Written Testimony of James Grimmelmann
Professor of Law, New York Law School

House Committee on the Judiciary
Subcommittee on Intellectual Property, Competition, and the Internet
New Technologies and Innovations in the Mobile and Online Space,
and the Implications for Public Policy
June 19, 2012

Mr. Chairman and Members of the Subcommittee:

Thank you for the invitation to testify today and to discuss with you these important issues of innovation, privacy, and consumer protection. My name is James Grimmelmann. I am a professor at New York Law School. My teaching and research focus on the Internet, intellectual property, and privacy law. Although I am happy to respond to the Subcommittee's questions about any of today's topics, my testimony will focus primarily on privacy.

The central goal for privacy policy online and on mobile devices must be ***empowered consumer choice***. Some people are comfortable sharing even the most personal details about their lives widely; others treasure being known well only by their close friends. Most of us fall somewhere in between, revealing some things about ourselves to some people some of the time. Good privacy technologies and good privacy laws enable people to choose whether, when, and how open they want to be about their lives. I would like to endorse three essential principles that I consider indispensable for making real consumer choice a reality.

- The first is ***usability***. A choice that consumers do not know about, cannot find, or cannot understand is no choice at all. Privacy interfaces must be clear and clearly disclosed.

- The second is is ***reliability***. A consumer who has expressed a choice is entitled to expect that it will be honored. This is true whether she has chosen to share or to keep private.

- And the third is ***innovation for privacy***. Users benefit from good tools to help them manage their privacy. Privacy policy should encourage the development of these technologies, and protect them from interference.

These principles are simple and broadly applicable. In my scholarship, I have discussed their application to a number of privacy challenges. Today, I will focus on three: personal information on social networks like Facebook, behavioral tracking of web and mobile users, and video rental records on the Internet.

Information-Sharing on Social Networks

Social networks are one of the great success stories of Internet innovation in the last decade. Many millions of Americans use these networks to share the daily joys and of their lives with family and friends, to connect with colleagues for professional projects, and to express their creative talents for appreciative worldwide audiences. In many cases, the value of these networks depends on controlled access: the ability of users to limit their communications to a particular audience. Everything from a private email with advice from a mother to her daughter in college to a collaborative spreadsheet shared among four co-workers to a confidential discussion group for recovering alcoholics requires sharing with some people but not others.

This is innovation for privacy in action. The proliferation of social networks demonstrates vividly the intense consumer desire for sharing mechanisms that fit their personal preferences. Technology companies need to be free to develop new controlled-access sharing models, and to explain their benefits to users.

Crucially, however, social networks must also satisfy usability and reliability in their privacy practices. Users who misunderstand how their information will be shared can be badly hurt if it leaks and is misused. Mishandled personal information can cause embarrassment and fear; stalkers and harassers revel in the revealing details they can discover from misconfigured social networks. People have lost jobs and been splashed across the tabloids because Facebook's privacy settings were too confusing to understand.[1]

It is important to recognize that in these cases the social networks themselves are rarely the direct privacy offenders. These are typically peer-to-peer privacy violations committed by one user against another: the reporter who takes unprotected personal photographs, the "friend" who forwards a message meant to be eyes-only. The social network provides the setting within which these privacy violations occur, but only in some cases does it bear responsibility for them.

One type of case in which social networks contribute to privacy harms involves usability problems, in the form of confusing privacy control interfaces. Facebook has had recurring trouble here, and the frequency with which it changes its interface contributes to the problem. A 2010 New York Times article documented more than 50 settings with 170 distinct privacy options in its controls.[2] Surveys consistently find that Facebook users'

---

[1] *See generally* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009), *available at* http://works.bepress.com/james_grimmelmann/20/.

[2] Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 12, 2010, at B8, *available at* http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html.

privacy settings are different than what the users think they are.[3] That is, users are sharing with more people than they wish to, without understanding that they are. In an earlier version of the interface, for example, listing yourself as being located in "New York" would make your posts and photographs were visible to the millions of other Facebook users in New York.[4]

An even more troubling problem concerns what I call privacy "lurches": sudden and unexpected shifts in a social network's information-sharing practices. Lurches threaten the reliability of users' choices about privacy. A particularly egregious example was Google's 2010 rollout of its Buzz social network. Here is how I described the problem in an article:

> Buzz users post items such as photos, videos, random thoughts, and hyperlinks in order to share them with others. These items can then be viewed and commented on by other Buzz users. What differentiates Buzz from a blog is its tight integration with e-mail. Gmail users can receive Buzz updates the same way they receive regular e-mails, and reply to them too, all within Gmail. Google also built social networking features into Buzz at a deep level: choosing other users whose updates you want to follow is as easy as clicking a checkbox to let Buzz import your list of most-e-mailed contacts from Gmail.
>
> It was this last design decision that caused the privacy trouble. Google also required Buzz users to set up public profile pages that listed their Buzz contacts. Turning on Buzz, therefore, automatically published a list of users' most-emailed Gmail contacts. In Nicholas Carlson's words, this step "made Google Buzz a danger zone for reporters, mental health professionals, cheating spouses and anyone else who didn't want to tell the world who they emailed or chatted with most." For a business lawyer conducting confidential negotiations or a criminal lawyer corresponding with witnesses, this kind of exposure could easily be a sanctionable violation of client confidences. . . .
>
> As a political analyst put it, "If I were working for the Iranian or the Chinese government, I would immediately dispatch my Internet geek squads to check on Google Buzz accounts for political activists and see if

---

[3] *See, e.g.* Michelle Madejski, Maritza Johnson, & Steven M. Bellovin, *A Study of Privacy Setting Errors in an Online Social Network*, PROCEEDINGS OF THE 4TH INTERNATIONAL WORKSHOP ON SECURITY AND SOCIAL NETWORKING (2012), *available at* https://www.cs.columbia.edu/~smb/papers/fb-violations-sesoc.pdf; Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PRIVACY ENHANCING TECHNOLOGIES: 6TH INTERNATIONAL WORKSHOP, PET 2006, at 36 (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

[4] *See Facebook Members Bare All on Networks, Sophos Warns of New Privacy Concerns*, SOPHOS (Oct. 2, 2007), http://www.sophos.com/en-us/press-office/press-releases/2007/10/facebook-network.aspx.

they have any connections that were previously unknown to the government."[5]

The Buzz rollout was a privacy lurch, one that violated the principle of reliability. It took software with a clearly defined privacy model—Gmail—and used personal information in a sharply different and less private way that users could not have anticipated and that was capable of causing significant harm to them. The Federal Trade Commission investigated Google over this incident and reached a settlement that includes independent audits of Google's privacy practices.[6]

I have also argued that privacy lurches of this sort may potentially expose companies to legal liability for distributing an unreasonably dangerous product.[7] Just as the maker of a defective lawnmower whose blade injures a consumer's hand will be held accountable, so too should the maker of a defective social network whose sharing settings injure a consumer's privacy. Lawnmowers and social networks are both valuable products offering consumers important benefits, but it is important that they be designed with real-world safety in mind, and law must ensure that they are.

An important special case of information sharing is when the third party is the government. Information posted to social networks is becoming increasingly useful as evidence in criminal prosecutions. Police and prosecutors have used Facebook and MySpace posts to disprove alibis, to establish gang membership, to prove violations of parole, and even to demonstrate a defendant's attempt at witness tampering.[8] These are valuable uses, and the question is how to balance law enforcement's need for access with users' legitimate expectations of privacy.

Fortunately, the Fourth Amendment establishes an appropriate baseline. The Sixth Circuit's 2010 decision in *United States v. Warshak* established that users have a reasonable expectation of privacy in the contents of their emails stored with Internet service providers.[9] Some communications via social networks, such as Facebook private messages sent to a single user, are closely akin to email. Under *Warshak*, law enforcement is entitled to obtain the contents of these messages from social network providers only with a valid search warrant. This is the right result. It respects the traditional consensus in favor of communications privacy while preserving law enforcement's ability to obtain the messages on a showing of probable cause.

Other information posted through social media is not intended to be private in the same way. I have a Twitter account that I use to comment on legal issues. My communications are intended to be seen by anyone on the Internet who is interested.

---

[5] James Grimmelmann, *Privacy as Product Safety*, 26 WIDENER L.J. 793, 823–24 (2010), *available at* http://works.bepress.com/james_grimmelmann/27/.

[6] *See In re* Google Inc., No. C-4336, 2011 WL 5089551 (F.T.C. Oct. 13, 2011).

[7] *See* Grimmelmann, *supra* note 5.

[8] *See, e.g.*, Griffin v. State, 419 Md. 343 (2011).

[9] 631 U.S. 266 (6th Cir. 2010).

These are not private information, and I understand that by posting them I have voluntarily shared them with the world. But this fact does not make anything on Twitter fair game. Some users have "protected" accounts and make their communications visible only to a controlled list of other users; other users, myself included, send private "direct messages" that are only visible to the recipient. The courts are currently engaged in the process of sorting through users' expectations of privacy in different kinds of social network information. This is a valuable evolutionary process that should continue. It would be a mistake to attempt to legislate specific technological details in this era of rapid innovation.

One trend, however, is troubling. In the recent case of *People v. Harris*, a New York state court granted a prosecutor's subpoena for all of the user information associated with a Twitter account.[10] Part of the court's reasoning was that the defendant did not even have standing to challenge the subpoena because the defendant's content was "not his" under Twitter's user agreement. This was a misreading of the limited and nonexclusive copyright license in Twitter's user agreement, which left ownership of the posted content with Twitter's users. Worse, the court's opinion would set a dangerous precedent that information sent via online intermediaries would automatically become non-private information outside of the Fourth Amendment's protection simply because the terms of service give those intermediaries the ability to use and transfer that information as part of providing their services. Packages do not become public simply because they are handed to FedEx for delivery; neither should communications handed to online intermediaries for delivery.

Twitter's response to this decision was admirable. Not only did it intervene to assert the user's privacy rights in the information the court had mistakenly decided belonged to Twitter, it amended its Privacy Policy to state, "However, nothing in this Privacy Policy is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your information."[11] Congress should ensure that other online intermediaries are not placed in the same position by amending the Stored Communications Act so that the compelled disclosure of information not readily accessible to the general public requires a search warrant based on probable cause. This standard is technologically neutral and would provide clear and effective guidance for users, service providers, and law enforcement. It accords with common user expectations and makes the choice to depend on a social network's privacy protections both usable and reliable.

Browser Cookie Tracking of Users

Another good example of the principles in action is online behavioral advertising. Advertising companies place unique identifiers known as "cookies" on users' computers to track them from one session to another and from one website to another. The resulting

---

[10] __ N.Y.S.2d __, 2012 WL 1381238, 2012 N.Y. Slip Op. 22109 (N.Y.C. Crim. Ct. Apr. 20, 2012).
[11] *See Twitter Privacy Policy*, TWITTER (effective May 17, 2012), https://twitter.com/privacy.

profiles are used to target ads to consumers based on the websites they visit. Technology enthusiasts, for example, see ads for the latest gadget, rather than the latest tracksuit.

Some users appreciate receiving ads customized for them; others find the tracking creepy and offensive. Most reputable participants in the online advertising industry recognize this difference in opinions and offer users a choice of whether to be tracked or not. Unfortunately, these choices all too frequently fall short of the three essential principles of empowered consumer choice I have mentioned.

I am particularly concerned that some actors in the online advertising ecosystem are working to thwart the development of effective privacy-protecting technologies. A good example of one such technology is browser-based cookie blocking. All major web browsers offer users the ability to set a global policy on which kinds of cookies to accept under what circumstances. These user preference options have evolved from the confusing and blunt choices of the 1990s into thoughtful, well-balanced, and usable systems. In addition, third-party browser add-ons, such as Ghostery, provide users with easy-to-use tools for understanding cookies and automatically blocking unwanted ones.

These tools represent the best tradition of technological innovation. Companies compete to offer users more effective control over their online presence. The winners are the ones who offer the most usable products that best enable consumers to reveal what they want to reveal while keeping private what they want to keep private.

Too many advertising and technology companies treat these expressions of user preference as an inconvenient obstacle to be overcome, rather than genuine user choices deserving of respect. One form of this disdain for user preferences involved cookie variants with colorful names like "Flash cookies," "zombie cookies," "respawning cookies," and "supercookies." These terms describe a wide variety of technical practices with a common aim: ensuring that any deleted cookies are promptly replaced.

For example, imagine that Chris, a user concerned about his privacy who wished not to be tracked, followed the advice web users had been receiving for years, and deleted his cookie from the online television site Hulu.com. Unfortunately for Chris, this regular "HTTP" cookie was not the only cookie Hulu used. A program running on Hulu.com also set a "Flash" cookie on Chris's computer. When this program detected that Chris's HTTP cookie was gone, it used the Flash cookie to "respawn" the HTTP cookie. It was as though Chris had never taken action; Hulu completely thwarted his attempt to protect his privacy.

There is no good justification for this practice. Chris and other privacy-conscious users expressed their privacy preferences in their actions. A website that encounters a missing cookie should respect the user's likely desire for privacy, not surreptitiously attempt to thwart that desire. What Hulu did with respawning cookies violated all three principles of user empowerment. It made consumers' privacy choices less usable by making it harder for users to discover all the cookies they needed to remove to avoid being tracked. It made consumers' privacy choices less reliable by undermining the cookie

choices they did made. And it hurt innovation for privacy by circumventing the tools users employed to control cookies on their computers.

The use of respawning cookies became the subject both of Federal Trade Commission enforcement action[12] and of industry self-regulatory efforts.[13] Unfortunately, many companies have not accepted the basic lesson of the cookie wars: respecting users' choices. I will briefly describe three further examples in which this lesson has gone unheeded: Google's circumvention of the cookie blocker in Apple's Safari browser, numerous apps' circumvention of privacy-protecting policies on the iPhone, and recent controversy about Do Not Track defaults.

Google and Safari: Apple's Safari web browser has an important user-protective feature: by default, it blocks the "third-party" cookies that track users from one website to another. Apple advertises this feature as a benefit of Safari; some users specifically chose Safari because of it.[14] Safari still allows websites to set "first-party" cookies, which websites rely on for features like shopping carts and to keep users logged in. Google and three other advertising companies discovered a way to make third-party cookies look like first-party cookies to Safari—in essence by tricking Safari into thinking that the user had clicked on something she had not.[15] Google used the trick to combine its advertising network with its Google+ social network. It had the effect of undermining Safari's privacy promises about cookie-based tracking. Bloomberg News has reported that the Federal Trade Commission is investigating.[16]

iPhone User Information: The Apple iPhone's runaway success has been fueled by the more than 700,000 apps available to users. Many of these apps, however, are careless with user data. When users ran the social network app Path, for example, it accessed their entire address books, then transmitted everything in them to Path's servers, without using encryption to protect users from malicious hackers, and all without notice to the user.[17] This and other privacy-violating techniques were prohibited by Apple's rules for apps, but many developers came to a "quiet understanding" that they could get away with it.[18] I am

---

[12] *See In re* ScanScout, Inc., No. C-4344, 2011 WL 6800915 (F.T.C. Dec. 14, 2011).

[13] *See, e.g. FAQs*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/managing/faqs.asp (last visited June 15, 2012) (discussing NAI policy against use of Flash cookies).

[14] *See What Is Safari?*, APPLE, http://www.apple.com/safari/what-is.html (last visited June 15, 2012).

[15] *See* Julia Angwin & Jennifer Valentino-DeVries, *Google's iPhone Tracking*, WALL ST. J., Feb. 17, 2012, at A1, *available at* http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html; Jonathan Mayer, *Safari Trackers*, WEB POLICY, http://webpolicy.org/2012/02/17/safari-trackers/ (Feb. 17, 2012).

[16] *See* Sara Forden, *Google Said To Face Fine by U.S. over Apple Safari Breach*, BLOOMBERG NEWS (May 5, 2012), *available at* http://www.bloomberg.com/news/2012-05-04/google-said-to-face-fine-by-u-s-over-apple-safari-breach.html.

[17] *See* David Sarno, *Phone Apps Dial Up Privacy Worries*, L.A. TIMES, Feb. 16, 2012, at A1, *available at* http://articles.latimes.com/2012/feb/16/business/la-fi-app-privacy-20120216.

[18] Dustin Curtis, *Stealing Your Address Book*, DCURTIS, http://dcurt.is/stealing-your-address-book (Feb. 8, 2012).

concerned about a Silicon Valley culture in which behavior that is illegal, unethical, and expressly forbidden is nonetheless considered routine, and I support greater enforcement efforts against mobile app companies that consciously ignore the privacy rules of mobile app platforms.

Do Not Track Defaults: An open and participatory multi-stakeholder process is underway to define a "Do Not Track header": a flag that a user's web browser could set to indicate a request that the user's online activities not be tracked by the website that receives the request.[19] This is an important and valuable initiative, but it will only succeed if the Do Not Track request is usable and respected. Microsoft recently took a valuable step towards that goal by announcing that Do Not Track would be on by default in the next version of its Internet Explorer browser.[20] I consider this move an excellent example of innovation for privacy. Users benefit from being able to delegate the choice to enable Do Not Track to Internet Explorer; it simplifies the option of choosing this form of privacy. Microsoft will succeed in the competitive browser market if and only if users consider this a valuable feature. But some other participants in the Do Not Track process, including representatives from Yahoo! and Google, have been pressing for the ability to disregard the Do Not Track request if it comes from a browser, like Internet Explorer, in which it is on by default.[21] This attempt to sabotage the practical usability of Do Not Track would make it pointlessly harder for consumers to express their privacy preferences. Congress should legislate full compliance with Do Not Track—which means that websites may not second-guess properly expressed user requests.

Video Record Privacy

A final example of this framework in action is the Video Privacy Protection Act ("VPPA"), enacted in 1998 to ensure privacy in consumers' video rentals. It prohibits the disclosure of the videos rented or purchased by an individual without that person's consent.[22] In many respects, the VPPA is a model privacy statute. It gives consumers confidence that personally sensitive information will remain confidential. Its commands are backed up by forceful but reasonable penalties. Its requirements are specific and clear, so that companies know when it applies to them and when it does not, and know what they need to do to comply. For all of these reasons, the VPPA does an excellent job of ensuring reliability.

As an example, in 2007, when Facebook introduced its Beacon feature, users' actions on other websites, such as the recipes they clipped on Epicurious, were

---

[19] *See generally Tracking Protection Working Group Charter*, WORLD WIDE WEB CONSORTIUM, http://www.w3.org/2011/tracking-protection/charter.html (last visited June 15, 2012).

[20] *See* Brendon Lynch, *Advancing Consumer Trust and Privacy: Internet Explorer in Windows 8*, MICROSOFT ON THE ISSUES, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2012/05/31/advancing-consumer-trust-and-privacy-internet-explorer-in-windows-8.aspx (May 31, 2012).

[21] These views are detailed in the archives of the Tracking Protection Working Group's public mailing list at http://lists.w3.org/Archives/Public/public-tracking/.

[22] 18 U.S.C. § 2710.

automatically posted to Facebook.[23] This broke users' implicit privacy model of the Internet; it thwarted their expectation that what happens on Epicurious stays on Epicurious. The minimal notices Facebook provided were easy to miss, and it opted users into Beacon without their consent. I very much doubt that most of us would like the food we cook, the books we read, and the movies we watch to be automatically trumpeted to all our friends and acquaintances.

Most of the companies that partnered with Facebook in this privacy mistake escaped being held accountable for their actions due to the lack of clear general online privacy laws. The one exception was Blockbuster, and it faced up to its responsibility because the VPPA gives such unambiguous direction. A class-action lawsuit against Facebook and Blockbuster resulted in a $9.5 million settlement.[24]

Significantly, the VPPA provides consumers with genuine choice. While it sets a default of privacy, it specifically excepts any disclosure made "with the informed, written consent of the consumer given at the time the disclosure is sought."[25] If a video site would like to share with a user's friends the fact that she just watched and loved *Wall-E*, all it needs to do is ask. If a user would like to share this fact with her friends, all she needs to do is tell the site that it is okay to share. The VPPA understands that some users will choose to share, and others will choose not to.

In the last year, some critics have questioned the usability of this choice. The VPPA's requirement that consent must be given "at the time the disclosure is sought" means that users cannot give blanket, up-front permission for their video views to be shared. It does not matter how clearly Netflix explains this sharing to users, or how unambiguously they say that the sharing is okay, the VPPA still prohibits advance consent. I can share with my friends on Facebook the titles of all the songs I listen to on Spotify, but I cannot share the titles of all the movies I watch on Netflix. This is a usability issue: the VPPA does not offer a usable general choice in favor of sharing. H.R. 2471, which passed the House in December, would amend the VPPA to permit advance consent.

While I am sympathetic to H.R. 2471's goal of enabling genuinely symmetric consumer choice, I am concerned about how it achieves that goal. Consent given at the time of disclosure requires relatively straightforward notice. The provider can explain the specific disclosure it is about the make, and the consumer can understand the full scope of the disclosure. But consent given in advance requires more detailed notice in order for the consumer to give genuinely "informed" consent. If you ask for my consent to say on Facebook that I have just watched *Schindler's List*, I will understand that you are about to post a single, specific item to tell my friends on Facebook that I watched . . . *Schindler's List*. If you ask for my general consent up front, then I will need both to anticipate what kinds

---

[23] *See* Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1.
[24] *See* Lane v. Facebook, No. 5:08-CV-03845-RS (N.D. Cal. settlement approved Mar. 17, 2010).
[25] 18 U.S.C. § 2710(b)(2)(B).

of movies I might watch, and also what kinds of services you may share it with and how you will share it.

These uncertainties over what counts as "informed" advance consent will undermine the VPPA's admirable clarity. Consumers deserve specific guidance about the kinds of sharing that will take place if they click "yes." If the VPPA is to be amended to permit advance consent, it should require video providers to give that specific guidance, and state that advance consent is permissible only for identified classes of disclosures to specifically named partners.[26]

---

[26] For more on the VPPA and H.R. 2471, *see generally The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the Subcomm. on Privacy, Tech., and Law of the Senate Comm. on the Judiciary*, 112th Cong. (2012) (testimony of William McGeveran), *available at* http://www.judiciary.senate.gov/pdf/12-1-31McGeveranTestimony.pdf.