privacy issues is that many consumers have started using the services that raise privacy concerns. As Sidney Tarrow writes, social movements grow because individuals see common values or interests and want to join together with others similarly situated to strengthen "common claims against opponents, authorities, or elites."[88] The rapidly increasing use of the Internet, mobile phones, and social networking services has led users increasingly to recognize their shared interest in online privacy.

As of June 2011, 79 percent of American adults reported that they used the Internet.[89] From July 2010 to April 2012, Facebook's user base increased from 500 million to 845 million worldwide, and the company estimates that

87. *See infra* Section III.

88. *Id.* at 203 (quoting SIDNEY TARROW, POWER IN MOVEMENT: SOCIAL MOVEMENTS AND CONTENTIOUS POLITICS 6 (1998)).

89. Keith Hampton, Lauren Sessions Goulet, Lee Rainie, & Kristen Purcell, *Social Networking Sites and Our Lives*, PEW INTERNET (June 16, 2011), http://www.pewinternet.org/Reports/2011/Technology-and-social-networks.aspx.

approximately 20 percent of these users are in the United States.[90] By February 2011, most adult Americans with Internet access used Facebook at least once per month.[91] And by May 2011, studies showed that social media reaches the majority of Americans over 12 years old.[92]

Americans also started owning mobile phones in very large numbers. A 2010 Pew Internet study found that 82 percent of Americans owned mobile phones, and the numbers were even higher for young people and people of color.[93] By July 2011, 35 percent of American adults owned a smartphone.[94] In the fourth quarter of 2010, Apple reported record sales as consumers purchased 16 million iPhones and over 7 million iPads.[95] In fact, as of October 2011, the United States was home to more active wireless devices than people.[96]

Lawmakers and federal agencies are also among the technology-utilizing converts, using online services and mobile devices to stay connected professionally and personally. As of April 2012, over 25 million people "liked" President Barack Obama's Facebook page.[97] President Obama became the first President to use a Blackberry[98] and has started using Foursquare to share his location history.[99] More than five hundred members of Congress maintain an official Facebook page,[100] as do federal agencies such as the Federal Trade

90. *See Statistics*, FACEBOOK, http://newsroom.fb.com/content/ default.aspx?NewsAreaId=22 (last visited Apr. 15, 2012); Tom Cheredar, *Facebook Reaches 750 Million Active Monthly Users,* VENTURE BEAT (June 23, 2011), http://venturebeat.com/2011/06/23/facebook-750-million-users/.

91. Jolie O'Dell, *Nearly Half of Americans Use Facebook; Only 7 % Use Twitter*, MASHABLE (Feb. 24, 2011), http://mashable.com/2011/02/24/facebook-twitter-number/.

92. Tom Webster, *The Social Habit 2011,* EDISON RESEARCH (May 29, 2011), http://www.edisonresearch.com/home/archives/2011/05/the_social_habit_2011.php.

93. Specifically, the study found that 90 percent of 18- to 29-year-olds and 87 percent of African Americans and English-speaking Latinos own cell phones. AMANDA LENHART, PEW INTERNET, CELL PHONES AND AMERICAN ADULTS 3–4 (2010), *available at* http://pewInternet.org/~/media/Files/Reports/2010/PIP_Adults_Cellphones_Report_2010.pdf.

94. *35% of American Adults Own a Smartphone*, PEWRESEARCH.ORG (July 11, 2011), http://pewresearch.org/pubs/2054/smartphone-ownership-demographics-iphone-blackberry-android.

95. Doug Aamoth, *Mac, iPhone and iPod Sales Fuel Apple's Record-Breaking Quarter*, TIME TECHLAND (Jan. 19, 2011), http://techland.time.com/2011/01/19/mac-iphone-and-ipad-sales-fuel-apples-record-breaking-quarter.

96. *America: Where Wireless Devices Outnumber People*, CHI. TRIB., Oct. 13, 2011, http://www.chicagotribune.com/news/ct-talk-mobile-gadgets-1013-20111013,0,303402.story (citing a report from wireless industry trade association CTIA).

97. *Barack Obama (Facebook Fan Page)*, FACEBOOK, https://www.facebook.com/barackobama (as of Apr. 15, 2012).

98. *Cf.* Jeff Zeleny, *Obama Gets a Thumbs-Up for His BlackBerry*, N.Y. TIMES: THE CAUCUS (Jan. 22, 2009, 12:29 PM), http://thecaucus.blogs.nytimes.com/2009/01/22/obama-gets-a-thumbs-up-for-his-blackberry/.

99. Elizabeth Montalbano, *Where's Obama? White House Joins Foursquare*, INFORMATIONWEEK (Aug. 16, 2011, 12:00 PM), http://www.informationweek.com/news/government/mobile/231500050.

100. Congress on Facebook, *The Social Congress: Key Findings*, FACEBOOK (July 28, 2011, 11:38 AM), http://www.facebook.com/note.php?note_id=10150328408545071&comments.

Commission.[101] The Rules of the House of Representatives were amended at the beginning of the 2011 term to allow members to use electronic devices on the House floor.[102] By May 2011, at least sixteen members of Congress had released their own applications ("apps") for the iPhone.[103] In August 2011, the House of Representatives Page Program, a program for high school students to spend the summer working in Congress, was eliminated in part because changes in technology have obviated the need for most page services. Dozens of pages were once needed on the House floor to deliver phone messages to Representatives, but in recent years the pages were frequently underutilized, as Representatives were increasingly contacted directly via BlackBerrys and similar devices.[104]

From Main Street to Pennsylvania Avenue and Capitol Hill, the majority of Americans are now fully engaged with modern technology. The growth in the use of common services by such a large percentage of the American public has created a shared identity and common stake in online privacy that did not exist even just a few years ago. This development has encouraged the growth of a social movement to address these common interests.

B. Economic Factors Are Influencing Corporate Decisions about User Data and Putting Privacy in the Spotlight

Changing economic factors have also played a role in increasing user awareness of online privacy issues and, as a result, in overcoming obstacles to building a privacy social movement. The United States entered a major recession in 2008, the worst since the Great Depression.[105] In response to financial stress, many companies faced pressure to increase revenue by monetizing user information. As these practices became more widespread, public awareness surrounding online privacy issues began to increase and companies found themselves facing countervailing pressures to maintain and further build user trust and loyalty. As a result, many companies were forced to become more transparent about how personal information was collected, retained, used, and shared. Though these disclosures were only a small step, information asymmetry

---

101. *Federal Trade Commission*, FACEBOOK, http://www.facebook.com/federaltradecommission (last visited Jan. 7, 2012).

102. Tom Murse, *House of Representatives Allows Use of iPads, Blackberrys on Floor*, ABOUT.COM (Jan. 6, 2011), http://usgovinfo.about.com/od/uscongrss/a/iPads-Allowed-On-House-Floor.htm. In the previous session of Congress, the rules stated: "A person may not smoke or use a wireless telephone or personal computer on the floor of the House." In 2011, the House Republican Conference amended that section of the rules to read: "A person on the floor of the House may not smoke or use a mobile electronic device that impairs decorum."

103. Melanie Zanona, *Members Launch Personal Apps*, ROLL CALL NEWS (May 17, 2011, 12:00 AM), http://www.rollcall.com/issues/56_123/-205655-1.html.

104. *See* Sheryl Gay Stolberg, *House Shuts Down Its Page Program*, N.Y. TIMES, Aug. 9, 2011, at A13, *available at* http://www.nytimes.com/2011/08/09/us/politics/09page.html.

105. Bob Willis, *U.S. Recession Worst Since Great Depression, Revised Data Show*, BLOOMBERG (Aug. 1, 2009, 12:00 PM), http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aNivTjr852TI.

started to decrease and evaluation of risk became more possible, helping fuel the growth of collective knowledge about privacy and creating a stronger foundation for collective action.

1. User Data as a Potential Revenue Source

After 2008, venture capital funds were "drying up in the doldrums of the global economic downturn," with fewer funds raising money in the first quarter of 2009 than in any quarter since 2003.[106] Advertising dollars also became very scarce. The pain for the advertising business, already "especially acute" by December 2008, was expected to continue: analysts projected that advertising revenue would drop an additional 10 percent in 2009 and would not stabilize until 2010.[107] In the second quarter of 2009, the advertising revenues of Google, Yahoo, Microsoft, and AOL, which represented the "lion's share" of all online advertising revenues at that time, were approximately $7.8 billion dollars—a 3.4 percent drop from the prior year.[108]

Facing reduced venture capital funding and increasingly competition for a share of the shrinking advertising pie, many Internet sites explored new ways to increase their value and bring in revenue. Although some sites, notably including many operated by News Corporation, began charging consumers directly,[109] most companies looked for other methods to increase advertising revenue. Many of these methods—such as behavioral and location-based advertising and repurposing existing content to attract more viewers and improve search engine rankings—relied on greater collection, use, or sharing of user personal information. As it became apparent to users that companies were utilizing their personal information in ways that they did not anticipate or desire, visibility and tension around issues of online privacy increased.

In the midst of the economic recession, many online companies started to offer behaviorally-targeted advertising to attract marketers and advertisers who wanted pinpointed access for their advertising dollars in order to target the "consumers who mattered most."[110] By February 2008, Yahoo started testing

106. Kieron Murphy, *Report: Venture Capital Drying Up in Early 2009*, IEEE SPECTRUM TECH TALK (Apr. 13, 2009), http://spectrum.ieee.org/tech-talk/semiconductors/devices/report_venture_capital_drying.

107. *See* Jeffrey F. Rayport, *Why Online Ads are Weathering the Recession*, BLOOMBERG BUSINESSWEEK (Dec. 24, 2008, 12:53 PM), http://www.businessweek.com/technology/content/dec2008/tc20081224_411499.htm.

108. Erick Schonfeld, *The Online Ad Recession Continues, Is This What a Reset Looks Like?*, TECHCRUNCH (July 31, 2009), http://techcrunch.com/2009/07/31/the-online-ad-recession-continues-is-this-what-a-reset-looks-like/.

109. *See* Ian Paul, *Murdoch to Charge for All Newspaper Sites*, PCWORLD (Aug. 6, 2009, 6:21 AM), http://www.pcworld.com/article/169739/murdoch_to_charge_for_all_newspaper_sites.html.

110. *See* Rayport, *supra* note 107 (concluding that a "new and different ad equilibrium will emerge from the coming economic recovery").

behavioral advertising with its newspaper partners.[111] The following year, Yahoo expanded behavioral targeting to reach its entire search and display advertising program.[112] Google announced in March 2009 that it would also start to offer behaviorally-targeted advertisements.[113] Microsoft, which had been using behavioral targeting for several years, released its behavioral targeting for mobile devices in September 2009.[114] Advertisers were willing to pay for the opportunity to target customers, paying significantly higher prices—one study placed it at 2.68 times as much—for online ads that utilized behavioral targeting in 2009.[115] Startup companies that utilized targeted behavioral data were increasingly likely to receive venture capital funding.[116]

The economic slowdown has also influenced companies to explore location-based services and location-based advertising as new revenue sources. Advertisers were anxious to utilize geolocation services to deliver even more targeted advertisements based on a consumer's physical location.[117] Mobile advertising revenue increased from $491 million in 2009 to an estimated $550 to $650 million in 2010.[118] Businesses spent $42.8 million on location-based advertising in 2010, a figure projected to rise to $1.8 billion by 2015.[119] Location-based services were the "talk of the show" at the 2009 South by Southwest Interactive Festival as excitement grew about the potential for new revenue streams.[120] With location-based revenue in the United States expected

111. *See* Kate Kaye, *Yahoo to Offer Behavioral Targeting On Newspaper Consortium Sites*, CLICKZ (Feb. 28, 2008), http://www.clickz.com/clickz/news/1692030/yahoo-offer-behavioral-targeting-newspaper-consortium-sites.

112. Kevin Newcomb, *Yahoo Adds Behavioral Targeting Features for Search and Display Ads*, SEARCHENGINEWATCH (Feb. 24, 2009), http://searchenginewatch.com/article/2052709/Yahoo-Adds-Behavioral-Targeting-Features-for-Search-and-Display-Ads.

113. Miguel Helft, *Google to Offer Ads Based on Interests, With Privacy Rights*, N.Y. TIMES, Mar. 11, 2009, at B3, *available at* http://www.nytimes.com/2009/03/11/technology/internet/11google.html.

114. *Cf.* Jamie Wells, *Microsoft Launches Behavioral Targeting for Mobile*, MICROSOFT ADVERTISING BLOG (Sept. 15, 2009), http://community.microsoftadvertising.com/Blogs/Advertising/archive/2009/09/16/microsoft-launches-behavioral-targeting-for-mobile.aspx.

115. HOWARD BEALES, NATIONAL ADVERTISING INITIATIVE, THE VALUE OF BEHAVIORAL TARGETING 1 (2009), *available at* www.networkadvertising.org/ pdfs/Beales_NAI_Study.pdf.

116. *See* Cody Barbierri, *A New Hunch Points to the Money with Behavioral Targeting*, VENTUREBEAT (Aug. 5, 2010), http://venturebeat.com/2010/08/05/hunch-web-personalization/ (describing how companies targeting behavior data gained funding and acquisition momentum).

117. *Cf.* Rayport, *supra* note 107 (stating that "mobile advertising, which pinpoints a consumer's physical location, only adds to the expanding possibilities" for "target[ing] specific users and usage occasions").

118. Ryan Kim, *Mobile Advertising Heats Up with Funding, Deals*, GIGAOM (May 6, 2011, 10:15 AM), http://gigaom.com/2011/05/06/mobile-advertising-heats-up-with-funding-deals/.

119. *Cf.* John Egan, *Study: Spending on Location-Based Ads Will Reach $1.8B in 2015*, TECHNORATI (Sept. 4, 2010, 12:05 PM), http://technorati.com/business/advertising/ article/ study-spending-on-location-based-ads/.

120. M.G. Siegler, *Location Will Be This Year's Twitter at SXSW*, TECHCRUNCH (Feb. 25, 2010), http://techcrunch.com/2010/02/25/location-sxsw/.

to climb from $2.8 billion in 2010 to $10.3 billion in 2015,[121] big companies have been experimenting with location-based services, and "there are plenty of other players in this space who are making moves, picking up money and getting bought up."[122]

Social networking sites like Facebook have also sought to add value by increasing the amount of public content on their sites in order to attract advertisers. In December 2009, Facebook made a series of changes to its privacy practices that decreased the amount of information that could be kept private and rolled out a "Transition Tool" that recommended to many individuals that they loosen their privacy settings.[123] The changes to Facebook's privacy practices made profile pictures, current city labels, friends lists, gender, and fan pages "publicly available information," which meant that Facebook users had no way to prevent other users from viewing this profile information. That information also became publicly available on search engines unless the user adjusted her privacy settings.[124] As industry analysts have noted, moving users to a more "open" Facebook is also essential to helping Facebook make more money. The more content that Facebook has public and open, the more content inventory it has for advertising opportunities, and "Facebook knows that in order to compete with massive Google, they need more content to be public. . . . They must be open to win the end game of monetization."[125] Ultimately, Facebook's "maneuverings to get [users] to open up" have led to soaring advertising revenue,[126] with advertising revenue of $3.8 billion in 2011, up from $1.86 billion in 2010.[127]

121. *See* Jan ten Sythoff & Julian Morrison, *Location-Based Services, Market Forecast, 2011–2015: Key Findings*, PYRAMID RESEARCH (May 2011), http://www.pyramidresearch.com/store/ Report-Location-Based-Services.htm.

122. *See* Kim, *supra* note 118. *See also* Marty Zwilling, *Location-Based Services Are a Bonanza for Startups*, CAYENNE CONSULTING (Apr. 1, 2011), http://www.caycon.com/blog/2011/04/location-based-services-are-a-bonanza-for-startups/ (discussing the potential for location-based services as an opportunity for startup companies).

123. Nicole Ozer, *Facebook Privacy in Transition - But Where Is It Heading?*, ACLU OF N. CAL. (Dec. 9, 2009, 8:00 AM), http://www.aclunc.org/issues/technology/blog/facebook_privacy_in_transition_-_but_where_is_it_heading.shtml.

124. Hari O'Connell, *What Does Facebook's Privacy Transition Mean for You?*, ACLU OF N. CAL. DOTRIGHTS, http://www.dotrights.org/what-does-facebooks-privacy-transition-mean-you (last visited Jan. 7, 2012).

125. Jeremiah Owyang, *Matrix: How Facebook's 'Community Pages' and Privacy Changes Impact Brands*, WEB STRATEGY (May 16, 2010), http://www.web-strategist.com/blog/2010/05/16/matrix-how-facebooks-community-pages-and-privacy-changes-impact-brands/.

126. Leah Fabel, *The Business Of Facebook*, FAST COMPANY (Apr. 1, 2011), http://www.fastcompany.com/magazine/154/numerology-the-business-of-facebook.html.

127. Brian Womack, *Facebook Revenue Will Reach $4.27 Billion, EMarketer Says*, BLOOMBERG (Sept. 20, 2011, 3:44 PM), http://www.bloomberg.com/news/2011-09-20/facebook-revenue-will-reach-4-27-billion-emarketer-says-1-.html

2. Protecting Privacy, Protecting "Brand"

It is no coincidence that the areas where companies were pushing to grow revenues, such as behavioral targeting, social networking, and location-based services, are also the areas where consumer concern has grown most markedly. The push for greater monetization of personal information also led to increased recognition that privacy concerns can erode trust and harm a company's long-term outlook. More companies have come to understand that in order to protect their "brand," they must do more than comply with particular legal mandates; they must also work to ensure that corporate practices are "consistent with our global corporate values, and consistent with evolving consumer expectations."[128]

As a result, many companies are taking steps to demonstrate that they value user privacy, including backtracking from changes that generate significant public protest. For example, when Facebook's "privacy transition" resulted in a dramatic increase in publicly available data, a widespread public outcry, including an ACLU petition signed by 80,000 concerned users, forced Facebook to reverse some of its changes.[129] Incidents like this, where concerted advocacy efforts create results, help to build momentum that can sustain a social movement.

Companies are also trying to market their services as privacy-friendly in order to gain a competitive advantage. When Google announced its foray into behavioral targeting, it also launched three features, including its "Ad Preferences Manager," that it said "demonstrate[s] [its] commitment to transparency and user choice."[130] Microsoft released its Privacy Principles for Live Search and Online Ad Targeting and testified to the Senate Committee on Commerce, Science & Transportation that it is "deeply committed to these principles, which focus on bringing the benefits of transparency, control and security to the protection of consumers' data and privacy online."[131] A recent advertising startup, ADmantX, drew attention from the business media and investors by explicitly stating that it would generate relevant advertising without

128. Bamberger & Mulligan, *supra* note 41, at 270. As one Chief Privacy Officer explained: "[T]he end objective in my mind is always what's the right thing to do to maintain the company's trusted relationship. . . . [H]ow likely . . . is that customer going to be comfortable . . . [o]r will they start wanting to shut down the relationship, in other words, shut off the information, complain to the FTC, send nasty letters and threatening lawsuits . . . ?" *Id.* at 271.

129. *See, e.g.*, Caroline McCarthy, *Facebook Backtracks on Public Friend Lists*, CNET NEWS (Dec. 11, 2009, 8:04 AM), http://news.cnet.com/8301-13577_3-10413835-36.html (describing Facebook's quick modifications in response to user complaints). Petition no longer available online; on file with author. For a similar petition, *see Facebook's Privacy Transition: Push Facebook in the Right Direction*, ACLU, https://secure.aclu.org/site/SPageServer?pagename=Nat_Petition_Facebook_Policy (last visited Apr. 24, 2012).

130. Susan Wojcicki, *Making Ads More Interesting*, OFFICIAL GOOGLE BLOG (Mar. 3, 2009, 2:01 AM), http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html.

131. *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 110th Cong. 10 (2008) (statement of Michael D. Hintze, Associate General Counsel, Microsoft Corporation).

relying on tracking user behavior.[132] A new search engine, DuckDuckGo, based its business model on differentiating itself from other companies by not collecting or sharing personal information.[133] Most recently, Google emphasized the privacy features of its latest social networking product, Google+, influencing Facebook to respond by improving its own privacy settings.[134] In fact, online privacy has become such a central issue in the business world that Facebook hired a public relations firm to pitch stories critical of its competitor, Google, in order to shift the spotlight away from Facebook's privacy issues.[135]

As business models increasingly rely on monetizing data, companies have also had to consider how to respond to concerns about privacy and increase transparency about business practices in order to maintain consumer trust. A byproduct of this increased transparency has been the public's ability to better understand the risks to personal privacy and to engage in efforts to address those risks.

C. *The Growth of Technology-Focused Media*

Increasing attentiveness among the media, both traditional and online, to technology issues has also helped to make consumers, regulators, and companies more conscious of online privacy—thereby creating a climate more conducive to a privacy social movement.

Over the past several years, many traditional media outlets, particularly print newspapers, have confronted severe financial woes and been reducing overall reporting staff.[136] But at the same many outlets have increased the resources dedicated to technology coverage.[137] The mainstream media has increased its

---

132. David Kaplan, *Contextual Provider ADmantX Stresses 'Cookie-Less' Targeting In First Round*, PAIDCONTENT, (June 8, 2011, 10:14 AM), http://paidcontent.org/article/419-contextual-provider-admantx-stresses-cookie-less-targeting-in-first-rou/.

133. *See* Audrey Watters, *Writing Your Startup's Privacy Policy*, READWRITESTART (July 8, 2010, 2:30 PM), http://www.readwriteweb.com/start/2010/07/writing-your-startups-privacy.php (comparing the length of DuckDuckGo's privacy policy to that of Microsoft and Google).

134. *See* Chris Gayomali, *Facebook Adds New Google Plus-Like Privacy Features*, TIME TECHLAND (Aug. 23, 2011), http://techland.time.com/2011/08/23/facebook-adds-new-google-plus-like-privacy-features/ (stating that many of Facebook's new privacy features are "eerily reminiscent of Google Plus"); Catharine Smith, *Google+ Social Network: More Privacy, Tighter Social 'Circles'*, HUFFINGTON POST (June 29, 2011, 6:55 PM), http://www.huffingtonpost.com/2011/06/28/google-social-network_n_886185.html#s299885 (noting that Google "emphasizes Google+'s privacy customizations").

135. Geoffrey A. Fowler & Amir Efrati, *Facebook Hired Firm to Target Google*, WALL ST. J., May 13, 2011, at B1, *available at* http://online.wsj.com/article/SB10001424052748703730804576319351012761800.html#ixzz1YSywBi5x.

136. *The Changing Newsroom*, JOURNALISM.ORG (July 21, 2008), http://www.journalism.org/node/11961.

137. For example, *The Wall Street Journal* and *The New York Times* both have blogs dedicated to technology, *see* WALL ST. J.: DIGITS, http://blogs.wsj.com/digits/, *and* N.Y. TIMES: BITS BLOG, http://bits.blog.nytimes.com, and nearly every major newspaper or news magazine has a dedicated technology section on its web site. *See, e.g.*, TIME: TECHLAND, http://techland.time.com; *Technology News*, USA TODAY, http://usatoday.com/tech/index; *CNN*

online presence, collaborating with smaller tech-centric sources, and providing readers with more opportunities to take part in a dialogue about important stories. In 2008, *The New York Times* announced it would begin to focus more on its *Bits* blog covering technology issues.[138] The *Times* now licenses content from several online sources, including ReadWriteWeb and GigaOM, to appear on its technology page.[139] Mainstream media outlets have also at times adopted the more casual and personal style of blogs—allowing writers to provide personalized accounts that readers can easily understand[140]—and the comments area of online stories enables readers to share their own thoughts.[141] The resulting reports have both highlighted the benefits of new products and services and criticized their flaws, including those that threaten user privacy. A recent study found that "[a] host of explicit problems—from cyber-security, to privacy concerns, crime incidents and more—made up a nearly third (a combined 32%) of the [mainstream] technology coverage [between June 1, 2009 and June 30, 2010]."[142] In addition to reporting such stories, outlets like *The Wall Street Journal* have conducted independent research, publishing investigative reports about online privacy, such as the publication's "What They Know" series.[143] The first headline in the series, "The Web's New Gold Mine: Your Secrets," set the stage for a string of investigations into the challenges of maintaining control of personal information in an era of emerging technologies.[144]

Tech, CNN, http://www.cnn.com/TECH/. For a discussion of how many outlets have increased resources dedicated to technology coverage over the past several years, *see* Neal Ungerleider, *Bloomberg Expanding Tech Coverage*, FAST COMPANY, Mar. 5, 2012, http://www.fastcompany.com/1822690/bloomberg-expanding-tech-coverage; *We Got the Betabeat! 'The Observer' Tech Site Launches Tomorrow*, N.Y. OBSERVER, Mar. 15, 2011, http://www.observer.com/2011/03/we-got-the-betabeat-the-observer-tech-site-launches-tomorrow/; Press Release, *Bloomberg Television Launches New Technology Program*, BLOOMBERG PRESS ROOM, Mar. 1, 2011, http://www.bloomberg.com/pressroom/ 2011/03/01/bloomberg-television-launches-new-technology-program-2/index.html; Lauren Drablier, *US:* The New York Times *Announces Plans to Expand Online Business Coverage*, EDITORSWEBLOG.ORG (Sept. 24, 2008, 8:33 AM), http://www.editorsweblog.org/multimedia/2008/09/us_the_new_york_times_announces_plans_to.php; Jemima Kiss, *BBC Appoints US Tech Reporter*, Guardian (UK), Feb. 8, 2008, http://www.guardian.co.uk/media/2008/feb/08/web20.digitalmedia1.

138. Drablier, *supra* note 137.

139. *Id. See, e.g.*, N.Y. TIMES: TECHNOLOGY, http://www.nytimes.com/tech/ (last visited Nov. 14, 2011).

140. *See, e.g.*, Jenna Wortham, *What Location Data, Exactly, Does an iPhone Reveal?*, N.Y. TIMES: GADGETWISE (Apr. 21, 2011, 12:18 PM), http://gadgetwise.blogs.nytimes.com/2011/04/21/what-location-data-exactly-does-an-iphone-reveal/ (describing being troubled that her phone had logged her trips to visit her family when she explicitly tried to be "off the social grid").

141. *Id.*

142. *When Technology Makes Headlines: Social Trends and New Devices Garner Greatest Attention from the MSM*, JOURNALISM.ORG (Sept. 27, 2010), http://www.journalism.org/analysis_report/social_trends_and_new_devices_garner_greatest_attention_msm.

143. *See* WALL ST. J.: WHAT THEY KNOW, http://online.wsj.com/wtk (last visited Jan. 7, 2012).

144. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J.: WHAT THEY KNOW (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

Independent blogs and social media have also assumed a prominent role in generating and distributing content about technology. Technology-centered web sites such as CNET and TechCrunch are among the most popular sites on the Internet.[145] Informal blogs provide individual users with an outlet to contribute their own content, and technology stories have been more popular on blogs than in the mainstream media; according to a study conducted by the Pew Research Center's Project for Excellence in Journalism, "[d]uring the 13 months studied [June 1, 2009 to June 30, 2010], 11% of the top stories on blogs were technology-related [compared to] less than 2% . . . in the mainstream press."[146] Microblogging site Twitter provided an even greater forum for distribution of and dialogue about technology issues, as "[m]ore than half (51%) of the top five stories in a given week on Twitter were about a technology-related topic."[147]

Because media coverage of privacy stories, in both the mainstream and independent media, has grown exponentially, and because "right now, you see the P word all over the place," public awareness of privacy issues has increased, creating a robust "court of public opinion" that influences corporations to respond to privacy concerns and reinforces the sense of importance, solidarity, and impact necessary to forge a social movement.[148]

D. Regulators and Lawmakers Are Focused on Privacy Issues

The increased attention of regulators and lawmakers in the United States and abroad on privacy issues in recent years has helped to educate the public about the issues and has created some collective action "wins." These victories have helped to sustain and build energy for a privacy social movement. Legislative bodies have debated and passed privacy protection laws, including data breach notification and new digital book privacy laws, and have held companies accountable when their practices harmed users. Consumer protection and data privacy agencies have also exercised their enforcement powers, conducted studies, hosted conversations between companies and privacy advocates, and produced educational materials for consumers and businesses to promote best practices and enable users to protect their own personal information.

Regulators and lawmakers have focused their attention on privacy issues for some of the same reasons users have: because they too increasingly use smartphones, social networks, and other modern tools in their professional and

145. *See Top Sites in United States*, ALEXA, http://www.alexa.com/ topsites/countries/US (last visited Apr. 15, 2012). According to traffic metrics generated by Alexa as of April 15, 2012, CNET.com is the 55th most popular web site in the United States and TechCrunch is the 215th most popular web site.

146. *When Technology Makes Headlines: New Media's Take on Technology—A Separate Look*, JOURNALISM.ORG (Sept. 27, 2010), http://www.journalism.org/analysis_report/new_media%E2%80%99s_take_technology_%E2%80%93_separate_look.

147. *Id.*

148. Bamberger & Mulligan, *supra* note 41, at 277.

personal lives.[149] They also are attuned to concerns from users, to issues prominent in the media, and to pressures from non-profit and academic institutions. Increasingly, regulators are taking a proactive role, reaching out to experts from the non-profit and academic arenas to provide insight into policy issues and to suggest potential solutions. In doing so, regulators are not only responding to current public concerns and immediate issues; they are also demonstrating the effectiveness of collective action and providing the transparency and support required to allow a privacy social movement to emerge.

1. The Federal Trade Commission

In the United States, the FTC has increased its role in the privacy arena. The FTC initially served a primarily advisory role, issuing the Fair Information Practice Principles,[150] but has shifted to a more active role, initiating enforcement actions to counteract a broad range of harmful or deceptive behavior.[151] Recent FTC enforcement actions include: an action against Sears Holdings for failing to adequately inform users of the extent to which a downloaded program monitored their online activity,[152] an action against Google for failing to adequately notify users that its Buzz feature would migrate their private email and chat contacts to their public profile, sometimes even if they chose not to use Buzz,[153] an action against Twitter for deceiving users and failing to institute adequate security measures to safeguard user information,[154] and an action against Facebook for deceiving consumers by failing to keep privacy promises.[155] The actions against Google, Twitter, and Facebook resulted in settlements that included not only cessation of current practices but also wholesale changes in the companies' internal approach to privacy and regular external audits over the next ten years (for Twitter) or twenty years (for Google

149. *See, e.g.*, Murse, *supra* note 102 (explaining how in early 2011, the U.S. House of Representatives amended its rules to allow the use of mobile devices on the House floor).

150. *See Fair Information Practice Principles*, FTC, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

151. *See generally* RAPID CHANGE, *supra* note 44, at ii. The Commission's authority to bring such actions is based on Section 5 of the Federal Trade Commission Act, codified at 15 U.S.C. § 45 (2008).

152. Press Release, FTC, Sears Settles FTC Charges Regarding Tracking Software (June 4, 2009), *available at* http://www.ftc.gov/opa/2009/06/sears.shtm.

153. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

154. *See* Press Release, FTC, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011), *available at* http://www.ftc.gov/opa/2011/03/twitter.shtm.

155. *See* Press Release, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm.

and Facebook) to ensure that these changes are being carried out.[156]

In addition to bringing enforcement actions, the FTC has taken an active role in promoting dialogue between companies and privacy advocates. As early as 2002, the FTC began looking into issues of privacy and security for users of web-enabled wireless devices and mobile data services.[157] In 2007, the FTC hosted a workshop examining privacy concerns with behavioral advertising.[158] From December 2009 to March 2010 the FTC hosted a series of privacy roundtables, bringing in experts from various disciplines and organizations to discuss the privacy challenges surrounding new technology.[159] The FTC also consulted with the Federal Communications Commission ("FCC") in hosting a forum aimed at helping users navigate the privacy challenges of location-based services and location-aware devices.[160]

Finally, the FTC has also produced independent research examining the consequences of emerging technologies and proposing policy solutions to identified problems. In February 2012, the FTC issued a report on mobile privacy, *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing*,[161] which focuses on the issue of protection of children's privacy but recommends solutions that would apply broadly to all makers of mobile applications and application platforms. And in March 2012, the FTC issued a broad-ranging report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers,* which proposed a framework for addressing privacy concerns arising from new technologies.[162] The report recommended several approaches to addressing these concerns, including: "privacy by design," which refers to proactively building privacy

156. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm; Press Release, FTC, FTC Accepts Final Settlement with Twitter for Failure to Safeguard Personal Information (Mar. 11, 2011), *available at* http://www.ftc.gov/opa/2011/03/twitter.shtm; Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), *available at* http://ftc.gov/opa/2011/11/privacysettlement.shtm.

157. *See* FED. TRADE COMM'N, THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES 8–19 (Feb. 2002) [hereinafter MOBILE WIRELESS WEB], *available at* http://www.ftc.gov/bcp/reports/wirelesssummary.pdf.

158. *See Ehavioral Advertising: Tracking, Targeting, and Technology*, FTC, http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml (last visited Jan. 7, 2012). Following the workshop, the FTC released a set of principles for self-regulation in the behavioral advertising industry. *See* Press Release, FTC, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), *available at* http://www.ftc.gov/opa/2007/12/principles.shtm.

159. *See Exploring Privacy: A Roundtable Series*, FTC, http://www.ftc.gov/bcp/workshops/privacyroundtables/ (last visited Jan. 7, 2012).

160. *See* Press Release, FCC, FCC Staff to Host Forum Aimed at Helping Consumers Navigate Location-Based Services (May 17, 2011), *available at* http://www.fcc.gov/document/fcc-staff-host-forum-aimed-helping-consumers-navigate-location-based-services.

161. FTC, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (2012), *available at* http://www.ftc.gov/os/2012/02/ 120216mobile_apps_kids.pdf.

162. *See* RAPID CHANGE, *supra* note 44.

protections into new products and services rather than addressing privacy issues as they arise; providing consumers with choices about data practices in a simpler and more streamlined manner than in the past; giving users meaningful and usable controls and options; greater transparency, including user access to data about the user held by the company and increased notice of any chances to data use practices; and an extensive public education program regarding consumer options related to commercial data practices.[163] The report also made several specific policy recommendations, including the creation of a "Do Not Track" mechanism that allows users a simple, comprehensive mechanism to opt out of behavioral tracking and advertising[164]

In sum, the FTC has taken several steps in recent years to ensure its ability to protect consumer privacy in light of threats created by emerging technologies. The FTC has also expanded its research and analysis capabilities. In 2010, the agency named its first Chief Technologist: Edward W. Felten, a professor of computer science and founding director of Princeton's Center for Information Technology Policy.[165] When Felten was appointed, FTC leadership stated that his position would involve providing input into agency recommendations and enforcement actions related to the protection of online privacy.[166]

2. *The Federal Communications Commission*

In addition to the FTC, the FCC has increasingly focused on consumer privacy issues relating to cellular carriers, Internet service providers, and other entities within its jurisdiction.[167] In February 2009, FCC Acting Chairman Michael J. Copps issued a statement asserting that "the Commission continues to make consumer privacy protection a top priority" and pledging to continue to expand its privacy enforcement actions.[168] As noted above, the FCC hosted a hearing on the privacy implications of location-based services in June 2011.[169]

---

163. *Id.* "Privacy by Design" is a concept originated by the Office of the Information and Privacy Commissioner of Ontario, Canada. *See* PRIVACY BY DESIGN, http://www.privacybydesign.ca (last visited Jan. 7, 2012).

164. RAPID CHANGE, *supra* note 44, at 4–5.

165. Press Release, FTC, FTC Names Edward W. Felten as Agency's Chief Technologist; Eileen Harrington as Executive Director (Nov. 4, 2010), *available at* http://www.ftc.gov/opa/2010/11/cted.shtm.

166. *Id.*

167. "The FCC was established by the Communications Act of 1934 and is charged with regulating interstate and international communications by radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and U.S. possessions." *About the FCC*, FCC, http://transition.fcc.gov/aboutus.html (last visited Feb. 7, 2012).

168. Press Release, FCC, Statement of FCC Acting Chairman Michael J. Copps on Enforcement Bureau Actions Regarding Protection of Consumer Privacy (Feb. 24, 2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-288810A1.pdf. *See also* Ryan Singel, *FCC to Telecoms: Explain Privacy Protection or Pay Up*, WIRED EPICENTER (Feb. 25, 2009, 10:52 AM), http://www.wired.com/epicenter/2009/02/fcc-threatens-t/.

169. *See* Press Release, FCC, FCC Staff to Host Forum Aimed at Helping Consumers Navigate Location-Based Services (May 17, 2011), *available at* http://www.fcc.gov/

Along with the FTC and the National Telecommunications and Information Administration ("NTIA"), the FCC has testified before Congress regarding its position on the privacy issues connected with emerging technology and its own role in overseeing and addressing those issues.[170]

3. Congress

Congress has also been increasingly active in the online privacy arena. Numerous privacy bills have been introduced, including bills mandating that the FTC create and enforce a "Do Not Track" mechanism,[171] updating the law governing voluntary and mandatory disclosure of electronic data to third parties,[172] providing consumers with additional rights to control the collection and use of their personal information,[173] limiting the collection and use of consumer location information without express authorization of the individual from whom the information is being collected,[174] and requiring notice to users in the case of a data breach.[175]

Congress has also held several hearings at which it has requested that companies explain their behavior in light of user privacy concerns. On August 1, 2008, thirty-three companies, including Google, Microsoft, Comcast and Cox Communications, received letters from four members of the House Committee on Energy and Commerce requesting details on company privacy policies.[176] In May 2011, after news broke that iPhones and Android smartphones were retaining user location information, the newly formed Senate Judiciary Subcommittee on Privacy, Technology, and the Law called a hearing to question executives from Google and Apple about mobile privacy.[177] On July 14, 2011,

---

document/fcc-staff-host-forum-aimed-helping-consumers-navigate-location-based-services.

170. *See* Jim Smith, *Congressional Subcommittees Hold Consumer Data Privacy Hearing Featuring Testimony by FCC, FTC, and NTIA*, PRIVACY & SECURITY L. BLOG (July 15, 2010), http://www.privsecblog.com/2011/07/articles/main-topics/marketing-consumer-privacy/congressional-subcommittees-hold-consumer-data-privacy-hearing-featuring-testimony-by-fcc-ftc-and-ntia/.

171. *See* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011).

172. *See* Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011).

173. *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

174. *See* Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011).

175. *See* Data Accountability and Trust Act, H.R. 1707, 112th Cong. §3(a)-(b) (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Cong. §3 (2011); Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. §102(a) (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. §3 (2011).

176. Stephanie Clifford, *Web Privacy on the Radar in Congress,* N.Y. TIMES, Aug. 11, 2008, at C1, *available at* http://www.nytimes.com/2008/08/11/technology/11privacy.html.

177. Tanzina Vega, *Congress Hears from Apple and Google on Privacy*, N.Y. TIMES: MEDIA DECODER, (May 10, 2011, 2:36 PM), http://mediadecoder.blogs.nytimes.com/2011/05/10/congress-hears-from-apple-and-google-on-privacy/. For more information on the iPhone location file controversy, *see infra* Section IV. A.

two Subcommittees of the House Energy and Commerce Committee held a joint hearing intended to "kick off a series on privacy issues to examine how information is collected, protected, and utilized in an increasingly interconnected online ecosystem" and invited testimony from the FTC, FCC, and NTIA.[178] According to observers, this hearing "indicated significant interest in prospective online privacy legislation."[179]

4. The White House

The White House has recently initiated attempts to broker solutions to online privacy dilemmas that incorporate the input and participation of privacy advocates. In 2012, the White House released an extensive report on consumer privacy, endorsing the idea of a "Consumer Privacy Bill of Rights" that would give technology users broad, context-dependent rights over their own personal information.[180] The report proposed a multi-faceted approach to protecting privacy rights, including a multi-stakeholder effort that explicitly gives privacy advocates a seat at the table to work towards a solution that addresses both individual and corporate interests.[181] The White House also announced an agreement with several major technology companies to implement and adhere to a "Do Not Track" mechanism, and subsequently indicated that it will work with the World Wide Web Consortium, an independent standards body, to finalize the details of the mechanism.[182]

5. State Governments and State Officials

State legislators have also actively addressed certain aspects of consumer privacy. In particular, legislators in at least forty-five states have passed data breach legislation since 2002, requiring corporations to notify consumers if their

178. *See* Jim Smith, *supra* note 170.

179. *See, e.g., id.* (noting "unusually strong participation by subcommittee Members including the Chairman of the full Committee, Fred Upton (R-MI), and ranking Democrat Henry Waxman (CA)"); Ronald P. Whitworth, *First Joint Privacy Hearing of 112th Congress Highlights House of Representative Members' Mindset Regarding Potential Federal Privacy Legislation*, SULLIVAN & WORCHESTER (July 15, 2011) (on file with author) ("At the hearing . . . many House of Representatives members...indicated that they see a need to pass federal privacy legislation this Congress, to safeguard consumers against an escalating number of dangers online.").

180. WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

181. *Id.* at 23.

182. *See* Press Release, White House, Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Bill of Rights (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.; Danny Weitzner, *We Can't Wait: Obama Administration Calls for a Consumer Bill of Rights for the Digital Age*, WHITE HOUSE BLOG (Feb. 23, 2012, 4:00 PM), http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age.

data is lost or disclosed.[183] These laws, which have "transformed previously unnoticeable corporate lapses into press events with deep brand implications," have drawn attention not only to breaches themselves, but also to corporations' collection and retention of information about users. Such laws have given privacy advocates an opportunity to sustain activism by "keep[ing] privacy and data protection on the front burner."[184]

Data breach laws have been effective on multiple levels. The laws have created both direct and indirect costs for a company. If a company experiences a data breach, it must pay hard costs to notify customers and to remediate breached records, and it also faces the loss of both customer trust and potential future business.[185] These laws also provide an ongoing opportunity for consumers to engage in public dialogue with companies about their security practices and to pressure companies to take steps to reduce the risks of a data breach.[186] This in turn leads companies to give greater weight both to internal voices arguing for stronger privacy protection and to consumer concerns, leading to visible responses that encourage future collective action.

The California legislature passed, and Governor Brown signed, the first book privacy law for the digital age—the California Reader Privacy Act—on October 2, 2011. The Act, which went into effect on January 1, 2012,[187] ensures that government entities and third parties cannot demand access to personal reading information held by any book service, whether online or at the corner bookstore, without obtaining a court order and showing both a compelling interest for the information and that demanding reading records is the least intrusive means of obtaining necessary information.[188] Book service providers are also required to provide transparency to consumers about how often their reading information is disclosed by reporting government demands for personal reading records and the type of information disclosed.[189] Any book service provider with an online presence must make this information publicly available in an online searchable format on an annual basis.[190]

In 2012, California Attorney General Kamala Harris announced that her

183. Bamberger & Mulligan, *supra* note 41, at 292.

184. *Id.*

185. *Id.* at 293.

186. *Id.*

187. *See Reader Privacy Act of 2011 – Signed by Governor Brown!*, ACLU OF N. CAL., https://www.aclunc.org/issues/technology/reader_privacy_act_of_2011_-_signed_by_governor_brown.shtml (last visited Apr. 3, 2012).

188. See final chaptered bill language. S. 602, 2011–12 Leg., Reg. Sess. (Cal. 2011), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0601-0650/sb_602_bill_20111002_chaptered.html. A book service provider is required to publish a report if it has disclosed personal information related to the access or use of a book service or book of more than thirty total users consisting of users located in California or users whose location is unknown or of both types of users.

189. *Id.*

190. *Id.*

office would be enforcing the California Online Privacy Protection Act of 2003[191] against mobile applications that failed to provide a privacy policy detailing their collection and use of personal information.[192] Attorney General Harris also announced an agreement with major mobile platform providers that would allow users to review an app's privacy policy before downloading and installing the app.[193]

6. International Regulators and Lawmakers

International regulators have been active in engaging with privacy concerns arising from the development of new online products and services. While these regulators work outside of the United States, the global reach of online services means that when their work has improved corporate privacy protections, it has often strengthened the baseline of protections for many users around the world.

The Office of the Privacy Commissioner of Canada ("OPC") and provincial privacy commissioners within Canada have been particularly active in addressing privacy threats that new technology presents. In 2009, OPC completed a year-long investigation of Facebook. OPC found that the company had violated Canadian privacy law in several instances. OPC negotiated with the company to resolve those violations and strengthen controls for third-party apps for all Facebook users worldwide.[194] Meanwhile, the Ontario Information & Privacy Commissioner's Office has established itself as a leading advocate of the "Privacy by Design" concept, working with companies to ensure that privacy is part of the product design process.[195]

Privacy regulators and lawmakers in Europe have also been active defenders of online privacy. The EU Data Protection Working Party issued a report in May 2009 addressing the application of EU law, including privacy regulations, to social networking services.[196] That same year, the European Parliament passed a directive requiring both prior consent before data collection and breach

191. CAL. BUS. & PROF. CODE §§ 22575–79 (West 2005).

192. Press Release, Cal. Office of the Attorney Gen., Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Apps (Feb. 22, 2012), *available at* http://oag.ca.gov/news/press_release?id=2630. *See also Joint Statement of Principles*, OFFICE OF ATTORNEY GENERAL KAMALA D. HARRIS (Feb. 22, 2012), available at http://ag.ca.gov/cms_attachments/press/ pdfs/n2630_signed_agreement.pdf? ("It is the opinion of the Attorney General that the California Online Privacy Protection Act requires mobile applications that collect personal data from California consumers to conspicuously post a privacy policy.").

193. *Id.*

194. *See* Press Release, Office of the Privacy Comm'r of Can., Facebook Agrees to Address Privacy Commissioner's Concerns (Aug. 27, 2009), *available at* http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_e.cfm.

195. *See* PRIVACY BY DESIGN, http://privacybydesign.ca (last visited Jan. 7, 2012).

196. *See* Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, 01189/09 (2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

notification in all EU nations.[197] In 2011, EU regulators issued a renewed call for a comprehensive approach to data protection.[198] Data protection officers in individual European countries have also actively engaged in online privacy matters. For example, when Google revealed that its Street View cars had been capturing wireless network traffic in late 2010, it faced investigations and sanctions in many European nations, including the Czech Republic, France, Italy, Germany, and Spain.[199]

In addition to acting independently, international privacy regulators have increasingly operated in concert to investigate and address potential threats to consumer privacy. In 2008, the International Working Group on Data Protection in Telecommunications issued a set of recommendations for social networking users and providers.[200] Later that same year, the 30th International Conference of Data Protection and Privacy Commissioners adopted a similar resolution.[201] And in September 2010, thirteen privacy enforcement agencies worldwide, including the FTC, formed the Global Privacy Enforcement Network.[202] As online companies increasingly reach out to international consumers, the role of international cooperation in regulating online privacy is likely to expand.

E. Increased Resources for Privacy Community

Increased financial resources available to the privacy community have also shaped the coalescing of a privacy social movement by enabling the privacy community to engage in more consistent, robust, and coordinated efforts to investigate and identify emerging online privacy issues and educate the press, lawmakers, regulators, businesses, and the public. The current level of expertise, focus, and coordination in the privacy community is the product of many years

197. *See* Directive 2009/136/EC, 2009 O.J. (L 337) 11, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF.

198. *See* Press Release, Europa, European Data Protection Commissioners Insist on the Need for a Comprehensive EU Approach to Data Protection (Apr. 6, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/11/4&format=HTML&aged=0&language=EN&guiLanguage=en.

199. Stephanie Bodoni, *Google Street View Privacy Probe Joined by Spain, Italy, France*, BLOOMBERG (May 20, 2010, 9:28 AM), http://www.bloomberg.com/news/2010-05-19/google-street-view-privacy-breach-probe-is-joined-by-spain-italy-france.html. The investigation in France was ultimately settled after Google paid a fine of €100,000. Mimosa Spencer & Ruth Bender, *Google Fined in France Over Street View*, WALL ST. J. (Mar. 21, 2011, 11:25 AM), http://online.wsj.com/article/ SB10001424052748703858404576214531429686752.html.

200. INT'L WORKING GRP. ON DATA PROT. IN TELECOMMS., REPORT AND GUIDANCE ON PRIVACY IN SOCIAL NETWORKS (Report No. 675.36.5, Mar. 4, 2008), *available at* http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf.

201. 30TH INT'L CONFERENCE OF DATA PROT. AND PRIVACY COMM'RS, RESOLUTION ON PRIVACY PROTECTION IN SOCIAL NETWORKING SERVICES, (Oct. 17, 2008), *available at* http://www.lda.brandenburg.de/sixcms/media.php/3509/resolution_social_networks_en.pdf. *See also* Data Protection Working Party, *supra* note 196.

202. *See* GLOBAL PRIVACY ENFORCEMENT NETWORK, https://www.privacyenforcement.net/ (last visited Jan. 7, 2012).

of infrastructure development and planning. The process of building an effective privacy movement began with the greater availability of funding allocated for privacy work in the early 2000s, but only in recent years has the movement reached the critical mass required to establish cohesive and long-term structures that support meaningful change.

The availability of cy pres funding [203] to privacy organizations and the increasing investment in privacy and technology policy by academic institutions have helped to create the steady resources and support the collaborative work necessary to create positive change for online privacy. Since 2002, the Consumer Privacy Rights Fund managed by the Rose Foundation has awarded over $4.5 million to support privacy-related research, education, advocacy and policy development in California and throughout the United States, with more than $1.5 million allocated in the summer of 2008 alone.[204] The California Consumer Protection Foundation (CCPF) has also managed and distributed substantial cy pres funding for privacy work.[205] CCPF's Privacy Rights Fund, active from 2007 to 2010, awarded thirteen organizations a total of approximately $1 million for a variety of privacy protection efforts.[206] Since many organizations throughout the country applied to the same grant funds during the same time period, all for consumer privacy projects, complementary projects emerged that addressed a range of important online privacy work:

- The University of California-Berkeley Law School and School of Information received funding to conduct survey research on consumer understanding of online privacy policies and attitudes towards privacy.[207]
- The Stanford Law School Center for Internet and Society received funding to create its Consumer Privacy Project.[208]
- The Electronic Frontier Foundation received funding to focus on mobile

203. Cy pres are funds in class action cases (and sometimes other types of proceedings) that cannot be distributed to the class members or beneficiaries who were the intended recipients, and that courts distribute to charitable causes. See *The California Bar Foundation and* Cy Pres *Awards*, CAL. BAR FOUND., http://www.calbarfoundation.org/contribute/cypres.html (last visited Apr. 4, 2012).

204. *See Consumer Privacy Rights Fund*, ROSE FOUND., http://www.rosefdn.org/article.php?list=type&type=111 (last visited Jan. 7, 2012). The $1.5 million figure represents the sum of the listed grant allocation amounts.

205. *See CCPF and Cy Pres*, CAL. CONSUMER PROT. FOUND., http://consumerfdn.net/about-cy-pres/ccpf-and-cy-pres/ (last visited Jan. 22, 2012).

206. *Trust Funds*, CAL. CONSUMER PROT. FOUND. http://consumerfdn.net/about-us/trust-funds/. (last visited Jan. 22, 2012).

207. *Grantee's Database*, CAL. CONSUMER PROT. FOUND., http://consumerfdn.org/ about-us/grantees/grantees-database/ (last visited Apr. 15, 2012) (hereinafter Grantee's Database); *Grants List, Berkeley Center for Law and Technology*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13071 (last visited Apr. 15, 2012);

208. *Grants List, Stanford Law School*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13120 (last visited Apr. 15, 2012);

privacy issues.[209]

- The Center for Democracy and Technology received funding to support its policy work related to behavioral advertising and policy ideas related to developing a "Do Not Track" list.[210]
- Consumer Watchdog received funding to support its Google Privacy Rights Project.[211]
- Privacy Rights Clearinghouse received funding to sustain and expand its work to provide resources to individuals experiencing online privacy problems and to support the passage of consumer privacy bills in California.[212]
- PrivacyActivism received funding to produce an educational curriculum for students about social networking privacy.[213]
- ACLU-NC received funding to support the development of its "Demand Your dotRights" campaign to educate and activate consumers, policymakers, and businesses to update privacy protections for the modern online world.[214]

Academic institutions have also taken on substantial new research, developed student resources, and prepared a new generation of attorneys to grapple with the legal and policy implications of online privacy. Legal academics, such as Professors Orin Kerr and Daniel Solove of George Washington University, who explore online privacy from a primarily legal perspective, are joined by colleagues, such as Professor Paul Ohm of the University of Colorado and Professor Deirdre Mulligan of the University of California, who apply computer science and consumer research perspectives to online privacy issues.[215] In the past decade, multiple academic institutions have established research centers that encourage students to pursue projects related to

209. *Grantee's Database, supra* note 207; *Grants List, Electronic Frontier Foundation/First Amendment Project*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13094 (last visited Apr. 15, 2012).

210. *Grantee's Database, supra* note 207; *Grants List, Center for Democracy & Technology*, THE ROSE FOUNDATION, http://www.rosefdn.org/ userdata_display.php?modin=67&uid=13077 (last visited Apr. 15, 2012);

211. *Grants List, Consumer Watchdog*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13088 (last visited Apr. 15, 2012).

212. *Grantee's Database, supra* note 207; *see, e.g.*, *Grants List, Privacy Rights Clearinghouse*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13116 (last visited Apr. 15, 2012).

213. *Grants List, Privacy Activism*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13113 (last visited Apr. 15, 2012).

214. *Grantee's Database, supra* note 207; *Grants List, ACLU Foundation of Northern California*, THE ROSE FOUNDATION, http://www.rosefdn.org/userdata_display.php?modin=67&uid=13069 (last visited Apr. 15, 2012).

215. *See Orin S. Kerr*, GW LAW, http://www.law.gwu.edu/Faculty/profile.aspx?id=3568; *Daniel J. Solove*, DANIELSOLOVE.COM, http://danielsolove.com; *Paul Ohm*, PAULOHM.COM, http://paulohm.com/; *Deirdre Mulligan*, BERKELEY LAW, http://www.law.berkeley.edu/php-programs/faculty/facultyProfile.php?facID=1018 (all sites were last visited on Jan. 22, 2012).

privacy and technology and provide training for new attorneys to work in this field. These centers include the Berkman Center for Internet & Society at Harvard University, the Berkeley Center for Law & Technology at the University of California-Berkeley, the Center for Internet & Society at Stanford University, the Center for Information Technology Policy at Princeton University, and the Center for Communications Law & Policy at the University of Southern California.[216]

In addition to research centers, clinics at several law schools in North America provide law students with hands-on experience dealing with clients and cases concerning online privacy and other technology policy issues. The first such clinic, the Samuelson Law, Technology and Public Policy Clinic at University of California, Berkeley, was founded in 2001. Since then, the principal initial funders of that clinic, Professors Pam Samuelson and Robert Glushko, have endowed additional clinics at the Washington College of Law at American University, the University of Ottawa, the University of Colorado, and Fordham University.[217] Other law schools, including Harvard Law School and the University of Southern California School of Law, also offer students clinical experiences dealing with online privacy.[218] Students and faculty at these clinics have made significant contributions; for example, the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic ("CIPPIC") at the University of Ottawa filed an initial complaint[219] that led to an investigation of Facebook's privacy practices by the Information Privacy Commissioner of Canada.[220] Clinics have also become an important training ground for new talent for

216. See *Berkman Center for Internet & Society*, HARV. U., http://cyber.law.harvard.edu/; *Berkeley Center for Law & Technology*, BERKELEY L., http://www.law.berkeley.edu/bclt.htm; *The Center for Internet and Society*, STAN. L. SCH., http://cyberlaw.stanford.edu/; *Center for Information Technology Policy*, PRINCETON U., http://citp.princeton.edu/; *Center for Communication Law & Policy*, U. S. CAL. GOULD SCH. OF L., http://cclp.usc.edu/ (all sites were last visited on Jan. 22, 2012).

217. *See Samuelson Law, Technology, & Public Policy Clinic*, BERKELEY L., http://www.law.berkeley.edu/4391.htm; *Glushko-Samuelson Intellectual Property Law Clinic*, AM. U. WASHINGTON COLL. OF L., http://www.wcl.american.edu/ipclinic/ (last visited Apr. 15, 2012); *Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)*, CIPPIC.CA, http://www.cippic.ca/; *Samuelson-Glushko Technology Law & Policy Clinic*, COLO. L., http://www.colorado.edu/law/clinics/tech/; *Samuelson-Glushko Intellectual Property and Information Law Clinic*, FORDHAM SCH. OF L., http://law.fordham.edu/clinical-legal-education/5428.htm (all sites were last visited Apr. 15, 2012).

218. *Intellectual Property and Technology Law Clinic*, USC GOULD SCH. OF L., http://weblaw.usc.edu/why/academics/clinics/iptl/ (last visited Apr. 15, 2012); *Cyberlaw Clinic*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U., http://cyber.law.harvard.edu/teaching/cyberlawclinic (last visited Apr. 15, 2012).

219. Press Release, CIPPIC, CIPPIC Files Privacy Complaint Against Facebook (May 30, 2008), *available at* http://www.cippic.ca/uploads/NewsRelease_30May08.pdf. For more details, *see* infra nn.277–316 and accompanying text.

220. *PIPEDA Complaints: Facebook (May 2008-Facebook)*, CIPPIC, http://www.cippic.ca/en/pipeda-complaints ((last visited Apr. 3, 2012). *Facebook Breaches Canadian Privacy Law: Commissioner*, CBC NEWS TECH. & SCI. (July 16, 2009, 3:20 PM), http://www.cbc.ca/news/technology/story/2009/07/16/facebook-privacy-commissioner.html.

organizations, from interns and legal fellows to permanent staff. A sample of the presenters at the tenth anniversary event of Berkeley's Samuelson Clinic reveals the diverse privacy work of clinic graduates, from the work of public interest organizations like the ACLU and the Electronic Frontier Foundation ("EFF"), to that of government agencies, academic institutions, and the offices of in-house policy counsel at Internet companies like Google.[221]

In recent years, regular meetings and conferences have supported opportunities for diverse members of the privacy community to meet and collaborate. The Privacy Coalition, a loose coalition of privacy organizations, was established in 1995 and continues to meet monthly to discuss strategies for addressing privacy issues as they arise.[222] In recent years, the privacy community has created more institutionalized methods for communicating and collaborating with one another. For example, a coalition of California-based privacy groups, including organizations and representatives from law school clinics, meet in Sacramento each year to discuss plans for the upcoming legislative session. Since 2007, staff from organizations, law school clinics, and centers in Northern California have met quarterly as the "Bay Area Privacy Group" to discuss current and emerging work.

New conferences have also provided additional opportunities to connect. The Computers, Freedom, and Privacy Conference, now in its twenty-second year, was for a long time the primary annual event for organizations and individuals interested in privacy issues to meet and share information.[223] In recent years, new events have provided additional opportunities for the privacy community to interact and to collaborate. For example, the Privacy Law Scholars Conference provides a forum for privacy scholars from many disciplines and practitioners from companies, private practice, public interest, and government to enhance ties and facilitate dialogue among different parts of the privacy community.[224] In 2011, the conference brought together over 200 participants to discuss emerging issues, new research, and new ways to approach privacy concerns.[225]

With additional funding and trained talent, privacy organizations are better equipped to fulfill their missions as opportunities ripen for meaningful change in the arena of online privacy. These organizations can (and often do) act independently to promote change through direct dialogue with companies and lawmakers. However, recent successes have shown that privacy work is more

221. Examples can be found in the list of presenters for the Samuelson Clinic Anniversary, BERKELEY L., *available at* http://www.law.berkeley.edu/10580.htm (last visited Oct. 24th, 2011).

222. *See Privacy Coalition*, PRIVACYCOALITION.ORG, http://privacycoalition.org/about.php (last visited Apr. 16, 2012).

223. *Computers, Freedom & Privacy*, CFP.ORG, http://www.cfp.org/2011/wiki/index.php/Main_Page (last visited Apr. 16, 2012).

224. *Privacy Law Scholars Conference*, GEO. WASH. U. L, SCH., http://docs.law.gwu.edu/facweb/dsolove/PLSC/ (last visited Jan. 7, 2012).

225. *Id.*

effective when it leverages the other factors discussed here to create a holistic campaign to address privacy concerns. The next section explores how the privacy community has successfully leveraged changes related to users, the media, lawmakers, regulators, and the economy to address specific privacy issues and create change.

IV.
LEVERAGING SPECIFIC INCIDENTS TO CREATE VIRTUOUS CYCLES AND A SUSTAINABLE PRIVACY SOCIAL MOVEMENT

As noted in Part I,[226] one of the primary challenges of establishing a privacy social movement is sustainability. While the privacy community has had success in the past in addressing specific incidents, these successes did not initially lead to a coherent and sustainable privacy social movement.[227] More recently, however, advocates have successfully leveraged the environmental changes discussed in Part II to win specific battles to protect individual privacy. The privacy community has also used those victories to reinforce the climate for change and support the discussion necessary to sustain the nascent social movement. This has helped to create a much-needed "virtuous cycle"[228] in which each successful advocacy effort reinforces awareness of the ongoing issues concerning online privacy and makes it easier both to challenge specific practices in the future and to lay the groundwork for broader-reaching change.

The following two case studies illustrate how recent changes have contributed to positive outcomes in specific privacy conflicts, to increasing attention to privacy issues generally, and to the creation of ongoing support for a sustainable online privacy movement.

A. Location Information Privacy: Apple iPhone Case Study

On April 20, 2011, Apple faced a storm of controversy when researchers Alasdair Allan and Pete Warden published research showing that iPhones were capturing and storing location information in unencrypted form in a file on the phone.[229] Although forensic phone analysts had written about the data files

226. *See supra* notes 81–86 and accompanying text..

227. *See generally* BENNETT, *supra* note 2, at 133–67, 199–200 (discussing controversies that have arisen throughout the privacy advocacy network and would-be movements that have disbanded).

228. A virtuous cycle is "a beneficial cycle of events or incidents, each having a positive effect on the next." *Virtuous Cycle Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/virtuous+cycle (last visited Jan. 7, 2012).

229. Alasdair Allan & Pete Warden, *Got an iPhone or 3G iPad? Apple is Recording Your Moves*, O'REILLY RADAR (Apr. 20, 2011), http://radar.oreilly.com/2011/04/apple-location-tracking.html. A few days later, researchers revealed that Android phones also retained location information in a file on the phone; however, only 12 hours worth of cell tower data and 48 hours worth of WiFi data was retained (with a maximum of 50 entries), and the file was not accessible to users or copied to any other device. Matthew Panzarino, *It's Not Just the iPhone, Android Stores*

months earlier,[230] the initial discovery went largely unnoticed by the media and public. The new research attracted the public's attention because it included both analysis of the implications of the data and an app that allowed users to view their own location history on a map.[231] It was also released at the Where 2.0 conference on location-based services, where it caught the attention of media and public interest organizations in attendance.[232]

In years past, the location file might not have sparked much interest or controversy. However, widespread ownership of the iPhone, Allan and Warden's app that clearly communicated the privacy implications to users, and the increased attention paid to mobile and location-based services by media, public interest groups, and regulators resulted in an explosion of attention from lawmakers and the press.[233] The public outcry led to Apple's quick decision to fix the "bug" and clarify its location-tracking practices.

1. Environmental Factors that Promoted a Positive Outcome

a. Adoption of Mobile and Location-Based Services and User Awareness

The public reacted strongly when news of the iPhone location file broke because a large percentage of the public (including regulators and lawmakers) owned iPhones or similar devices and therefore felt personally affected by the issue. As of July 2011, 35 percent of American adults owned a smartphone.[234] The iPhone has been one of the most popular smartphones, with over 70 million phones sold by the fall of 2010.[235] Consumers had also steadily increased their use of location-based apps and services.[236]

Your Location Data Too, THENEXTWEB (Apr. 21, 2011), http://thenextweb.com/google/2011/04/21/its-not-just-the-iphone-android-stores-your-location-data-too/.

230. Alex Levinson, *3 Major Issues With the Latest iPhone Tracking "Discovery,"* ALEX LEVINSON (Apr. 21, 2011), https://alexlevinson.wordpress.com/2011/04/21/3-major-issues-with-the-latest-iphone-tracking-discovery/.

231. Allan & Warden, *supra* note 229.

232. *See, e.g.*, Thomas Claburn, *iPhone Software Tracks Location of Users*, INFORMATIONWEEK SECURITY (Apr. 20, 2011, 2:51 PM), http://www.informationweek.com/news/security/privacy/229401960. Claburn notes that "French blogger Paul Coubis appears to have been the first to report this issue last year, though his findings didn't attract much attention," unlike the demonstration at the Where 2.0 conference. *Id.*

233. As of Jan. 22, 2012, over 27,500 web sites linked to the initial blog post. *See* GOOGLE, http://www.google.com (search for "http://radar.oreilly.com/2011/04/apple-location-tracking.html").

234. Aaron Smith, *Smartphone Adoption and Usage*, PEW INTERNET (July 11, 2011), http://pewinternet.org/Reports/2011/Smartphones.aspx.

235. Greg Kumparak, *Apple Sold Over 14.1 Million iPhones Last Quarter, Over 70 Million Since Launch*, TECHCRUNCH (Oct. 18, 2010), http://techcrunch.com/2010/10/18/apple-sold-14-1-million-iphones-last-quarter-over-70-million-since-launch/.

236. As of November 2010, online adults ages 18 to 29 accessed location-based services at a rate of eight percent, and ten percent of online Hispanics used the services. Kathryn Zickuhr &

Furthermore, Allan and Warden's visualization app strengthened the public's sense of being directly affected by the iPhone location file. iPhone owners who used the app were able to see how the data stored on their own iPhone could reveal sensitive information about their travels and activities. By making the information visceral and personal, the app helped people understand how their own personal information was at risk and led users to demand that Apple address the privacy issues at stake.

b. Economic Factors

Economic factors appear to have both contributed to the existence of the location file on iPhones and driven Apple to quickly respond when the story about the file broke. Apple, like many other companies, was looking for ways to develop and support location-based services and utilize location data to take advantage of the rapidly emerging market for such services and for geographically targeted advertising.[237] Two months before the iPhone story broke, Apple banned location-based advertising by third parties, leading to speculation that it planned to control (and profit from) such advertising itself.[238] Ongoing research, including the filing of a patent application the previous month for "location histories for location aware devices," also suggested Apple's strong interest in utilizing location data.[239] Thus, it was unsurprising when Apple explained that it had been collecting and storing cell tower data in order to make location-based services more efficient and to support location-based advertising.[240]

However, during the time that Apple and other companies were increasing their attempts to monetize location data, consumers were becoming more sensitive to the fact that their location information was being collected and more

---

Aaron Smith, *4% of Online Americans Use Location-Based Services,* PEW INTERNET (Nov. 4, 2010), http://www.pewInternet.org/Reports/2010/Location-based-services.aspx. *See generally* ACLU OF N. CAL., LOCATION-BASED SERVICES: TIME FOR A PRIVACY CHECK-IN (2010), *available at* http://dotrights.org/sites/default/files/lbs-white-paper.pdf.

237. *Apple Q & A on Location Data,* APPLE PRESS INFO (Apr. 27, 2011), http://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html. At the time the market for location-based services was estimated at $2.9 billion, and expected to rise to $8.3 billion in 2014. Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data,* WALL ST. J. ONLINE (Apr. 22, 2011), *available at* http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html. Location-based advertising was also seen as a potential revenue stream, with brands including Burger King, Westin Hotels & Resorts and The Home Depot among a growing list of companies that use mobile apps to target consumers by location. Tim Peterson, *Location-Based Targeting Through Ads and Apps Increases Consumer Interaction,* DIRECT MARKETING NEWS (June 1, 2011), http://www.dmnews.com/location-based-targeting-through-ads-in-apps-increases-consumer-interaction/article/203565/.

238. Daniel Indiviglio, *Why Is iPhone Banning Location-Based iPhone Ads?,* THE ATLANTIC (Feb. 5, 2010, 12:30 PM), http://www.theatlantic.com/business/archive/2010/02/why-is-apple-banning-location-based-iphone-ads/35435/.

239. Ryan Tate, *Apple Patent Reveals Extensive Stalking Plans,* GAWKER (Apr. 25, 2011, 5:58 PM), http://gawker.com/5795442/apple-patent-reveals-extensive-stalking-plans.

240. *Apple Q & A, supra* note 237.

concerned about the associated privacy and security risks.[241] Consumers' growing realization that their location information is increasingly being collected, stored, and used in ways that they did not intend or desire threatens the profitability of location-based services and advertising. Thus, when this story broke, Apple had a strong incentive to respond quickly and assuage user concerns, and other companies had an incentive to ensure that their products did not contain similar privacy flaws.

c. Growth of Specialized Media

The specialized technology media played a very significant role in the iPhone story and the rapid response to this privacy issue. Several factors, including a series of stories recently published about mobile and location-based privacy, the iPhone controversy breaking at a location-based technology conference in Silicon Valley, and the development of the app allowing users to see the implications of this data collection, made this story ripe for widespread press attention.

Before the iPhone story broke, the technology press had become increasingly attentive to developments in location-based services. When Facebook announced its new location-based service component, "Places," many of the stories focused on privacy implications related to increased sharing and use of location information.[242] The "What They Know" series in *The Wall Street Journal* included articles about mobile apps and location privacy,[243] including research showing that, among 101 popular apps, the majority collected and transmitted the user's device ID, location, and/or demographic data without the user's knowledge and consent—and that companies receiving such data included Apple and Google, as well as advertising networks.[244] In March 2011, just a few weeks before the iPhone story, there was also significant coverage about telephone companies and tracking practices in Germany.[245] German Green party

241. *See supra* notes 18–22 and accompanying text.

242. *See, e.g.*, Stephanie Goldberg, *New Facebook Feature Raises More Privacy Concerns*, CNN TECH (Aug. 19, 2010), http://articles.cnn.com/2010-08-19/tech/facebook.places.privacy_1_privacy-controls-privacy-concerns-feature; Jemima Kiss, *Facebook Places Location Tool Revealed, Sparking Fresh Privacy Concerns*, THE GUARDIAN (Aug. 18, 2010), *available at* http://www.guardian.co.uk/technology/2010/aug/19/facebook-places-location-tool-unveiled.

243. Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL ST. J.: WHAT THEY KNOW (Aug. 3, 2010), *available at* http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html; Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J.: WHAT THEY KNOW (Dec. 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html. When the iPhone story broke, the *Journal* quipped: "This kind of cellphone tracking will come as no surprise to *Wall Street Journal* readers, of course." Jennifer Valentino-Devries, *What Your iPhone Knows About You,* WALL ST. J. DIGITS BLOG (Apr. 20, 2011, 2:45 PM), http://blogs.wsj.com/digits/2011/04/20/what-your-iphone-knows-about-you/.

244. Thurm & Kane, *supra* note 243.

245. *See* Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know,* N.Y.

politician Malte Spitz sued Deutsche Telekom to find out just how much data they were collecting about him and discovered that the mobile provider had logged his location over 35,000 times in a six-month period between August 2009 and February 2010.[246]

The fact that the iPhone tracking story broke at the Where 2.0 location-based services conference in Silicon Valley, which already held the attention of the technology media, contributed to how quickly it spread. Technology writers and bloggers from publications including the *Washington Post*, *Forbes*, and *ReadWriteWeb* were present at the conference when the story first broke.[247] This led to rapid dissemination of the story through a range of domestic and international media channels.

d. Non-Profits and Academics

Prior to the iPhone location file controversy, non-profit organizations had already invested a significant amount of time analyzing privacy issues related to location information and so were ready to respond quickly and knowledgeably about the issues related to this story.[248] ACLU and EFF had been involved in several cases opposing warrantless tracking of an individual's location. The organizations had filed amicus briefs in support of a magistrate judge's authority to refuse to order the disclosure of location records under the Electronic Communications Privacy Act ("ECPA"),[249] in support of the suppression of cell site location information obtained in a criminal investigation without a search warrant,[250] and in support of the suppression of evidence obtained by placing a

---

TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html.

246. *Id.*

247. *Cf.* Nathanial Vaughn Kelso, *A Recap of Where 2.0: The Conference for All Things Location-Aware*, WASH. POST @INNOVATION (Apr. 29, 2011), http://on.washingtonpost.com/post/5045617385/a-recap-of-where-2-0-the-conference-for-all-things; Aaron Perlut, *Sights and Sounds from Where 2.0*, FORBES MARKETSHARE (Apr. 21, 2011, 5:43 PM), http://www.forbes.com/sites/marketshare/2011/04/21/sights-and-sounds-from-where-2-0/; Mike Melanson, *What to Expect from Where 2.0 in 2011: Context, Crowdsourcing, and Proximity*, READWRITEWEB (Apr. 14, 2011, 4:15 PM), http://www.readwriteweb.com/archives/what_to_expect_from_where_20_in_2011_context_crowd.php.

248. However, Alasdair Allan and Pete Warden, the researchers who broke the story and created the visualization app, were not in either the academic or the non-profit sector. They were primarily looking at the data on the iPhone for visualization purposes. Allan & Warden, *supra* note 213.

249. Brief for Elec. Frontier Found. et al. as Amici Curiae Supporting Affirmance of the District Court, In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. Sept. 7, 2010) (No. 08-4227), *available at* http://www.aclu.org/files/assets/FiledCellTrackingBrief.pdf.

250. Brief for Am. Civil Liberties Union et al. as Amici Curiae Supporting Motion to Suppress, United States v. Soto, No. 3:09-cr-200 (AWT) (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf.

GPS tracking device on a criminal suspect's vehicle without a search warrant.[251] EPIC had filed complaints with the FTC about Facebook Places in August 2010,[252] and ACLU-NC published its concerns about the feature.[253] ACLU-NC also published a white paper about privacy issues related to location-based services and a companion chart analyzing the privacy practices of six leading location-based services.[254] Several non-profit institutions had also highlighted the need for location privacy reform as part of congressional hearings on reforming the ECPA.[255]

Academic researchers were also taking a closer look at issues related to location information. Several legal scholars had raised concerns about the lack of clear legal protections for location information.[256] Researchers at institutions such as the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon and the School of Information at Berkeley had examined technical aspects and user perceptions of threats to the privacy of location information.[257]

Thus, when the iPhone story broke, privacy lawyers, technologists, and academics were poised to provide well-informed commentary and responses. By

---

251. Brief for Elec. Frontier Found. and Am. Civil Liberties Union of the Nat'l Capital Area as Amici Curiae Supporting Appellant Jones, United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *cert granted sub nom* United States v. Jones, No. 10-1259 (Mar. 3, 2009), *available at* https://www.eff.org/files/filenode/US_v_Jones/Jones.DCCirBrief.EFFACLU.PDF.

252. *See* Press Release, Electronic Privacy Information Center, Facebook "Places" Embeds Privacy Risks, Complicated and Ephemeral Opt-Out Unfair to Users (June 10, 2011), *available at* http://epic.org/privacy/inrefacebook/.

253. Nicole A. Ozer, *Facebook Places: Check This Out Before You Check In*, ACLU OF N. CAL. (Aug. 18, 2010, 5:45 PM), http://www.aclunc.org/issues/technology/blog/facebook_places_check_this_out_before_you_check_in.shtml.

254. *See Location-Based Services: Time for A Privacy Check-In,* ACLU OF N. CAL. DOTRIGHTS, http://dotrights.org/lbs/ (last visited Nov. 16, 2011).

255. *E.g.*, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 2 (2010) (Statement of James X. Dempsey, Vice President for Public Policy, Center for Democracy & Technology), *available at* https://www.cdt.org/files/pdfs/20100922_jxd_testimony_ecpa.pdf; *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 2 (2010) (Statement of Am. Civil Liberties Union), *available at* http://www.aclu.org/files/assets/Statement_senate_judiciary_committee_ECPA_hearing.pdf.

256. *E.g.*, Ian J. Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324 (2008); Kevin King, *Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies*, 21 ALB. L.J. SCI. & TECH. 61 (2010).

257. *See, e.g.*, JANICE Y. TSAI, PATRICK GAGE KELLEY, LORRIE FAITH CRANOR & NORMAN SADEH, CARNEGIE MELLON CYLAB, LOCATION-SHARING TECHNOLOGIES: PRIVACY RISKS AND CONTROLS (updated 2010), *available at* http://cups.cs.cmu.edu/LBSprivacy/; NICK DOTY, DEIRDRE K. MULLIGAN & ERIK WILDE, UC BERKELEY SCHOOL OF INFORMATION, PRIVACY ISSUES OF THE W3C GEOLOCATION API, (Report No. 2010-038, 2010), *available at* http://escholarship.org/uc/item/0rp834wf. *See generally The Collection and Use of Location Information for Commercial Purposes: Hearing Before the Subcomm. on Commc'ns, Tech., and the Internet of the H. Comm. on Energy and Commerce,* 111th Cong. (2010) (statement of Lorrie Faith Cranor, Director, CyLab Usable Privacy and Security Laboratory), *available at* http://democrats.energycommerce.house.gov/Press_111/20100224/Cranor.Testimony.2010.02.24.pdf (describing various academic research into the use of location information).

providing immediate analysis of the controversy[258] and engaging in dialogue with the media,[259] momentum for the story grew, reinforcing public awareness and the climate necessary to push for change.

e. Attention from Lawmakers and Regulators

In addition, lawmakers and federal agencies had already started looking into issues related to location privacy before the iPhone story broke. As early as 2002, the FTC had been reviewing issues of privacy and security for users of web-enabled wireless devices and mobile data services.[260] In June 2010, when the press reported on changes Apple had made to its privacy policy, indicating that Apple was sharing geographic location data of people who were using iPads, iPhones, and other Apple products, Representative Edward Markey co-wrote a letter to Apple CEO Steve Jobs asking about details of the new policy.[261]

2. Immediate and Enduring Consequences

Although Apple defended the presence of the file found on iPhones as harmless and unintentional,[262] it ultimately agreed to address the concerns raised by the privacy community, lawmakers, and regulators. On April 27, 2011, Apple announced plans to limit location database files on the iPhone to data collected within the past seven days, to prevent the file from being copied to other devices, and to delete the file entirely when Location Services was turned off.[263] Apple also asserted that the file would be encrypted on the iPhone in the next major iOS software release.[264] Apple promptly followed up, announcing in May that it would release updates by the fall.[265]

The iPhone story's popularity helped to reinforce the media's attention to location privacy. By January 2012, over 27,500 web pages linked to the original post announcing Allan and Warden's discovery.[266] In addition, news coverage of

258. *E.g.*, Chris Conley, *Your iPhone Knows Where You Were Last Night. Who Else Knows?*, ACLU OF N. CAL. (Apr. 20, 2011, 1:30 PM), http://www.aclunc.org/issues/technology/blog/your_iphone_knows_where_you_were_last_night._who_else_knows.shtml.

259. *See* Martin Kaste, *Your iPhone May Be Logging Your Physical Positions*, NAT'L PUBLIC RADIO (Apr. 21, 2011), https://www.npr.org/2011/04/21/135610178/your-iphone-may-be-logging-your-physical-positions (interviewing Peter Eckersley of the Electronic Frontier Foundation).

260. *See* MOBILE WIRELESS WEB, *supra* note 157, at 8–19.

261. Markey had received a response from Apple's General Counsel on July 12, 2010 with details of the privacy policy. Press Release, Congressman Ed Markey, Markey to Apple: Is it iPhone or iTrack? (Apr. 21, 2011), *available at* http://markey.house.gov/press-release/april-21-2011-markey-apple-it-iphone-or-itrack.

262. *Apple Q & A on Location Data*, *supra* note 237.

263. *Id.*

264. *Id.*

265. Mark Gurman, *Apple and Verizon to Deliver Over-the-Air iOS Updates to Verizon iPhone*, 9TO5 MAC (May 4, 2011, 8:28 PM), http://9to5mac.com/2011/05/04/apple-and-verizon-to-deliver-over-the-air-ios-updates-to-verizon-iphone/.

266. *See* Google, http://www.google.com (search for "http://radar.oreilly.com/2011/04/apple-

location privacy increased significantly in 2011, with significant attention also paid to other corporate practices of collecting and using consumer information.[267]

Lawmakers and regulators responded immediately to the news of the iPhone location file, and continued their investigation of location privacy practices long after Apple changed its practices. The day the iPhone story broke, Senator Al Franken wrote a letter to Jobs, demanding a prompt explanation as to why Apple collected and compiled the data, how the data was generated, the level of precision of the location information, whether Apple planned to start encrypting the data, why Apple did not seek consent before collecting the data, whether Apple believed it had complied with its own privacy policy, and to whom, if anyone, had the data been released.[268] The following day, Reps. Markey and Joe Barton wrote a similar letter.[269] Illinois Attorney General Lisa Madigan and European lawmakers also began inquiries.[270] On May 10, the Senate Judiciary Subcommittee on Privacy, Technology and the Law held a hearing on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy."[271] On May 19, the Senate Committee on Commerce, Science, and Transportation held a hearing on "Consumer Privacy and Protection in the Mobile Marketplace," which included statements from both the FTC and Internet companies.[272] The FCC and the FTC co-hosted a Location-Based Services Forum on June 28, inviting representatives from industry, consumer advocacy groups, and academia to discuss best practices for location-aware devices and apps.[273] The FTC released a staff report, *Protecting Consumer Privacy in an Era*

---

location-tracking.html").

267. *See Location Privacy in 2011*, GOOGLE TRENDS, http://www.google.com/trends/?q=location+privacy&ctab=0&geo=all&date=2011 (last visited Apr. 4, 2012) (tracking online media coverage of location privacy in the year 2011).

268. Letter from Sen. Al Franken to Steve Jobs, CEO, Apple Corp. (Apr. 20, 2011), *available at* http://www.franken.senate.gov/files/letter/110420_Apple_Letter.pdf.

269. Markey and Barton's letter to Jobs included similar questions and asked for a response within 15 days. They asked whether the data tracking was intended to track user location and to what end; whether Apple used or planned to use the information for commercial purposes; and whether customers could disable the feature. *E.g.* Letter from Rep. Ed Markey to Steve Jobs, CEO, Apple Corp. (Apr. 21, 2011) (on file with Author), *available at* http://markey.house.gov/docs/apple_ios_letter_04.21.11.pdf.

270. Roy Rasmussen, *Apple iPhone Privacy Concern Response Leaves Lawmakers Leery*, ARCHIVE-NEWS.NET (Apr. 29, 2011), http://archive-news.net/apple-iphone-privacy-concern-response-leaves-lawmakers-leery/534169/.

271. *Notice of Hearing: Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy*, U.S. S. COMM. ON THE JUDICIARY (Apr. 25, 2011), http://judiciary.senate.gov/hearings/hearing.cfm?id=e655f9e2809e5476862f735da16bd1e7.

272. *Notice of Hearing: Consumer Privacy and Protection in the Global Marketplace*, U.S. S. COMM. ON COMMERCE, SCI., AND TRANSP., http://commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=ea6a7c76-be52-4648-a988-3abe93283ad6 (last visited Jan. 8, 2012).

273. Press Release, FCC, FCC to Host Forum Aimed at Helping Consumers Navigate Location-Based Services (May 17, 2011), http://www.fcc.gov/document/fcc-staff-host-forum-aimed-helping-consumers-navigate-location-based-services.

of Rapid Change, which discussed concerns related to privacy of location information.[274] The report outlined recent FTC privacy initiatives related to enforcement, consumer and business education, and policymaking.[275] It also addressed limitations of privacy models and promising new business models.[276]

The legislative, agency, media, and user attention that resulted from this controversy has made it evident to Apple and to other providers of smartphones and location-based services or advertising that protecting user privacy is not optional—and that policymakers are prepared to take action if user data is not adequately safeguarded. The controversy and media attention have also continued to raise the public's awareness of broader location privacy issues. Thus, the iPhone location privacy controversy not only led to immediate changes; it also contributed to the virtuous cycles necessary for the growth of a lasting online privacy social movement.

B. Third Party Applications & Privacy: Facebook Platform Case Study

In 2009, Facebook's policy of granting third party apps broad access to user data came under fire. Since the launch of its "Platform" for apps in 2007, Facebook had allowed any app to access almost all data about the user running the app, as well as that user's friends—whether the app needed that data or not.[277] Thus, a "quiz" about Star Wars trivia or a birthday reminder app was given access to the user's friends list, photos, events, political and religious leanings, and more. Because users were not informed about the breadth of data that apps collected, Platform created the kind of information asymmetry that hinders privacy-protective choice.

Facebook ultimately decided to revamp its data permissions model for apps to reduce access to user information and increase transparency. This decision came about as a result of widespread user adoption and use of apps, economic factors pushing Facebook to address the issue, and concerted pressure from media, public interest groups, and regulators. The granular permissions model adopted by Facebook in response to the controversy has not only addressed specific criticisms leveled at Platform; it has also increased transparency, allowing users to overcome a lack of information about the actual practices of apps and encouraging those apps to consider the economic costs of over-collection of user data.[278] Thus, privacy advocates achieved a specific victory in

274. RAPID CHANGE, *supra* note 44, at 33–34.

275. *Id.*

276. *Id.*

277. *See e.g.*, J.R. Raphael, *The Hidden Secrets of Online Quizzes*, PC WORLD (May 12, 2009, 7:00 PM), http://www.pcworld.com/article/164527/the_hidden_secrets_of_online_quizzes.html (describing several websites' opaque privacy policies).

278. Applications that "overcollect" data that is not needed may have additional security vulnerabilities and even legal liability for that data, in addition to the risk of user outrage if the data collection is unexpected in context. *See generally Privacy and Free Speech: It's Good for Business*, ACLU OF N. CAL., http://dotrights.org/business/primer (last visited Apr. 3, 2012).

forcing these changes, laid the groundwork for future efforts, and sustained consumer and business awareness of privacy issues.

1. Environmental Factors that Promoted a Positive Outcome

a. User Adoption and Awareness

The widespread use and visibility of Facebook Platform apps contributed to the attention and concern that this issue received. Because the vast majority of active Facebook users used apps themselves, or were at least aware that their friends did, they were readily mobilized to take action when made aware that application privacy protections were inadequate to protect their own personal information.

By 2009, when the controversy arose over its data collection practices, Facebook had experienced explosive growth. Within a year of its launch in February 2004, the site had over one million active users, and by September 2009 it had over 300 million active users.[279] 2009 also marked the year that Facebook surpassed rival social network MySpace in the battle for social network market share.[280] Platform also grew rapidly. Platform was first launched in 2007 with apps from over 70 partners.[281] Within two years, application usage exploded, with almost 700 apps attracting more than 100,000 active users in a month and over 49,000 apps attracting at least 50 users.[282]

User awareness was also fostered by the ubiquity of apps on users' Facebook pages. Due to Facebook's News Feed, even Facebook users who did not use apps themselves were often aware when their friends used apps because the services could post to a user's news feed and try to attract additional users. Automatic posts from apps commonly dominated feeds.[283] Thus, once users understood that any app run by their friends could access their data, they might

279. *Timeline*, FACEBOOK, https://www.facebook.com/press/info.php?timeline (last visited Oct. 27, 2011).

280. Priit Kallas, *Top 10 Social Networking Sites by Market Share of Visits 2008–2011*, DREAMGROW, http://www.dreamgrow.com/top-10-social-networking-sites-by-market-share-of-visits-2008-2011/ (last visited Oct. 27, 2011).

281. Kristen Nicole, *Facebook Platform: 30+ Awesome Applications for Facebook*, MASHABLE (May 24, 2007), http://mashable.com/2007/05/24/facebook-platform-30-apps/.

282. Ben Lorica, *2 Years Later, the Facebook Platform Is Still Thriving*, O'REILLY RADAR (May 13, 2009), http://radar.oreilly.com/2009/05/facebook-app-platform-2-year-anniversary.html. The current numbers are even more staggering. "More than 7 million apps and websites are integrated with Facebook, and 500 million people use an app on Facebook every month." Justin Kistner, *How Facebook Will Take Over the Rest of the World in 2012*, VENTUREBEAT (Jan. 2, 2012, 9:56 a.m.), http://venturebeat.com/2012/01/02/facebook-total-world-domination/.

283. *Cf.* Eric Eldon, *Some Ways That Facebook's Platform Changes Will Affect Social Gaming*, INSIDE SOCIAL GAMES (Oct. 30, 2009), http://www.insidesocialgames.com/2009/10/30/some-ways-that-facebooks-platform-changes-will-affect-social-gaming/ (stating that, according to one source, "45% of all stream posts were games and a nearly equivalent amount were from quizzes" prior to planned changes to the News Feed).

recognize their vulnerability to potential privacy invasions by numerous apps.

b. Economic Factors

Facebook's decision to revise its data collection practices was also influenced by economic incentives implicated by Platform. Although allowing apps broad access to information may have pleased app developers, Facebook likely realized that its long-term interest in monetizing Platform required that users trust the service, which meant ensuring that apps functioned according to user expectations.

In 2009, Facebook's explosive growth, coupled with declining advertising markets, drove it to consider taking on additional investors and to explore ways to increase revenues.[284] Platform apps provided one potential source of revenue, as Platform developers were expected to generate up to $500 million in revenue in 2009.[285] By late 2009, Facebook began rolling out "Credits," a form of currency for use across all Platform apps—with Facebook retaining a share of the proceeds.[286]

The launch of Credits gave Facebook an economic incentive to ensure that Platform apps were not merely interesting, but also trustworthy and trusted. Facebook's first effort, the Verified App Program, was launched in May 2009, highlighting apps that "passed Facebook's review for trustworthy user experiences."[287] However, Facebook terminated that program later the same year, announcing that it was "standardizing the idea of verification to apply to all of the applications on Facebook Platform."[288] Addressing expressed concerns with application transparency may have been part of that effort.

---

284. *See* Michael Arrington, *Facebook "Definitely" Raising Capital This Year; Google Considered Acquisition*, TECHCRUNCH (Mar. 27, 2009), http://techcrunch.com/2009/03/27/facebook-definitely-raising-capital-this-year-google-considered-acquisition/ (discussing reports of Facebook's efforts to raise new capital).

285. *See* Eric Eldon, *Facebook Platform Developers Could See $500M in Revenue This Year*, VENTUREBEAT (May 8, 2009), http://venturebeat.com/2009/05/08/facebook-platform-developers-could-see-500m-in-revenue-this-year/; Michael Learmonth, *App Revenue Is Posted to Surpass Facebook Revenue*, AD AGE DIGITAL (May 18, 2009), http://adage.com/article/digital/app-revenue-poised-surpass-facebook-revenue/136700/.

286. *See* Nick O'Neill, *8 Facebook Applications Now Accepting Facebook Credits*, ALL FACEBOOK (Aug. 17, 2009, 4:13 PM), http://www.allfacebook.com/facebook-credits-applications-2009-08. As of July 1, 2011, all social games on Facebook are required to process in-game purchases using Facebook Credits, although non-game apps are not required to do so. Deborah Liu, *Facebook Credits: Concluding the Migration*, FACEBOOK DEVELOPER BLOG (July 1, 2011, 12:30 PM), http://developers.facebook.com/blog/post/519/.

287. Jason Kincaid, *The Facebook Verified App Saga Ends Tomorrow*, TECHCRUNCH (Nov. 30, 2009), http://techcrunch.com/2009/11/30/facebook-verified-app/. *See also* Monica Walsh, *Introducing Our First Verified Apps*, FACEBOOK DEVELOPER BLOG (May 20, 2009, 9:09 AM), http://developers.facebook.com/blog/post/247/.

288. *Id.*

c. Growing Media Awareness

The explosive growth of social networks in general—and of Facebook in particular—led to increasing scrutiny of its privacy practices by both niche and mainstream media, which in turn helped drive awareness of the privacy issues with Platform apps. Media coverage of Facebook ranges from sites expressly dedicated to the service, like AllFacebook,[289] to prominent coverage on technology-centric web sites like CNET and TechCrunch.[290] Traditional newspapers and media outlets also have increased their coverage of technology in general and Facebook in particular by staffing their own technology departments, acquiring or making arrangements with tech-centric sites, or both.[291]

By 2009, the media was regularly investigating and reporting on issues related to privacy on Facebook, including concerns about the privacy implications of Facebook apps. Many sites wrote privacy guides for Facebook users and updated those guides regularly when privacy options and threats emerged or changed.[292] A number of these guides specifically highlighted concerns about third-party Platform apps.[293] In addition, one researcher noted that "nearly a third" of the most popular Facebook apps had no privacy policy that users could access, while others provided access to their privacy policy only after a user installed the app.[294]

Given the focus on privacy issues related to Facebook, the media was ready to provide both coverage and analysis of privacy concerns raised by the public and by government entities. Moreover, as users became more aware of the privacy issues, the media provided sustained attention to the issues that ultimately contributed to Facebook's change of course.

d. Non-Profit and Academic Focus

Non-profit and academic organizations played a critical role in encouraging Facebook to improve privacy for users of Platform apps. Organizations produced

289. *About Us*, ALL FACEBOOK, http://www.allfacebook.com/about (last visited Oct. 27, 2011).

290. CNET, http://www.cnet.com/ (last visited Oct. 27, 2011); TECHCRUNCH, http://techcrunch.com (last visited Oct. 27, 2011).

291. For example, the *New York Times'* Technology page features both its own Bits blog and headlines from partner sites such as ReadWriteWeb, GigaOm, and VentureBeat. *Technology*, N.Y.TIMES, http://nytimes.com/tech/ (last visited Nov. 17, 2011).

292. *See, e.g.*, Jacqui Cheng, *An Updated Guide to Facebook Privacy: December 2009 Edition*, ARS TECHNICA (Dec. 27, 2009, 5:00 PM), http://arstechnica.com/web/guides/2009/12/an-updated-guide-to-facebook-privacy-december-2009-edition.ars (updating a previous Facebook privacy guide dated Aug. 14, 2009).

293. *See, e.g., id.*

294. theharmonyguy, *Privacy Policies on the Top 25 Facebook Applications*, SOCIAL HACKING (July 28, 2009), http://theharmonyguy.com/oldsite/2009/07/28/privacy-policies-on-the-top-25-facebook-applications/.

materials and tools that helped users, the media, and regulators grasp the issue. Organizations leveraged several tools, including Facebook itself, to build a broad base of support for change, and organizations used this base to pressure Facebook to address privacy concerns with Platform.

Academic and non-profit researchers were among the first to identify privacy issues with Platform. By October 2007, researchers Adrienne Felt and David Evans began examining the disparity between the amount of information that applications actually needed and the amount of information to which they had access.[295] Researcher Chris Soghoian expanded upon Felt and Evans's research, pointing out Facebook's "caveat emptor" view on policing apps:

> "[each application] has not been approved, endorsed, or reviewed in any manner by Facebook . . . we are not responsible for . . . the privacy practices or other policies of the Developer. YOU USE SUCH DEVELOPER APPLICATIONS AT YOUR OWN RISK."[296]

In May 2008, CIPPIC, at the University of Ottawa, filed a complaint with the Office of the Privacy Commissioner of Canada alleging that Facebook was in violation of Canadian privacy law for, among other things, failing to limit third-party developer access to unnecessary data and failing to inform users about the extent to which third-party apps could access their personal information.[297] This complaint led to an extensive investigation by the Privacy Commissioner.[298]

In 2009, ACLU-NC developed tools to help users understand exactly what information Platform apps could access. In particular, the organization wrote its own Platform app: a "quiz" about quizzes that pulled information from the user's profile and displayed it to demonstrate exactly how much information apps could access.[299] Thanks to substantial coverage by the media[300] and other non-profit entities,[301] over 180,000 Facebook users took ACLU-NC's quiz, and over 100,000 users signed the associated petition.

---

295. *See* Adrienne Felt & David Evans, *Privacy Protection for Social Networking Platforms*, U. OF VA., http://www.cs.virginia.edu/felt/privacy/ (last visited Oct. 27, 2011).

296. Chris Soghoian, *Exclusive: The Next Facebook Privacy Scandal*, CNET (Jan. 23, 2008), http://news.cnet.com/8301-13739_3-9854409-46.html (quoting Facebook's Terms of Service as of that date).

297. Letter from Philippa Lawson, Director, CIPPIC, to Jennifer Stoddart, Privacy Comm'r of Can. (May 30, 2008), *available at* http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf.

298. *See infra* notes 306–308 and accompanying text.

299. *See* Sarah Perez, *What Facebook Quizzes Know About You*, READWRITEWEB, Aug. 27, 2009, http://www.readwriteweb.com/archives/what_facebook_quizzes_know_about_you.php (discussing the ACLU's Facebook quiz).

300. *E.g.*, Martin Kaste, *Is Your Facebook Profile as Private as You Think?*, NAT'L PUBLIC RADIO (Oct. 27, 2009), https://www.npr.org/templates/story/story.php?storyId=114187478; Caroline McCarthy, *ACLU Chapter Flags Facebook App Privacy*, CNET (Aug. 26, 2009, 3:28 PM), http://news.cnet.com/8301-13577_3-10318842-36.html.

301. *E.g.*, Laura Northrup, *Quiz Yourself About Facebook Quiz Applications*, THE CONSUMERIST (Sept. 5, 2009, 11:30 AM), http://consumerist.com/2009/09/quiz-yourself-about-facebook-quiz-applications-and-privacy.html.

As CIPPIC, ACLU-NC, and other non-profit entities focused on the issue that had been previously identified by academic and public interest researchers, they attracted the attention of the media, regulators, and users—increasing the pressure on Facebook to change its policies and improve privacy protections for users of Platform apps.

e. Regulatory and Legislative Focus

As use of social networking sites exploded, regulators and lawmakers began to focus on the privacy issues and other concerns that these sites presented. The general increase in regulatory attention, particularly by the Information Privacy Commissioner of Canada, helped drive Facebook's decision to alter its Platform privacy protections.

As early as April 2008, international regulators focused on the specific concerns arising from social networks. That month, the International Working Group on Data Protection in Telecommunications adopted the Rome Memorandum, which analyzed the privacy and security risks for users of social networks and issued recommendations for providers, users, and regulators.[302] In October 2008, the 30th International Conference of Data Protection and Privacy Commissioners adopted a similar resolution concerning privacy protections in social networking services.[303] In 2009, the EU Data Protection Working Party followed with an advisory opinion on the application of EU law, including privacy regulations, to social networking services.[304]

Similarly, in the United States and Canada, lawmakers and regulators had begun turning their attention to privacy concerns raised by social networks. Rep. Markey recognized the need to address the growing amount of information collected and shared by services such as Facebook and called for "[s]ome type of omnibus electronic privacy legislation" that applies "regardless of the particular technologies or companies involved."[305]

OPC moved beyond a general concern with online privacy when it launched a formal investigation of Facebook's privacy practices, including Facebook's practice of granting broad access to user data to third-party apps. OPC's investigation of Facebook was initiated by a complaint filed by CIPPIC.[306] After over a year of investigation and discussions with Facebook, OPC found that Facebook's privacy protections for Platform apps failed to provide adequate safeguards to protect misuse of data and failed to obtain the informed consent of users whose information was made available to Platform apps.[307] As a result,

302. INT'L WORKING GRP., *supra* note 200.

303. 30th INT'L CONFERENCE, *supra* note 201. *See also* Data Protection Working Party, *supra* note 196.

304. Data Protection Working Party, *supra* note 196.

305. *See* Clifford, *supra* note 176.

306. Lawson, *supra* note 297.

307. OFFICE OF THE PRIVACY COMM'R OF CAN., COMMISSIONER'S FINDINGS: PIPEDA CASE

OPC recommended "that Facebook implement measures (1) to limit application developers' access to user information not required to run a specific application; (2) whereby users would in each instance be informed of the specific information that an application requires and for what purpose; (3) whereby users' express consent to the developer's access to the specific information would be sought in each instance; and (4) to prohibit all disclosures of personal information of users who are not themselves adding an application."[308]

2. Immediate and Enduring Consequences

After the negative media coverage of Platform privacy issues and the recommendations from OPC, Facebook announced in August 2009 that it would revamp its permissions model for third-party Platform apps, requiring those apps to specify exactly what information they would access and prohibiting access to any other non-public information.[309] The company previewed the new model in April 2010 and required that all existing apps migrate to the new permissions model by June 1, 2010.[310]

On September 22, 2010, Jennifer Stoddart, Canada's Privacy Commissioner, finalized her review of CIPPIC's Facebook complaint. She lauded the change that put in place technical controls to ensure that apps could only access specifically requested user information, stating that "[t]he changes Facebook has put in place in response to concerns we raised as part of our investigation last year are reasonable and meet the expectations set out under Canadian privacy law."[311] She went on to add, however, that "our work with Facebook is not over. . . . We've asked Facebook to continue to improve its oversight of application developers and to better educate them about their privacy responsibilities," among other areas of concern.[312]

The privacy community also issued tempered praise of the changes to Facebook's privacy policies. Several organizations approved of Facebook's decision to increase transparency and require apps to specify the data that would be accessed, but remained concerned about the fact that Platform apps could access a user's information without that user's knowledge or consent if her

---

SUMMARY #2009-008 ¶¶ 192–210 (July 22, 2009), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.

308. *Id.* at ¶ 383.

309. *See* Justin Smith, *Facebook Announces Significant Changes to the Way Applications Can Access User Data*, INSIDE FACEBOOK (Aug. 27, 2009), http://www.insidefacebook.com/2009/08/27/major-changes-to-the-way-facebook-applications-can-access-user-data-are-coming-soon/.

310. *See* Ethan Beard, *A New Data Model*, FACEBOOK DEVELOPER BLOG (Apr. 21, 2010, 1:45 PM), https://developers.facebook.com/blog/post/378/.

311. Press Release, Office of the Privacy Comm'r of Can., Privacy Commissioner Completes Facebook Review (Sept. 22, 2010), *available at* http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.cfm.

312. *Id.*

friend ran an app and accepted its terms.[313]

Facebook's change to require Platform apps to be transparent about the data they collect and use does not appear to have in any way hindered the development of apps: as of November 2011, Facebook stated that its users "install apps more than 20 million times every day" and that "more than 7 million apps and websites" have integrated with Facebook via Platform.[314] However, the new data permissions model has allowed users and privacy advocates to understand better the way that data is collected by apps. It has also put pressure on app developers to justify the data they request.

The privacy issues identified with Facebook Platform highlighted the need for experts in the media, in academia, and in the non-profit sector to not only carefully examine new tools and features released by Facebook and other technology companies but to ensure that any findings are communicated to the public effectively. Although many of the issues with Facebook Platform apps were identified immediately after the feature launched in 2007, responses to ACLU-NC's Facebook Privacy Quiz indicated that most users were unaware of the extent to which apps could access their personal information, what the ACLU-NC coined the "app gap."[315] In recent years, these entities have developed additional tools and visual aids to help users understand how features and changes can impact their privacy.[316] These resources have become an essential part in raising user awareness and creating the momentum needed to enact change.

V.
THE FUTURE OF THE PRIVACY SOCIAL MOVEMENT

In 2012, online privacy issues are now "above the fold," both literally and figuratively. Consumers, companies, and policymakers are thinking increasingly about collection and control of personal information, and the media is highlighting these issues prominently. The five factors identified in this article—widespread technology adoption, economic incentives among corporations, the

313. The ACLU of Northern California, the Electronic Frontier Foundation, and several other privacy and technology groups issued an open letter to Facebook in June 2010 requesting that Facebook take additional steps to address the "app gap." *See* Press Release, Elec. Frontier Found., Open Letter to Facebook: More Privacy Improvements Needed (June 16, 2010), *available at* https://www.eff.org/press/archives/2010/06/16.

314. *Statistics*, FACEBOOK, https://www.facebook.com/press/info.php?statistics (last visited Nov. 18, 2011).

315. *See* Nicole A. Ozer, Tech. and Civil Liberties Policy Dir., ACLU of N. Cal., Comments of the American Civil Liberties Union of Northern California to the Federal Trade Commission at 5–6 (Dec. 21, 2009), *available at* http://www.ftc.gov/os/comments/privacyroundtable/544506-00068.pdf.

316. *See, e.g.*, Matt McKeon, *The Evolution of Privacy on Facebook*, MATTMCKEON.COM, http://www.mattmckeon.com/facebook-privacy/ (last visited Nov. 4, 2011) (providing a visual graph illustrating how privacy controls and defaults have changed on Facebook over the last 6 years).

growth of technology-focused media, increased attention from regulators and lawmakers, and additional resources for the privacy community—are giving rise to a larger social movement around online privacy. But for the privacy movement to truly be viable, it must reinforce these conditions. It must also neutralize the informational asymmetry, behavioral tendencies, and societal factors that make it difficult for individuals to understand the data ecosystem and why privacy issues matter, so they can be inspired to join together to engage in long-term battles and to create real change.

The privacy movement is not alone in confronting these challenges. The environmental movement has faced similar challenges and has already demonstrated success in overcoming them. In this respect, the environmental movement provides a promising example for a successful and sustainable online privacy social movement. In fact, the ACLU's "Demand Your dotRights" campaign has integrated some of the successful strategies of the environmental movement in order to address some of the specific challenges of building an effective online privacy movement, and has achieved some notable success. The privacy community must continue to build the infrastructure for a social movement and must use this infrastructure to strategically focus on tackling particular online privacy policy and legal issues that reinforce the five factors described above.

A. The Environmental Movement as a Model for the Privacy Movement

Like the environmental movement, the online privacy movement must become successful at taking threats that are often intangible, hidden, impersonal, and delayed and make them concrete, visible, personal, and immediate. The environmental movement has been successful in its ability to show people how daily activities like eating, drinking, and disposing of trash "are intimately and often problematically linked to each other, as well as with wider issues of the quality and sustainability of life on earth."[317] The privacy movement should be no less capable of reinforcing a coherent ecosystem frame. Such a frame would allow individuals to understand how their daily interaction with the digital world is part of a larger "data ecosystem" and how failing to address online privacy issues has deeper personal and societal implications. The privacy movement can also utilize existing environmental metaphors. Computer security expert Bruce Schneier commented in 2006 that the "tidal wave of data is the pollution problem of the information age."[318] Privacy author Cory Doctorow added to this sentiment in 2008, writing that "[p]ersonal data is as hot as nuclear waste . . . it is dangerous, long-lasting and once it has leaked there's no getting it back."[319]

317. *See* Clement & Hurrell, *supra* note 2, at 4.

318. Bruce Schneier, *Data as Pollution*, SCHNEIER ON SECURITY (Jan. 30, 2008), http://www.schneier.com/blog/archives/2008/01/data_as_polluti.html.

319. Cory Doctorow, *Personal Data is as Hot as Nuclear Waste*, THE GUARDIAN (Jan. 15, 2007, 8:27 AM), http://www.guardian.co.uk/technology/2008/jan/15/data.security.

The privacy movement, like the environmental movement, must also recognize the risk of overwhelming an individual so that she doubts that change is possible. While reversing climate change is a complex and potentially impossible challenge to the average individual, the environmental movement has responded by promoting accessible action steps like recycling and composting or reducing carbon emissions and buying products from recycled materials. These opportunities make it possible for individuals to focus on daily actions that keep them personally connected to broader efforts to address environmental concerns. For the privacy social movement to grow, it must also find ways to engage a broader base by nurturing a positive feedback mechanism with practical, possible, and proactive action strategies related to a person's daily life. By promoting smaller-scale, individual actions that create tangible change for a particular person, advocates can reinforce the mindset that change is possible and strengthen that person's affinity toward the privacy movement.

The privacy movement must also develop and maintain an overarching frame to encourage collaborative activities and educate the public, policymakers, and businesses about how and why change must happen. The environmental movement has been successful in addressing this challenge by creating a base of individuals and companies that identify with each other by defining themselves as "environmentalist" or "green" and in creating a common frame and symbols that connect environmental issues. The privacy movement has had difficulty developing a unifying frame, term or symbol to connect people who are concerned and motivate them to take action to protect their privacy or companies that are privacy-protective.

B. Addressing Specific Challenges of a Privacy Movement: Demand Your dotRights

In 2009, ACLU-NC launched the Demand Your dotRights campaign. ACLU-NC developed Demand Your dotRights as a response to some of the challenges facing the online privacy movement, and the campaign was designed to integrate some of the successful strategies of the environmental movement. The goal of the campaign is to "connect the dots" so that the public and policymakers understand how their individual actions affect the interconnected issues in the data ecosystem. The Demand Your dotRights campaign has utilized three primary strategies.

First, Demand Your dotRights has engaged people about online privacy by making the issues personal, tangible, and accessible by illustrating—not just in words, but also through imagery, videos, and interactive technology tools like the Facebook Quiz about Facebook Quizzes—how what individuals do online every day leaves behind "digital footprints" (in the form of status updates, friends lists, emails, location information and more) that move through this ecosystem and how pieces of their own personal information can often end up

being used in ways that individuals did not intend or envision.[320]

Second, the campaign has identified and promoted accessible ways for individuals to become involved in pushing for change by taking action and demanding greater transparency and control over their own personal information and how it is collected, used, and disclosed. These opportunities include directly sending emails to Google demanding greater protections for reader privacy, signing petitions for Facebook to reinstate privacy settings for fan pages and friends lists and fix the app gap, or sending emails to lawmakers to update federal and state privacy laws.[321]

Third, the campaign has reinforced and explained how particular online privacy issues are interconnected with broader issues of personal privacy. Demand Your dotRights has encouraged individuals to do more than take action on a particular issue, but to "join the movement" and become part of the larger, long-term campaign aimed at creating enduring protections for the entire ecosystem of online privacy

The title of the campaign, "Demand Your dotRights," and the symbol of a fist were purposely selected to establish a term and symbol that communicated to the public, policymakers, and businesses a clear focus related to online privacy—and one that was also broad enough to connect and unify diverse issues and evoke imagery of more established social movements. Bright yellow was utilized as the primary color of the campaign—rather than dark colors traditionally used for surveillance campaigns or the blue color more commonly used for ACLU materials—to communicate that this was a very different campaign, one intended to bring together new constituencies and to take advantage of bright opportunities to work together collectively to move both online privacy and technology forward in the digital age.

Physical and environmental metaphors have also been employed in the campaign to reinforce the "data ecosystem" frame both visually and verbally, and to make the connection between social movements related to the physical and online world. Analogies between physical locations and online services, such as search engines and libraries or cloud computing services and storage centers, are depicted in campaign materials. Personal information collected by online services is characterized as "digital footprints left behind" in campaign materials and personal data is shown raining down and building up a "data mountain" in the campaign's educational video.[322]

In its first three years, the Demand Your dotRights campaign has had notable success in attracting diverse constituencies to learn more about the data

320. *See Education,* ACLU OF N. CAL. DOTRIGHTS, http://dotRights.org/education (last visited Nov. 4, 2011).

321. *See Take Action,* ACLU OF N. CAL. DOTRIGHTS, http://dotRights.org/take-action (last visited Nov. 4, 2011).

322. *See dotRights Home,* ACLU OF N. CAL. DOTRIGHTS, http://dotRights.org (last visited Nov. 4, 2011); *Education, supra* note 320.

ecosystem, and bringing those constituencies together to address issues of online privacy collectively and demand change.

Over 260,000 people have utilized campaign resources to learn more about online privacy and demand both increased transparency and user control from companies and updates to state and federal privacy laws.[323] More than 80,000 people have visited privacy resource pages and interactive educational tools and videos about everything from social networking to cloud computing to mobile services.[324] More than 180,000 people have utilized the Facebook Quiz to learn more about how their own personal information is shared with third party applications on Facebook and how to better protect their personal information on social networks.[325] More than 8,000 members of the public—including students, seniors, businesspeople, and community activists—have attended dotRights presentations and events about online privacy. Tens of thousands of people have already "joined the movement" by signing up to receive dotRights action alerts, "liking" the campaign on Facebook, and following it on Twitter.[326]

The actions of individuals who demanded their "dotRights" in the past three years helped support corporate and legislative change, putting significant pressure on Facebook to begin to address privacy issues with third party apps,[327] and helping to pass the first digital book privacy law in the nation, California's Reader Privacy Act of 2011.[328]

But what is next? How will the privacy community build on existing success in recent years and continue to support the growth of a viable social movement? Beth Givens, the Executive Director of the Privacy Rights Clearinghouse, commented in 2007 that she would "like to see an ACLU of informational privacy—a large membership group that has hundreds of thousands, if not millions of members who pay dues and get newsletters and alerts."[329] While such a large membership organization committed solely to information privacy does not exist, "Protecting Civil Liberties in the Digital Age" became one of the four organizational priorities of the National ACLU in 2011, and the Demand Your dotRights campaign is being expanded to serve as one of the primary vehicles to further this priority. Hopefully, the continued expansion of online privacy work by the ACLU, along with other current campaigns and coalitions that other organizations have developed in recent years, will be able to reinforce the infrastructure and resources needed to sustain collective action and to help

323. Statistics from page views at www.dotrights.org. On file with author.

324. *Id.*

325. Statistics from ACLU Facebook about Facebook Quizzes usage data page. On file with author.

326. *Take Action*, *supra* note 321; *dotRights Campaign*, TWITTER, http://twitter.com/#!/dotrights (last visited Apr. 2, 2012); *Demand Your dotRights Campaign*, FACEBOOK, www.facebook.com/dotrights (last visited Apr. 3, 2012).

327. *See infra* Part IV.B.

328. *See infra* Part III.D.5.

329. BENNETT, *supra* note 2, at 218.

further build a movement that has percolated for so long.

But, while resources and infrastructure are necessary for a social movement, building the infrastructure does not mean that people will necessarily come. For online privacy advocacy to mature into a viable social movement, the privacy community must think strategically about how best to focus available resources and existing infrastructure. The privacy community must focus on particular policy and legal issues that reinforce the five factors described above, which are helping to overcome obstacles of informational asymmetry, common behavioral tendencies, and societal pressure. The question is, "How?" My experiences since 2004 as the Technology and Civil Liberties Policy Director at ACLU-NC and in developing and managing the organization's Demand Your dotRights campaign since 2008, have informed a few suggestions.

C. Next Steps: Focus on Integrated Strategies To Increase Transparency, Support the Five Factors, and Address Obstacles to Online Privacy Social Movement Building

To build a viable online privacy social movement, the privacy community should focus on using a combination of integrated policy, lobbying, litigation, public education, and communications strategies to push companies to provide effective mechanisms by which individual users can access and control their own information. In particular, the privacy community should work to ensure that individuals have transparency about the flow of their information: how it is collected, retained, used, and disclosed to the government or other third parties. Efforts to increase data transparency about the flow of an individual's own information have been percolating for some time, and there are already some mechanisms in place. But more must be done to build on the existing framework.

1. Moving Beyond the Privacy Policy: Why It's Important

While privacy policies remain an important basic transparency tool and should certainly be improved, if the privacy social movement is going to continue to grow and build, the privacy community should focus on instituting mechanisms that allow an individual to know the flow of her own information. Even the best privacy policy provides only general information about a company's data practices. Instituting better mechanisms so that an individual knows the flow of her own personal information would reinforce the five factors by: (1) continuing to make privacy issues personal and common to a growing segment of consumers; (2) making corporate privacy practices more visible and building market pressure for company privacy change; (3) providing compelling stories for continued technology and mainstream press coverage; (4) illustrating tangible online privacy harms for regulatory, legislative, and court actions; and (5) creating momentum to interest foundations and individual donors in providing sustaining resources for the privacy community's work in this area. Knowing the flow of one's own information would also counteract information

asymmetries, behavioral tendencies, and societal pressures. Such knowledge would help consumers better understand how online privacy issues affect their daily lives, comprehend the information "costs" related to particular services and not be as likely to overvalue benefit and underestimate risk with "free" online services, and be less susceptible to the "nothing to hide" argument by understanding how information that they consider personal can wind up in the hands of others.

The case studies discussed in this article provide strong examples of how making the issue "personal" and "tangible" can advance efforts to educate users about the data ecosystem and drive change on privacy issues. While Facebook and Apple disclosed general statements about data practices in their privacy policies, and organizations and scientists had already noted the associated problems, it was only when individuals understood how their own social networking information was being shared with third party apps, or saw how their own location data was being collected by Apple through the iPhone tool, that privacy issues became personal and tangible. Consumers reacted; the press, legislators, and regulators took notice; and companies were forced to institute more privacy-protective practices.

2. Strengthen and Expand Mechanisms that Exist

Some legal mechanisms already provide opportunities for consumers to understand how their own information is collected, retained, used, or disclosed. These legal mechanisms include the European Union Data Protection Initiative and state data breach or use transparency laws in the United States. These mechanisms must be expanded and strengthened.

The European Union Data Protection Directive, passed in 1995,[330] provides the mechanism for the most substantial transparency rights to date. It goes beyond requiring generic notice to individuals about how information may be collected, used, and disclosed, and provides rights for Europeans to access their data. Max Schrems, an Austrian law student, has used this European access right to shed light on Facebook's data collection practices. Utilizing this European law and a little-known Facebook online interface for requesting data access under this law, Schrems requested his data file and received over 1,200 pages of data collected about him by Facebook since 2008, detailing a wide array of his personal information, from everyone he had ever friended or defriended, every Facebook event he had ever attended or been invited to, and all of his past messages and chats, including those he had "deleted."[331]

330. 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, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

331. Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012, 10:03 AM), http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-

These revelations about Facebook data collection spurred widespread media attention, questions from Congress, and a privacy probe by European privacy regulators,[332] and mobilized tens of thousands of individuals, including Americans (who are not covered under this law),[333] to take action to try to access their own data files.[334] As a result, Facebook was forced to make several privacy improvements for European consumers. These improvements included a more efficient transparency tool that provides a quick overview of data being maintained, as well as a new policy that limits data retention on most user activities to less than a year and deletes queries typed into Facebook's search field within six months, in compliance with European law.[335] European leaders are currently debating a proposal submitted on January 25, 2012 to update the Privacy Directive and further strengthen user transparency, data access, and other privacy rights.[336]

Discussion about transparency and access rights is also a topic of the FTC's report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*.[337] The report states as a "baseline principle" that "[c]ompanies should increase the transparency of their data practices" by providing clear privacy notices, providing reasonable access to the consumer data they maintain, and expanding efforts to educate consumers about commercial data privacy practices.[338] While the final report falls short of endorsing a consumer's individualized right to access and correct data used solely for marketing purposes, the FTC supports the idea that companies should provide individuals with access to the list of categories of data they hold and to provide more individualized access "when feasible."[339] The new Consumer Privacy Bill of Rights released by the White House also promotes both transparency and access rights for consumers.[340]

The privacy community should build off of existing momentum related to access rights in the European Union and the United States to advocate for individualized access and to ensure transparency for consumers about the

---

facebooks-side/.

332. *Id.*

333. Miranda Miller, *Your Facebook Data File: Everything You Never Wanted Anyone to Know*, SEARCH ENGINE WATCH (Oct. 3, 2011), http://searchenginewatch.com/article/2114059/Your-Facebook-Data-File-Everything-You-Never-Wanted-Anyone-to-Know.

334. Kevin J. O'Brien, *Austrian Law Student Faces Down Facebook*, N.Y. TIMES (Feb. 5, 2012), http://www.nytimes.com/2012/02/06/technology/06iht-rawdata06.html?pagewanted=all.

335. *Id.*

336. Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authority for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, 2012/0010 (COD), *available at* http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf.

337. RAPID CHANGE, *supra* note 44.

338. *Id.* at viii.

339. *Id.* at 65–66.

340. WHITE HOUSE, *supra* note 180.

personal information collected. Knowing how their own personal information has been collected and retained will help activists to educate others about the data ecosystem, to make the issues personal and tangible, and to further support the growth of a social movement to support real and lasting change.

The privacy community should also focus on providing consumers with the opportunity to learn how their information is being used and shared, including with the government. There are some current laws that should be expanded and strengthened in support of these goals. California's Shine the Light Law, for instance, which went into effect on January 1, 2005, is one of the few statutory mechanisms allowing consumers in the United States to learn how businesses disclose consumers' personal information to third parties.[341] Pursuant to the law, companies that do business with California residents must respond to an individual's request and detail how her personal information has been shared with a third party for direct marketing purposes, or must inform her about how she can opt out of the company's information sharing practices.[342] Early studies found that the passage of the law influenced companies to change their data practices by limiting their third-party personal information sharing, creating new due diligence procedures related to third-party sharing, and considering policies not to share with third parties.[343] However, the rise of targeted advertising and app platforms have altered the data-sharing ecosystem substantially since the law went into effect, rendering its focus on direct marketing less relevant. The time is now to revisit and revise this landmark California law, and to potentially utilize the revised law as a model for other state and federal transparency legislation.

California has also been a model for instituting mechanisms to provide transparency about how consumer data has been shared inadvertently through security breaches. California instituted the first security breach notification law in the nation in 2003, requiring any person or entity conducting business in California to notify California residents whose unencrypted "personal information" was (or is reasonably believed to have been) acquired by an unauthorized person through a security breach.[344] Since the passage of California's law, the majority of states have enacted similar security breach notification laws[345] and many companies have strengthened their privacy practices to try to avoid the firestorm of negative attention caused by publicly

341. CAL. CIV. CODE § 1798.83 (West 2005).

342. *Id.* at § 1798.83(a) (disclosure requirements); § 1798.83(c)(2) (opt-out provision).

343. Lauren Thomas & Chris Jay Hoofnagle, *Exploring Information Sharing through California's 'Shine the Light' Law* 3–4 (Working Paper, Aug. 2009), *available at* http://ssrn.com/abstract=1448365 (citing Larry Ponemon, *Shining the Light on Our Personal Information*, DARWIN (Sept. 1, 2004), *available at* http://web.archive.org/web/20041118164240/http://www.darwinmag.com/read/feature/column.html?ArticleID=1158).

344. CAL. CIV. CODE § 1798.82 (West 2005).

345. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have security breach notification laws. *State Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (FEB. 6, 2012), http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

known data breaches.

California updated its security breach notification law in 2012, making the information provided to consumers about security breaches more user-friendly and specific. The updated law requires the notice to be written in plain language and to include a description of the breach, details about the types of personal information subject to the breach, when the breach occurred, and whether notification was delayed due to law enforcement investigation.[346] This increased transparency about security breaches promises to reinforce the public's understanding of the data ecosystem and to push companies to take more privacy-protective steps. It should also be utilized as a model for greater expansion and strengthening of information about security breaches.

3. Reporting Requirements as a Transparency Tool

Finally, the privacy community also should focus on providing greater transparency to individuals about how their personal information is disclosed by an online company to the government or third parties. Privacy advocates should push for general reporting requirements and for notice to individuals when data is being sought in new laws, and should urge companies to provide greater transparency whenever legally possible.

Currently, the public has very little understanding about how often companies disclose their personal information—such as email, text messages, or location data—to the government and to other third parties. Outdated privacy laws do not require this reporting and few companies voluntarily disclose this data. The federal Wiretap Act, originally passed in 1968,[347] requires an annual Wiretap Report to be compiled by the Administrative Office of the Courts and submitted to Congress that details the nature and number of federal and state orders authorizing or approving interceptions of wire, oral or electronic communications.[348] However, there is no reporting requirement corollary in the portion of the federal Electronic Communications Privacy Act ("ECPA") that creates standards for government demands for communications stored with a company.[349] The few transparency reports made available by companies like Google are limited in their scope.[350] The ACLU is promoting an update to

346. S. 24, 2011–12 Leg., Reg. Sess. (Cal. 2011), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110831_chaptered.html.

347. Wiretap Act, 18 U.S.C. §§ 2510–22 (2006).

348. 18 U.S.C. § 2519 (2006). DIR., ADMIN. OFFICE OF THE U.S. COURTS, APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS (2011), *available at* http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2010/2010WireTapReport.pdf.

349. Stored Communications Act, 18 U.S.C. §§ 2701–12 (2006) (part of the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (codified as amended in scattered section of 18 U.S.C.) that covers electronically stored information).

350. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/ (last visited Apr. 2, 2012). Currently the report primarily covers requests in criminal matters. *Content Removal*

ECPA that would include a reporting requirement[351] and utilizing the Freedom of Information Act and state public records act laws to increase transparency about government demands for digital information.[352] Updating current privacy laws to require reporting is an important step toward providing necessary transparency to policymakers and the public.

The California Reader Privacy Act, which has some of the most robust privacy reporting and notice requirements recently passed in law, can also function as a model for how to utilize sector-specific privacy laws to increase transparency and notice to individuals about overall data flow.[353] The ACLU and EFF have also been advocating for companies to take steps to increase transparency regarding government demands for information, such as by publishing transparency reports, by making their law enforcement guidelines publicly available, and providing notice to users about demands whenever legally possible.[354] Putting even greater attention and effort into instituting reporting and notice requirements that will help consumers and policymakers understand just how much personal data is flowing to third parties, including the government, is important for efforts to create better privacy protections.

VI.
CONCLUSION

Unlike modern software, privacy practices and laws do not auto-update. There must be sustained public pressure to support real change. Since 2009, the privacy community has been able to leverage factors to start to build a viable social movement to push for legal and policy change. The next several years will be significant in determining whether a privacy social movement is able to grow and mature like the environmental movement by utilizing recent successes and current attention to put down roots, mobilize broad public support, and achieve major reforms. It is my hope that, by reflecting on recent successes related to online privacy, identifying factors that have contributed to these advances, and

---

Requests FAQ, GOOGLE, http://www.google.com/transparencyreport/faq/#governmentrequestsfaq (last visited Apr. 2, 2012).

351. *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited Apr. 3, 2012).

352. *Cell Phone Location Tracking Public Records Request*, ACLU (Apr. 4, 2012), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request.

353. S. 602, 2011–12 Leg., Reg. Sess. (Cal. 2011), *available at* http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0601-0650/sb_602_bill_20111002_chaptered.html.

354. *Hey! Do You Use the Internet?*, ACLU, https://secure.aclu.org/ site/ SPageServer?pagename=110419_Internet_Privacy (last visited Apr. 25, 2012); *When the Government Comes Knocking, Who Has Your Back?*, EFF.ORG, https://whohasyourback.eff.org/ (last visited Apr. 3, 2012); *Demand Your dotRights: Digital Transparency Now!*, ACLU OF N. CAL. DOTRIGHTS, https://secure.aclu.org/site/SPageServer?pagename=CN_petition_demand_transparency (last visited Apr. 1, 2012).

suggesting a focus for privacy work that can reinforce these factors and break down remaining obstacles, this article contributes to the discussion of why and how the privacy community should build and sustain a viable social movement. If the privacy community can continue building the necessary infrastructure and taking the strategic policy steps necessary to increase transparency about how an individual's own information flows through the data ecosystem, it will be possible to sustain a large-scale social movement to ensure that, as technology advances, privacy protections are safeguarded in the modern digital world.