



**2ND EDITION**

**A PUBLICATION OF THE ACLU OF CALIFORNIA  
ONLINE AT [ACLUNG.ORG/BUSINESS/PRIMER](https://aclung.org/business/primer)**

In recent years, online privacy and free speech have become hot topics among users, legislators, regulators, and investors. Many companies have experienced firsthand how decisions about privacy and free speech can impact their business. Companies that have failed to take privacy and free speech into account have been hit with public relations nightmares, costly lawsuits, government investigations, and the loss of customers and business partners. Meanwhile, companies that have designed their products and business plans to protect users have not only avoided these harms but benefitted from positive PR and increased customer trust.

Building privacy and free speech protections into your service and company takes planning. This publication is intended to get you started. It walks you through basic questions you need to address in order to properly integrate privacy and free speech into your products and illustrates how doing so can help your company thrive.

### **What's new in this edition**

This second edition of *Privacy & Free Speech: It's Good for Business* includes updated recommendations for policies and practices, as well as dozens of new real-life case studies from A(mazon) to Z(ynga). Its purpose is to help your company spot potential privacy and free speech issues in products and business models. The tools in this publication will enable you to make the smart, proactive decisions necessary to avoid problems, protect customers, and boost your bottom line.

The online version of this primer ([aclunc.org/tech/primer](https://aclunc.org/tech/primer)) includes continuously-updated resources to help you identify and employ best practices for building privacy and free speech into your product. You can also contact us directly with questions or comments at [dotRights@aclunc.org](mailto:dotRights@aclunc.org).

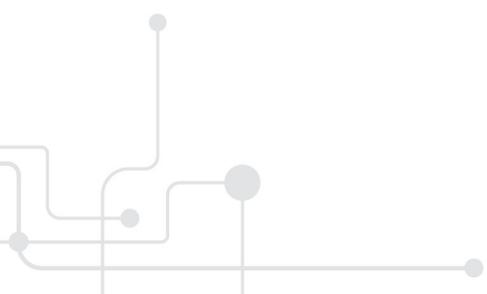
Companies will face many difficult decisions about users' privacy and free speech. Reading this primer and sharing it with your colleagues is a good start. We hope it will help you understand how building privacy and free speech protection into your products and business plans isn't just the right thing to do—it's good for your business, too.



Nicole A. Ozer  
Technology & Civil Liberties Policy Director  
ACLU of California



Chris Conley  
Technology & Civil Liberties Policy Attorney  
ACLU of Northern California



# CONTENTS

Promoting Privacy and Free Speech: A Roadmap . . . . .	1
Case Studies . . . . .	2
Protecting Privacy and Free Speech Is Good for Business . . . . .	3
Make Your Privacy Practices Stand Out . . . . .	4
• Respect Your Data: Limit and Protect the Data You Collect and Retain . . . . .	4
• Plan Ahead: Incorporate Privacy and Security from Start to Finish . . . . .	8
• Be Transparent: Give Users the Ability to Make Informed Choices . . . . .	11
• Partner with Your Users: Put Users in Control and Stand Up for Their Rights. . . . .	15
Give Your Users a Platform to Speak Freely. . . . .	20
• Encourage Users to Speak Freely: Establish Policies that Promote Speech in Every Form . . . . .	20
• Moderate Cautiously: Avoid Censoring or Removing Legitimate Speech . . . . .	23
• Promote Creativity: Let Customers Decide How to Use and Discuss Your Product . . . . .	25
• Speak Up for Free Speech: Take Action to Protect Your Users' Freedom of Expression . . . . .	28
Conclusion . . . . .	31
Appendix: Legal Landscape . . . . .	32
Endnotes . . . . .	37

**AUTHORS:** Nicole A. Ozer and Chris Conley,  
Technology and Civil Liberties Project, ACLU of Northern California

**CONTRIBUTING WRITERS, SECOND EDITION:**  
Cliff Helm, Tamar Gubins, Hari O'Connell, Alix McKenna

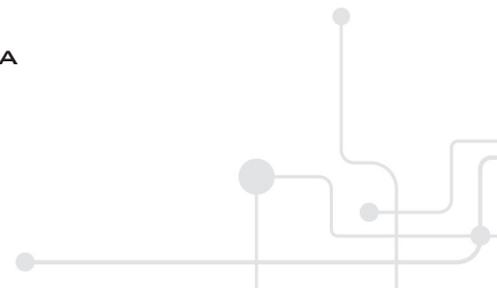
**CONTRIBUTING WRITERS, FIRST EDITION:**  
Christopher Soghoian, Aaron Brauer Rieke, Travis Brandon

**DESIGN:** Gigi Pandian

**PRINTING:** Inkworks Press

Special thanks to Policy Program Assistant Anna Salem and the many reviewers for their assistance.

**PUBLISHED BY THE ACLU OF CALIFORNIA  
SECOND EDITION, NOVEMBER 2012**



# PROMOTING PRIVACY AND FREE SPEECH: A ROADMAP

The following principles and questions provide a roadmap for your efforts to promote privacy and free speech. Each is discussed further in the following sections.

## MAKE YOUR PRIVACY PRACTICES STAND OUT

**RESPECT YOUR DATA:** LIMIT AND PROTECT THE DATA YOU COLLECT AND RETAIN

- Have you carefully evaluated the costs of collecting and retaining data?
- Do you properly handle any sensitive data that you do collect?
- Do you collect and store data securely?

**PLAN AHEAD:** INCORPORATE PRIVACY AND SECURITY FROM START TO FINISH

- Do you have a comprehensive privacy and security plan?
- Do you continue to evaluate your privacy and security practices as your products and company change and grow?
- Do you have a plan to notify and protect users if a breach occurs?

**BE TRANSPARENT:** GIVE USERS THE ABILITY TO MAKE INFORMED CHOICES

- Do you clearly communicate your privacy practices to your users?
- Can your users learn what data you hold about them and how it is used and shared?
- Do you clearly inform your users when you are collecting data about them?
- Do you clearly communicate product changes to your users?

**PARTNER WITH YOUR USERS:** PUT USERS IN CONTROL AND STAND UP FOR THEIR RIGHTS

- Do you give users control over their personal information?
- Do you identify and respect consumer expectations?
- Do you stand up for your users' privacy?

## GIVE YOUR USERS A PLATFORM TO SPEAK FREELY

**ENCOURAGE USERS TO SPEAK FREELY:** ESTABLISH POLICIES THAT PROMOTE SPEECH IN EVERY FORM

- Do you encourage users to express themselves as they choose?
- Do you give users control over the content they access and the tools they use?
- Do you let users speak for themselves?
- Do you encourage your users to speak without fear of being monitored?

**MODERATE CAUTIOUSLY:** AVOID CENSORING OR LIMITING LEGITIMATE SPEECH

- Do your policies protect your users and your company without deterring legitimate speech?
- Do you consistently apply your policies?

**PROMOTE CREATIVITY:** LET CUSTOMERS DECIDE HOW TO USE AND DISCUSS YOUR PRODUCT

- Have you considered the benefits of encouraging the unrestricted use and distribution of your content or product?
- Do you respect free speech if you do assert control?
- Have you considered the costs and risks of legally asserting control over your content or product?
- Have you carefully considered the implications of placing technological limits on your users?

**SPEAK UP FOR FREE SPEECH:** PROTECT YOUR USERS' FREEDOM OF EXPRESSION

- Do you support your users when you receive demands to take down their content?
- Do you protect the identities of anonymous and pseudonymous users?
- Do you advocate for laws that protect your users' freedom of expression?

# CASE STUDIES

The case studies listed here can help you follow the example of companies that have benefited from making privacy- and speech-friendly decisions—and avoid repeating the mistakes that have landed other companies in hot water.

Google Slammed for “Wardriving by Design”

Path “Discovered Phoning Home with Your Address Book”

Apple Products Record Location History

Broken Thumbs Fined for Collecting Children’s Information

AOL Releases Not-So-Anonymous Data

Blippy Users Share More than Expected

LinkedIn Criticized in Aftermath of Breach

Facebook’s Master Account

Citibank Hacked Using “Remarkably Simple Technique”

Microsoft Builds Security into Design

Cisco Tries to Silence Security Researcher

ChoicePoint Suffers for Failing to Protect Consumers

Sony’s “Half-Baked Response” to Security Breach

DuckDuckGo Keeps Privacy Simple

Zynga Makes Privacy a Game

App Platforms, California AG Reach Privacy Agreement

Myspace Fined, Sued for Deceptive Privacy Practices

Google Publishes Transparency Report

CarrierIQ Accused of Planting Spyware on Smartphones

NebuAd’s Plan to Monitor Internet Use Triggers Outrage

In-Car Assistance Systems Caught Spying on Drivers

Etsy Suffers Privacy “DIY-saster”

Facebook Backtracks on Privacy Changes

Apple’s Update Mechanism “Borders on Malware”

Google Creates “Data Liberation Front”

ScanScout Offers Opt-Out, Then Prevents It

Google Faces Record Fines for Bypassing Privacy Settings

Netflix Sued for Retaining Records About Former Customers

Facebook Makes It Hard to Leave

Fitbit Deals with Fireworks After Exposing “Sex Stats”

i-Free Forced to Pull App “Geared Toward Stalkers”

Google Buzz Exposes Private Contact Details

Yahoo! Successfully Fights Warrantless Demand

Amazon Sues to Protect Users

AT&T, Verizon Accused of Eavesdropping on Users

Qwest Resists Surveillance Efforts

Twitter’s “Remarkable Display of Backbone”

Google Fights Demand for Millions of Search Records

YouTube Wins Battle to Anonymize Data

Google Protects Readers of Digital Books

Facebook Called Out for Rejecting Drug Policy Reform Ads

Google+, Minus Anonymity

Apple Comes Under Fire when Siri Won’t Provide Reproductive Health Content

AT&T Faces the Music for Censoring Pearl Jam

AT&T Accused of “Holding FaceTime Hostage”

Verizon Pledges Not to Monitor Users

Socialcam Slammed for “Bullying” Users

Tagged Named “World’s Most Annoying Website” for Deceptive Emails

PayPal Flops as Moral Police

BART Sparks Controversy by Blocking Cell Service

Twitter Rethinks Its Code of Conduct

Facebook Faces “Nurse-In” over Breastfeeding Photo Policies

Twitter Bans Olympic Journalist for Heckling

Fan Mod Pushes 3-Year-Old Video Game up the Charts

Apple “Bites the Fans that Feed It”

Viacom Demands Removal of Political Videos

Bank Julius Baer Turns “Secret” Documents into Public Spectacle

Google Forced to Repay Purchasers of Unusable Content

Amazon’s Orwellian Mistake

Yahoo! Turns Over Dissident Identities to China

Verizon Resists Demand for User Information

Twitter Stands Up for Political Critics

Facebook “Likes” Free Speech

Google Slammed for Its “Betrayal” of Net Neutrality

Internet “Blackout” Helps Stop Anti-Piracy Bills

Go Daddy’s Political Position Leads to Boycott

# PROTECTING PRIVACY AND FREE SPEECH IS GOOD FOR BUSINESS

A “primer” is a “book of elementary principles.”<sup>1</sup> The document you are now reading is intended to be exactly that—a guide to the basic steps of building privacy and free speech into your current or future products.

But you may be asking a more fundamental question: why should I invest my company’s precious time and resources on protecting my users’ rights rather than focus on the bottom line?

The short answer is simple: because, in the long run, what’s good for your users is good for your company. Your users are your greatest asset, whether you are selling products, advertising, or data. Meeting and even exceeding your users’ privacy and free speech expectations can build trust and deepen their relationship with your company and products, while falling short can drive users away and threaten the viability of your enterprise.

Proactively identifying and addressing potential issues can allow you to avoid public relations fiascos and fines or lawsuits that could devastate your business before it can take off. For example, **Google’s** Buzz was described as a “privacy nightmare”<sup>2</sup> that led to an FTC privacy complaint<sup>3</sup> and a class action lawsuit<sup>4</sup> before the entire product was cancelled.<sup>5</sup> **Netflix** was recently forced to change its privacy policy and pay \$9 million to settle a class action lawsuit accusing it of illegally retaining records about former customers.<sup>6</sup> **Apple** was charged with “biting the fans that feed it” and saddled with legal fees after a failed attempt to clamp down on blog posts about rumored upcoming products.<sup>7</sup> And **AT&T** and **Verizon** have both been sued for hundreds of billions of dollars in multiple class action lawsuits and have spent massive amounts on attorney and lobbyist fees after reportedly collaborating with the National Security Agency’s warrantless wiretapping and data-mining program.<sup>8</sup>

Free speech and privacy missteps can also directly affect your company’s revenue. **NebuAd’s** plan to meticulously track online activity and use this information for targeted advertising went awry when consumers expressed their outrage and the company lost several major business partners.<sup>9</sup> **GoDaddy’s** support of the controversial Stop Online Piracy Act led to the loss of 37,000 domain customers that had previously used the company’s hosting services.<sup>10</sup> And **Facebook** lost major advertising partners for its Beacon service after failing to provide proper notice and consent to users about the service.<sup>11</sup>

On the other hand, a demonstrated commitment to privacy and free speech can draw positive attention from the press and the public that helps you attract and retain new users. **Twitter** has been repeatedly lauded for its determination to “protect our users from government” by exposing and resisting demands for censorship or information in the U.S. and abroad.<sup>12</sup> And when **Qwest** refused to join its fellow telephone companies in disclosing customer information to the National Security Agency, the *New York Times* stated: “Companies can’t buy that kind of buzz.”<sup>13</sup>

Privacy and free speech protections can have more direct economic benefits as well, encouraging users to increase their interaction with your product and attracting investors to your company. When **Facebook** changed its privacy tools to allow greater user control, the click-through rates for on-site advertising actually increased.<sup>15</sup> Investors may also take note of whether privacy and speech protections are part of your business plan in order to “save everyone—entrepreneurs and VCs alike—from future headaches.”<sup>16</sup>

Your company will face many privacy and free speech decisions in the days and years ahead. We hope that reading this primer now and utilizing its resources as you develop your next product or business venture will help you to avoid having millions read about your privacy or free speech mistakes later.

RESEARCH  
CONDUCTED  
IN 2011  
DEMONSTRATED  
OVER A 60 PERCENT  
CORRELATION  
BETWEEN HOW MUCH  
CONSUMERS TRUST  
A BRAND AND HOW  
MUCH THEY ARE  
WILLING TO PAY FOR  
A SERVICE COMING  
FROM THAT BRAND.<sup>14</sup>

# MAKE YOUR PRIVACY PRACTICES STAND OUT

The key to developing outstanding privacy practices is to proactively identify and address potential privacy risks before they happen. This requires a commitment to building privacy into your products from the beginning and to partnering with your users by giving them the information and tools to protect and control their own personal information. By doing so, you can not only avoid consequences ranging from scathing media coverage to class action lawsuits, you can make users feel truly invested in your product and build invaluable trust and loyalty.

For additional resources about the concept of privacy by design and existing tools to help you build privacy into your current and future projects, please visit the online version of this primer at [aclunc.org/tech/primer](http://aclunc.org/tech/primer).

## RESPECT YOUR DATA: LIMIT AND PROTECT THE DATA YOU COLLECT AND RETAIN

Protecting your users' privacy requires you to be thoughtful about the data you hold about them. By carefully considering the costs and benefits of collecting data and by properly safeguarding the information that you do collect, you may prevent privacy harms and increase consumer trust in your product.

### ➔ HAVE YOU CAREFULLY EVALUATED THE COSTS OF COLLECTING AND RETAINING DATA?

#### EVALUATE THE COSTS OF COLLECTING MORE DATA THAN YOUR PRODUCT NEEDS.

Being known as a repository for large amounts of user data can make you the target of technological attacks and legal demands alike. Google received more than 18,000 government requests or demands for user data between July and December 2011.<sup>18</sup> In addition, collecting information that isn't necessary for your service can surprise users, leading to mistrust and even legal action.

An efficient way to avoid these risks is to capture only the data that actually makes your service better. Do you really need a user's precise location? Alternatively, could your product work just as well with only a city or zip code? Or without associating location data with the user at all?

A 2012 SURVEY FOUND THAT 85 PERCENT OF CONSUMERS LIMIT HOW OR WHETHER THEY USE A MOBILE APPLICATION BASED ON PRIVACY CONCERNS.<sup>17</sup>

ACCORDING TO A 2012 STUDY, 54 PERCENT OF MOBILE APP USERS HAVE DECIDED TO NOT INSTALL AN APP WHEN THEY DISCOVERED HOW MUCH PERSONAL INFORMATION THEY WOULD NEED TO SHARE IN ORDER TO USE IT.<sup>19</sup>



**Google Slammed for “Wardriving by Design”:** Google's Street View, already the subject of numerous privacy complaints,<sup>20</sup> faced even more scrutiny when it was revealed in 2010 that the project had captured traffic from private wireless networks. As a result, Google faced multiple class action lawsuits<sup>21</sup> and investigations by at least seven countries.<sup>22</sup> Although the company initially stated that the collection was the result of a mistake by a single engineer,<sup>23</sup> an FCC investigation revealed that the collection “resulted from a deliberate software design decision” and that several other employees were notified of the practice.<sup>24</sup> These new revelations resulted in reopened investigations and have created the potential for additional penalties and other consequences for Google.<sup>25</sup>



**Path “Discovered Phoning Home with Your Address Book”:** Path came under harsh criticism when a Singaporean software developer discovered that the company violated its own Terms of Use policy by uploading users’ entire address books.<sup>26</sup> Path initially dismissed the criticism, stating that its app only used the address book data for “friend-finding” and that this usage was an industry standard. However, the overwhelming public condemnation forced the company to publicly apologize to users<sup>27</sup> and reassure them by deleting “the entire collection of user contact information from our servers.”<sup>28</sup> Despite these efforts to make amends, Path was hit with a class action lawsuit and roundly criticized in the press.<sup>29</sup>

## RETAIN INFORMATION ONLY AS LONG AS YOU NEED IT.

Some of the information that you collect may only be relevant to a specific transaction or may become essentially worthless to your service as times goes on. Identifying data that you do not need to permanently retain and deleting it once it is no longer necessary can eliminate potential privacy hazards.



**Apple Products Record Location History:** Apple was widely criticized after researchers discovered that iPhones and 3G iPads were collecting and storing a year’s worth of unencrypted data about user whereabouts.<sup>30</sup> Apple was also grilled about its practices by the Senate and federal agencies, and customers have filed a lawsuit seeking punitive damages accusing the company of invasion of privacy and computer fraud.<sup>31</sup> In the aftermath of the incident, the company admitted that it had erred and announced that it would reduce its storage period of location data to seven days or less, stop backing up data on people’s computers, and delete information when customers cease using location services.<sup>32</sup>



**Sonic.net Reduces Data Retention to Protect Customers:** Internet Service Provider Sonic.net has been widely lauded for cutting its retention period for user logs down to two weeks—far shorter than the reported retention period of any other major ISP.<sup>33</sup> Faced with “a string of legal requests for its users’ data,” the CEO asked engineers to evaluate the company’s actual storage needs and see if reducing data retention could help “protect my customers.”<sup>34</sup> The company determined that a two week retention period was more than adequate to address spam and security issues (system administrators found a day’s worth of logs was sufficient) and properly balanced “an ability to help law enforcement when it’s morally right to do so” with protecting users.

## ➔ DO YOU PROPERLY HANDLE ANY SENSITIVE DATA THAT YOU DO COLLECT?

Some kinds of data can be particularly sensitive and require special care. Information such as medical records, financial records, and data concerning children have specific legal requirements that you need to follow. But be mindful that collecting any data that users consider sensitive, including records that contain identifiers that may be linked to a specific person, creates the potential for consumer outrage, especially if such information is disclosed against the user’s wishes.

## IDENTIFY AND COMPLY WITH SPECIFIC REQUIREMENTS FOR THE DATA YOU COLLECT.

If your product handles certain types of information, you may be subject to specific legal requirements. For example:

- Any service that deals with electronic communications may be subject to the Electronic Communications Privacy Act.<sup>35</sup>
- Services that are designed for health care providers and related entities may be subject to the Health Insurance Portability and Accountability Act.<sup>36</sup>
- Any video content service may be subject to the Video Privacy Protection Act.<sup>37</sup>
- Websites and services that are “directed to children” may be subject to the Children’s Online Privacy Protection Act.<sup>38</sup>
- Other laws may apply if your service handles financial records,<sup>39</sup> consumer credit information,<sup>40</sup> government records,<sup>41</sup> motor vehicle records,<sup>42</sup> or student education records.<sup>43</sup>

Consult with an attorney or otherwise ensure that you comply with any specific requirements for the types of data you collect and use. See the Appendix for more information.



**Broken Thumbs Fined for Collecting Children’s Information:** In August 2011, mobile app maker Broken Thumbs Apps settled a complaint by the FTC for violating the Children’s Online Privacy Protection Act (COPPA).<sup>44</sup> The FTC alleged that the company’s “Emily” games collected information from children under 13 by encouraging them “to email ‘Emily’ their comments and submit blogs to ‘Emily’s Blog’ via email, such as ‘shout-outs’ to friends and requests for advice” and then used this information for marketing purposes—without obtaining the required parental consent.<sup>45</sup> Broken Thumbs’ settlement with the FTC required the company to pay a \$50,000 fine and submit to ongoing monitoring of its privacy practices.

## IDENTIFY AND CAREFULLY HANDLE ANY DATA THAT YOUR USERS MIGHT CONSIDER TO BE SENSITIVE.

Even if your company satisfies its legal requirements, it can still be called to account by users and the media if it mishandles data that your users consider sensitive—even if you expect that data to be innocuous.<sup>46</sup> All credit card and financial records, personal identifiers, passwords, and similar types of sensitive data should be treated with extra caution, as any kind of mishap with this sort of information can have major consequences both for your users and for your company.



**Blippy Users Share More than Expected:** In April 2010, Blippy users shared more than they bargained for when a Blippy security flaw made some users’ credit card numbers public in search engine results.<sup>47</sup> News of the breach traveled like wildfire and the mood at the startup “quickly went from elation to disbelief to disappointment.”<sup>48</sup> The company was forced to apologize for its mistakes, fix the problem, and take steps to better safeguard user data in the future, including hiring a Chief Security Officer and conducting security audits. Having a more solid security plan from the beginning might have prevented this data breach and saved Blippy from what its spokesperson called a “nightmare scenario.”<sup>49</sup>

## MINIMIZE THE LINKS BETWEEN COLLECTED DATA AND INDIVIDUAL USERS.

Tying identifiable data, including IP addresses or account information, to other records can increase the risk of harm to your users if a breach occurs and as a result may make your company more vulnerable to expensive lawsuits and government fines. In many cases, you may be able to avoid this risk without compromising your product or business goals. Explore approaches that effectively mask user identity while preserving the business value of collected information<sup>50</sup> and be particularly careful not to accidentally disclose identifiable data along with other potentially sensitive records.



**AOL Releases Not-So-Anonymous Data:** In 2006, AOL and its Chief Technical Officer learned the hard way that users do not appreciate disclosure of their online search activities. The company thought that it had properly anonymized the data when it posted online the search records of 500,000 of its users for use by researchers. It was wrong. The private search habits of AOL users became public knowledge.<sup>51</sup> AOL quickly pulled the dataset from its website, but not before the information had been mirrored on Web pages around the world and AOL's privacy breach was plastered on front pages around the globe.<sup>52</sup> The incident led to the firing of the researchers involved with the database's release and the resignation of the company's Chief Technical Officer.<sup>53</sup>

### ➔ DO YOU COLLECT AND STORE DATA SECURELY?

Creating a solid data-security plan is important both to protect user privacy and to safeguard your company's bottom line. Data breaches can be disastrous, leading to lawsuits, fines, and lost user trust. California law requires that all businesses maintain reasonable security procedures to protect the personal information of Californians from unauthorized access, destruction, use, modification, or disclosure.<sup>54</sup> The FTC has also made official recommendations for businesses to take stock of information they collect, minimize that collection where possible, secure the information that is maintained, and plan for the future.<sup>55</sup> Working with attorneys and security professionals to implement these recommendations will help protect you and your users from threats to the safety of their data.

“FIRESHEEP,” A PROOF-OF-CONCEPT PLUGIN FOR THE FIREFOX BROWSER, DEMONSTRATED HOW EASILY DATA AND EVEN ACCOUNT CREDENTIALS TRANSMITTED OVER AN INSECURE CONNECTION COULD BE INTERCEPTED.<sup>56</sup> THE MEDIA ATTENTION THAT THE APP ATTRACTED ENCOURAGED SERVICES LIKE FACEBOOK TO OFFER SITE-WIDE SECURE CONNECTIONS TO PROTECT THEIR USERS.

### COLLECT DATA SECURELY.

Secure every method of collecting data—whether over the phone, by mail, through email, via Web forms, or from affiliates or other third parties—against snooping and data theft. Follow best practices, such as ensuring that any Web connection carrying potentially sensitive information is secure, to protect your users' data in transit.

### STORE DATA SECURELY.

Data on your servers, on laptops, or in paper form should all be equally secure. Breaches can involve both high-tech methods such as hacking and phishing and decidedly low-tech methods such as rooting in dumpsters and stealing from mailboxes. Keep both your physical and network security up to date and use encryption and similar techniques to protect data wherever possible.



**LinkedIn Criticized in Aftermath of Breach:** In June 2012, LinkedIn was heavily criticized after hackers obtained nearly 6.5 million passwords and posted them on the Web.<sup>57</sup> Even though LinkedIn immediately acknowledged the leak and attempted to patch up its security, the company was criticized for its previous lax attitude toward security, including its lack of key security personnel, which resulted in the company being unprepared for a preventable attack.<sup>58</sup>

A 2010 SURVEY FOUND THAT NEARLY EIGHT IN TEN GLOBAL CONSUMERS WERE CONCERNED ABOUT UNAUTHORIZED ACCESS TO THEIR PERSONAL INFORMATION, A 6 TO 8 PERCENT INCREASE SINCE 2008.<sup>59</sup>

## LIMIT AND MONITOR ACCESS TO DATA.

While most people imagine shadowy hackers as their biggest security risk, in reality insiders with the ability to access records inappropriately and hide their misdeeds can also pose a significant threat. To minimize this threat, allow employees access only to the information they actually need to perform their jobs, thoroughly train individuals who handle user information in your privacy and security practices, and log all data access and review these logs regularly.



**Facebook's Master Account:** Users were outraged and the company's reputation was tarnished in 2007 when it came to light that the company had very poor internal security measures. Users demanded change when it was widely reported that the company was not properly safeguarding the private profiles of its users from employee misuse and that employees could view users' private profiles and track which users were viewing particular profiles.<sup>60</sup>

## PLAN AHEAD: INCORPORATE PRIVACY AND SECURITY FROM START TO FINISH

Thinking about the data you will collect and store while you design your product or service is only one part of "baking in" privacy. You also need processes in place to deal with issues that might arise in the future. Ensuring that your privacy and security plans are holistic and regularly re-evaluated and preparing ahead of time for potential security issues and legal demands for data can help you save time, money, and even your reputation in the long run.

### ➔ DO YOU HAVE A COMPREHENSIVE PRIVACY AND SECURITY PLAN?

Before your product or service launches, make sure that you have measures in place to protect the data you collect. Many privacy and security fiascos could have been avoided by following well-established best practices.

## IMPLEMENT ESTABLISHED BEST PRACTICES TO SECURE YOUR DATA.

Many security breaches could be prevented by following established best practices to protect data. Implementing a login system that does not require you to store your user's actual password, deploying firewalls and auditing network traffic, and utilizing other basic techniques can protect against data breaches and other security failures. Once you've put security measures in place, put them to the test by hiring outside "penetration testers" who will give you a real measure of the strength of your protection by attempting to break through your security measures.



**Citibank Hacked Using "Remarkably Simple Technique":** Citibank suffered a major security breach in 2011 and then faced a second wave of criticism for both its lack of preparation and its response to the incident.<sup>61</sup> The company waited three weeks before notifying the 210,000 customers that their data were compromised. Several days later, Citibank announced that, in fact, more than 360,000 accounts had been hacked. When it was revealed that the hackers used a "remarkably simple technique" to exploit a widely recognized vulnerability advantage, critics compared Citibank to a "mansion with a high-tech security system" in which "the front door wasn't locked tight."<sup>62</sup>

## ENSURE THAT YOUR PRIVACY AND SECURITY PRACTICES ARE FOLLOWED.

An effective privacy and security program requires both the commitment and the cooperation of every employee who is responsible for sensitive or private information. To ensure that the program is followed, the FTC recommends the establishment of a comprehensive privacy program, including the identification of key personnel who are assigned to oversee privacy issues throughout every stage of design and implementation and to ensure that developers are aware of and address privacy concerns as they are identified.<sup>63</sup>

## ➔ DO YOU CONTINUE TO EVALUATE YOUR PRIVACY AND SECURITY PRACTICES AS YOUR PRODUCTS AND COMPANY CHANGE AND GROW?

As your product evolves over time and you add or change features that involve user data, continue to review your privacy and security safeguards to make sure they keep pace. Internal audits and discussions with outside consultants and experts can help ensure that your privacy and security practices do not lag behind your expanding feature list and user base.

## RE-EVALUATE YOUR PRIVACY AND SECURITY PRACTICES AS YOUR COMPANY AND PRODUCTS EVOLVE.

Regular privacy and security assessments can help you evaluate how well your practices are being followed. The scope of each privacy assessment should depend on the data at stake and its potential vulnerability. Assessments should take place before a new product is launched and whenever major changes are implemented.



**Microsoft Builds Security into Design:** Microsoft's Security Development Life Cycle methodology, which includes privacy guidelines for each stage of a product's development, has evolved from an internal tool to a marketable product.<sup>64</sup> The company credited the tool with a 45 percent decrease in vulnerabilities in its transition from Windows XP to Windows Vista, and analysts have praised it for allowing developers who are not security experts to identify potential vulnerabilities.

## WORK WITH OUTSIDE EXPERTS TO IDENTIFY AND ADDRESS PRIVACY AND SECURITY RISKS.

In addition to regularly evaluating your internal processes, seeking advice from outside experts can bring a new perspective to your company's privacy and security risks. Working with researchers and other experts can help you identify and fix potential problems. On the other hand, trying to silence criticism may not only make it harder for you to secure your data, it may also lead to a public relations disaster.



**Cisco Tries to Silence Security Researcher:** In 2005, the company's reputation suffered after it threatened to sue the BlackHat security conference and a researcher for a presentation discussing flaws in the company's Internet router software.<sup>65</sup> The researcher had discovered that the flaw could potentially be exploited by hackers to seize control of a router and to monitor, intercept, delete, or misdirect communications. Although the conference and researcher were not deterred by the legal threats and the presentation went on as planned, Cisco's reputation in the technology world was heavily tarnished for trying to silence information about security threats.<sup>66</sup>

## ➔ DO YOU HAVE A PLAN TO NOTIFY AND PROTECT USERS IF A BREACH OCCURS?

Even with a solid data security plan, data can still be lost or stolen, but failing to respond appropriately to a data breach can make a bad situation far worse. Forty-six states, the District of Columbia, and several U.S. territories have laws that require businesses to notify users if their data are lost or stolen.<sup>67</sup> Your company needs to know how it will quickly and effectively inform users in the event of a data breach.

### NOTIFY USERS PROMPTLY.

Prompt notification is often crucial to allow users to prevent identity theft and other consequences of data loss before they occur. Failing to notify all affected users of a security breach, even if the law of every state does not require you to do so, could result in real costs to your users, bad press for your company, and the erosion of customer trust.



**ChoicePoint Suffers for Failing to Protect Consumers:** In 2005, data broker ChoicePoint paid with its capital, its stock price, and its reputation when it failed to secure the personal data of 163,000 individuals, allowing identity thieves to obtain this information.<sup>68</sup> ChoicePoint compounded its own injury by initially notifying only victims who happened to live in California, the only state at the time with a law mandating notification in the event of data loss. The ensuing public outcry forced ChoicePoint to notify all affected individuals, but not before its reputation was further tarnished.

### CLEARLY EXPLAIN WHAT HAPPENED.

Let users know what happened to their data, what you are doing to fix the problem, and how they can employ self-help to protect their own private information. By being forthright about the problem and offering clear guidance and assistance to your users about how they can protect and monitor their own privacy, you will reassure them that you take your business responsibilities—and their privacy—seriously.



**Sony's "Half-Baked Response" to Security Breach:** Sony "will have a long road ahead to win back the trust of gamers" after a security breach that shut down Sony's Playstation Network in spring 2011 turned into a major privacy fiasco.<sup>69</sup> The company waited five days before revealing that user data including passwords had been compromised, and then disclosed weeks later that at least some credit card information had been lost in the incident as well.<sup>70</sup> In the aftermath of the breach, Sony was excoriated by Congress, with Rep. Bono Mack (R-CA) describing its behavior as a "half-hearted, half-baked response [that] is not going to fly in the future."<sup>71</sup> The company also faces at least one lawsuit accusing it of not taking "reasonable care to protect, encrypt, and secure the private and sensitive data of its users."<sup>72</sup>

### CONTACT ALL RELEVANT INSTITUTIONS.

In the event of a data breach, you may need to contact law enforcement officials, banks, credit payment processors, and credit agencies. Generate a list of institutions to contact ahead of time so that you will be prepared if disaster strikes.

### PROTECT YOUR USERS AND REPAIR YOUR REPUTATION.

If you suffer a breach, do everything in your power to protect your users from further harm. Taking steps such as offering free credit monitoring to any user whose data was exposed can mitigate the damage both to your users and to your reputation.

## BE TRANSPARENT: GIVE USERS THE ABILITY TO MAKE INFORMED CHOICES

The first step in establishing a trust-based relationship with your users is giving them the information they need to make informed decisions. Doing so not only helps your users decide how to use your service, it can also build loyalty among your current users and help you recruit new ones.

### ➔ DO YOU CLEARLY COMMUNICATE YOUR PRIVACY PRACTICES TO YOUR USERS?

If your company operates a commercial website or mobile app targeting California residents, California's Online Privacy Protection Act requires that you post a conspicuous privacy policy that discloses the kinds of personally identifiable data collected and shared with third parties.<sup>73</sup> But a lengthy privacy policy filled with legal jargon may be difficult for most users to understand. A good approach is to also create easy-to-read privacy documents that spell out exactly what information you collect, retain, and use—and then to comply with all of your promises to users.

RESEARCH PUBLISHED IN 2012 ESTIMATED THAT IT WOULD TAKE AN AVERAGE AMERICAN UP TO 293 HOURS PER YEAR JUST TO SKIM THE PRIVACY POLICY OF EVERY SITE SHE VISITED.<sup>74</sup>

### EXPLAIN YOUR PRIVACY PRACTICES AS EFFECTIVELY AS POSSIBLE.

You can help your users understand your privacy practices by writing your privacy policy in plain, readable language. But your official policy doesn't have to be the only tool you use to explain your practices to users. Frequently Asked Questions pages, graphs and grids, and other communication methods can also help your users understand your privacy practices.



**DuckDuckGo Keeps Privacy Simple:** Fledgling search engine DuckDuckGo is reaping the benefits of having clear and privacy-friendly policies written in understandable English. Its privacy policy starts with a clear statement that "DuckDuckGo does not collect or share personal information,"<sup>75</sup> followed by a longer explanation about why users "should care." This policy has been highlighted by the press and the service has both increased traffic and obtained venture funding as a result of its privacy-friendly approach.<sup>76</sup>



**Zynga Makes Privacy a Game:** Social gaming company Zynga received kudos in 2011 for "making privacy a game" with "PrivacyVille," which provides users with an interactive mechanism to explore the company's privacy policy and rewards them with "zPoints" to spend in the company's other games.<sup>77</sup> The company was praised for creating a privacy tool "that makes sense and that users care and learn about."<sup>78</sup>

### EXPLAIN HOW INFORMATION IS SHARED WITH OTHER USERS OR THIRD PARTIES.

Users are very concerned about the possibility that their information might be shared without their knowledge or consent. You can address this worry by making it easy for users to understand who can view or access their information, how it can be used, and how your company ensures that it is not misused. "Third parties" should include anyone whom your users might not recognize as part of your company, even if they are not legally considered separate entities.

71 PERCENT OF RESPONDENTS TO A 2012 SURVEY WERE "VERY CONCERNED" ABOUT COMPANIES SELLING OR SHARING INFORMATION ABOUT THEM WITHOUT THEIR PERMISSION.<sup>79</sup>

## GIVE USERS AN OPPORTUNITY TO UNDERSTAND YOUR PRIVACY PRACTICES BEFORE THEY USE YOUR SERVICE.

Many privacy fiascos are triggered when users are unpleasantly surprised to learn how a service actually works and how their personal data has been or could be collected and used. Giving users at least a basic understanding of your product's key data practices and privacy protections before they jump in and use the service can prevent surprise and lead to a better relationship with your users in the long run.



**App Platforms, California AG Reach Privacy Agreement:** In February 2012, major mobile platforms Amazon, Apple, Google, HP, Microsoft, and RIM brought “good news” to smartphone users by reaching an agreement with the California Attorney General to give users information about mobile app privacy practices before the user downloads and runs the app.<sup>80</sup> The platforms agreed to require app-specific privacy policies for all applications and to allow users to view an app's policy before downloading it.

## MAKE SURE YOU COMPLY WITH YOUR PRIVACY PROMISES.

Failing to live up to your privacy statements may not only anger users but also result in government fines and lawsuits. Make sure that your privacy statements are accurate and that everyone who handles personal data understands and complies with them.



**Myspace Fined, Sued for Deceptive Privacy Practices:** In 2012, Myspace was hit with a class action lawsuit and an FTC investigation for failing to comply with its own privacy policy. The policy stated that it would not share personal information, yet the company allowed advertisers to access users' “Friend IDs,” which allowed the advertisers to obtain user names and personal information and track browsing history.<sup>81</sup> In a settlement with the FTC, Myspace agreed to implement a comprehensive privacy program and undergo regular, independent privacy assessments for the next 20 years.

## ➔ CAN YOUR USERS LEARN WHAT DATA YOU HOLD ABOUT THEM AND HOW IT IS USED AND SHARED?

### ALLOW USERS TO REVIEW THE INFORMATION THAT YOU HAVE COLLECTED ABOUT THEM.

Allowing users to review the data that you currently possess about them can give them a better understanding of the privacy consequences of their actions. It can also help you by allowing users to review and correct inaccurate data and flag any uses or disclosures that they find inappropriate.

### DISCLOSE THIRD PARTIES WITH WHOM YOU HAVE VOLUNTARILY SHARED A USER'S INFORMATION.

ACCORDING TO A 2009 SURVEY, 69 PERCENT OF AMERICANS BELIEVE THERE SHOULD BE A LAW THAT GIVES PEOPLE THE RIGHT TO KNOW EVERYTHING A WEBSITE KNOWS ABOUT THEM.<sup>82</sup>

Many users are particularly concerned about the possibility that their information might be shared with third parties without their knowledge and consent. Letting users identify the actual recipients of their personal information, as well as what those recipients are permitted to do with that information, is a critical step in building trust and empowering users to make informed choices—even if that choice is whether or not to use your service. Doing so also allows your users to identify and flag third parties who appear to be abusing their privileges by collecting excessive amounts of data or using that data in ways that violate your agreements with that party or your users. As with all of your policies and records, inform users of any change to your sharing practices before it goes into effect.

## BE TRANSPARENT ABOUT LEGAL DEMANDS FOR USER INFORMATION.

If you are confronted with a demand for a user's information, notify her as soon as possible so that she can defend herself rather than hold you accountable (fairly or not) if she later learns that her data were shared without her knowledge or consent. Beyond that, being transparent about how many demands for information you receive and when you comply with these demands can benefit not only your users but your reputation.



**Google Publishes Transparency Report:** In an important move toward transparency, Google released a Transparency Report tool in 2010 to track and display the number of government demands to remove content or disclose user data that the company receives worldwide, country by country.<sup>83</sup> Although the tool does not track all requests and only counts the numbers of requests received, not the number of user records requested, Google was applauded for providing some information about government demands.<sup>84</sup> Other companies such as Twitter have started to follow suit.<sup>85</sup>

## ➔ DO YOU CLEARLY INFORM YOUR USERS WHEN YOU ARE COLLECTING DATA ABOUT THEM?

If your company's product can turn on sensors or capture data about your user's location or activities, you need to clearly inform users of its capabilities and notify them whenever it is active. Failing to do so can lead to user outrage and legal consequences when users discover that your product has been secretly collecting information about them. You can take some important steps so that customers are not being forced to choose between your product and their privacy.

## INFORM USERS ABOUT ALL DATA COLLECTION AND OBTAIN OPT-IN CONSENT.

Inform users about all of the information that your product or service generates or collects and allow them to choose whether and when to share this information. Failing to keep users informed about data collection can lead to your product being labeled as "spyware" or worse.



**CarrierIQ Accused of Planting Spyware on Smartphones:** Mobile analytics company CarrierIQ and its business partners were hammered with negative press and legal actions when a researcher discovered that the company's software, capable of intercepting and recording almost every single use of the phone, had been pre-installed on millions of HTC, Samsung, and Apple phones provided by T-Mobile, Sprint, and AT&T without users' knowledge or consent.<sup>86</sup> The company initially tried to suppress reports about its product by threatening the researcher with a lawsuit<sup>87</sup> but later was forced to acknowledge that it held a "treasure trove" of information and was sharing this information with the carriers.<sup>88</sup> As a result, the company and its partners saw the situation "spiral out of control" and now face class action lawsuits alleging violations of federal wiretapping law,<sup>89</sup> as well as the scorn of users, the media, and Congress.<sup>90</sup>



**NebuAd's Plan to Monitor Internet Use Triggers Outrage:** NebuAd's "deep packet inspection" system, designed to track online activity without notifying the user, led to broad consumer outcry in 2008 when plans to use it were revealed.<sup>91</sup> The ensuing privacy storm included an inquiry into the system's legality by the House Energy and Commerce Committee, the resignation of the founder and chief executive, and the cancellation of major partnership agreements, including a pilot program with the fourth-largest Internet service provider in the United States.

## NOTIFY USERS WHENEVER MONITORING IS ACTIVE.

Users should be aware when a device or product is collecting information or when a microphone, camera, or other sensor is turned on. If your product allows user information to be collected and transmitted surreptitiously and this is discovered, user trust can be severely affected.



**In-Car Assistance Systems Caught Spying on Drivers:** Users who purchased in-car assistance systems they hoped would help them find their stolen cars or get help in an emergency were not happy to learn that these systems could be used to spy on them. Because some of these systems can be remotely activated without alerting the occupants of the vehicle, they have been secretly used by law enforcement to track individuals and silently snoop on their conversations. The press widely reported this undisclosed “feature” of such systems.<sup>92</sup>

## ➔ DO YOU CLEARLY COMMUNICATE PRODUCT CHANGES TO YOUR USERS?

### NOTIFY USERS ABOUT PRODUCT CHANGES THAT AFFECT PRIVACY BEFORE THE CHANGES ARE IMPLEMENTED.

Many of your users likely will embrace new or improved functionality as long as they are aware of what they are getting, but they may react negatively if they are surprised. Giving users notice and requiring them to opt in will allow them to voice possibly legitimate complaints and could prevent controversies when new features have unforeseen consequences.



**Etsy Suffers Privacy “DIY-saster”:** In early 2011, online marketplace Etsy suffered a “social media DIY-saster” after a change to the site made shoppers’ feedback posts, purchases, and in some cases, real names publicly visible and searchable.<sup>93</sup> The company was particularly criticized for announcing the change only on a forum rarely used by buyers and for refusing to take its users’ privacy concerns seriously before the media drew attention to the issue, leading to an incident described as “Etsy’s privacy Valdez.”<sup>94</sup> The online marketplace has since changed its default privacy settings, apologized for its behavior, and acknowledged that it will have to “work hard to regain your trust,”<sup>95</sup> for many users, however, this may have been the “last straw.”<sup>96</sup>



**Facebook Backtracks on Privacy Changes:** In 2010 Facebook suffered a backlash when it reduced user control by adding “Connections” (which were shared with all other Facebook users without any option to limit visibility) and “Instant Personalization” (which shared information with certain third-party sites without first asking for the user’s consent) and turning both features on by default.<sup>97</sup> Thousands of users posted comments expressing their frustration at being forced to manually disable instant personalization,<sup>98</sup> and senators asked the FTC to investigate Facebook’s actions and called for simpler privacy controls.<sup>99</sup> Less than two months later, Facebook was forced to backtrack (yet again) by creating privacy settings for “Basic Directory Information” and making it easier for users to opt out of Instant Personalization.<sup>100</sup>

## DISTRIBUTE UPDATES AND NEW PRODUCTS SEPARATELY.

Using an “update” to push out new, unrelated products can result in negative press and may cause users to lose faith in security update tools. Encourage users to install or use your great new product voluntarily—don’t trick them into it by attaching it to an update for a service they already use.



**Apple’s Update Mechanism “Borders on Malware”:** When Apple released Windows version 3.1 of its Safari Web browser, it wasn’t content to simply promote its new product. Instead, it released the browser as an “update” to its popular iTunes music software, causing many iTunes users to involuntarily install Safari. Critics claimed that Apple’s behavior “bordered on malware distribution practices,”<sup>101</sup> driving Apple to clearly identify Safari as a new product and enable users to opt in prior to installation.<sup>102</sup>

## PARTNER WITH YOUR USERS: PUT USERS IN CONTROL AND STAND UP FOR THEIR RIGHTS

Even if you plan to offer your product “for free” and generate revenue from advertising or other means, it is in your best interest to treat your users as partners: recognizing and respecting their expectations, giving them the tools to make their own decisions about their personal information, and standing up for them when they are unable to defend themselves. By doing so, you may not only avoid the consequences when users are unpleasantly surprised about how their data are used, you may find that users are more willing to pay for or engage with your service if you earn their trust.

A 2011 CARNEGIE MELLON STUDY ON PRIVACY PREFERENCES FOUND THAT “WHEN PRIVACY INFORMATION IS MADE MORE SALIENT AND ACCESSIBLE, SOME CONSUMERS ARE WILLING TO PAY A PREMIUM TO PURCHASE FROM PRIVACY PROTECTIVE WEBSITES.”<sup>103</sup>

### ➔ DO YOU GIVE USERS CONTROL OVER THEIR PERSONAL INFORMATION?

Users want to be in control of how their information is used or shared. California law already gives consumers the right to learn how their personal information is shared by companies and encourages the adoption of simple methods for individuals to have the ability to opt out of information sharing.<sup>104</sup> Failing to obtain explicit consent to use or share personal information, or making it difficult for users to remove themselves from lists or terminate use of products, risks alienating existing users and discouraging others from joining. Putting your users in control may lead to a far more positive relationship.

## ALLOW USERS TO REVIEW, MODIFY, AND EXPORT THEIR OWN DATA.

Allowing users to review and maintain their own records (with appropriate logging and oversight) and export their own data can benefit both your users and your company. Users are often in the best position to fix mistakes in your data and thus increase the market value of the data that you do collect. And making it clear that users can modify or export their data and use it as they see fit may encourage users to feel more comfortable with your service and boost your company’s reputation in the process.



**Google Creates “Data Liberation Front”:** In 2009, Google announced the creation of the Data Liberation Front, an internal project designed to allow users to export data from Google services.<sup>105</sup> The group took to heart then-CEO Eric Schmidt’s declaration that “if you don’t like Google, if for whatever reason we do a bad job for you, we make it easy for you to move to our competitor.”<sup>106</sup> One commenter noted that the Data Liberation Front both “makes perfect sense from a business perspective” and was “a positive step that’ll be beneficial to [Google’s] users.”<sup>107</sup>

## ALLOW USERS TO CONTROL HOW THEIR DATA ARE COLLECTED, USED, AND SHARED.

Although your service may require certain data to function properly, giving users the ability to choose how and whether any other information is collected, used, or shared can increase trust and even use of your service by providing users with the ability to choose the context in which they participate. You can increase user control by providing easy-to-use tools that allow users to understand and select their privacy and sharing preferences.

**93 PERCENT OF RESPONDENTS TO A 2008 SURVEY STATED THAT INTERNET COMPANIES SHOULD ALWAYS ASK FOR PERMISSION BEFORE USING PERSONAL INFORMATION, AND 72 PERCENT WANTED THE RIGHT TO OPT OUT WHEN COMPANIES TRACK THEIR ONLINE BEHAVIOR.<sup>108</sup>**



**ScanScout Offers Opt-Out, Then Prevents It:** In 2011, ScanScout, an online video advertising network, was investigated by the FTC<sup>109</sup> and hit with a class action lawsuit<sup>110</sup> for its deceptive practice of using persistent “supercookies” to track users online. Although ScanScout’s privacy policy stated that users could change their browser settings to “opt out” of its information tracking, the company actually used technology designed to prevent users from doing so. ScanScout settled with the FTC by submitting to ongoing oversight of the company’s privacy practices.



**Google Faces Record Fines for Bypassing Privacy Settings:** In 2012, Google agreed to pay a record \$22.5 million FTC fine<sup>111</sup> and was hit with multiple lawsuits<sup>112</sup> for violating its own statements and bypassing privacy settings on Apple’s Safari web browser. Although Google had told Safari users that they could use the browser’s privacy settings in order to prevent tracking, the company also deployed code that enabled its own software to bypass these settings.<sup>113</sup> Critics noted that the incident “represents another PR blow” for Google and called for the company to “make a pro-privacy offering to restore your users’ trust.”<sup>114</sup>

**ACCORDING TO A 2009 STUDY, 92 PERCENT OF ADULT AMERICANS AGREE THERE SHOULD BE A LAW THAT REQUIRES WEBSITES AND ADVERTISING COMPANIES TO DELETE ALL STORED INFORMATION ABOUT AN INDIVIDUAL, IF REQUESTED TO DO SO.<sup>115</sup>**

## CREATE A QUICK AND EASY PROCESS FOR USERS TO DELETE CONTENT OR TERMINATE ACCOUNTS.

Users may be more likely to share content on your site if they know they can change their mind and delete it later. And while you may hope that none of your users decides to leave your service, if a user wants to leave, she should be able to delete her entire record, including any archived or residual information. The negative publicity from denying users the right to terminate their account will far outweigh any marginal benefit from retaining their information.



**Netflix Sued for Retaining Records About Former Customers:** In 2012, Netflix settled a class action lawsuit alleging that it retained records about former customers in violation of the Video Privacy Protection Act.<sup>116</sup> The company ultimately settled the lawsuit by agreeing to pay \$9 million and change its policy to permanently de-associate records from accounts that had been inactive for more than 365 days.



**Facebook Makes It Hard to Leave:** Facebook users were very unhappy in 2008 when they realized that it was nearly impossible to remove their information from the social network.<sup>117</sup> One user reported that it took “two months and several email exchanges with Facebook’s user service representatives to erase most of his information from the site.” The lack of easy and effective deletion procedures led to anger from Facebook’s users, and many bloggers encouraged users to delete accounts and posted detailed instructions of how to do so.<sup>118</sup> To stem the tide of criticism, Facebook modified its settings and provided straightforward instructions for users who wish to delete their accounts.<sup>119</sup>

PARTNER WITH YOUR USER

## ➔ DO YOU IDENTIFY AND RESPECT USER EXPECTATIONS?

Many privacy disasters occur when users learn that they have been automatically enrolled in a new service or feature that they find invasive or when non-users are surprised to find out that your product has been collecting and using information about them without their consent. By evaluating products from a consumer perspective and giving users the option of activating new features, you can build trust and avoid unpleasant surprises for everyone involved.

### EVALUATE FEATURES AND DATA SHARING FROM MULTIPLE PERSPECTIVES.

Many privacy catastrophes occur because companies focus on their internal perspective of the value of collecting or sharing data without adequately considering the potential wider effects on users or the general public. By looking at your product from various points of view, including bringing in focus groups or outside advisors to evaluate the consequences of your new product or feature, you can better anticipate and design for consumers' actual expectations.



**Fitbit Deals with Fireworks After Exposing “Sex Stats”:** Fitbit, an online service that allows users to track their exercise habits, found itself faced with a different set of fireworks during the 2011 Fourth of July weekend when some users discovered that their sexual activity was being broadcast to the public.<sup>120</sup> The company had made all reported data visible to everyone by default without considering the full scope of “exercise data” that it allowed users to include. Although FitBit “pulled a quickie” by making activity reports private for all new and existing users and even contacting search engines to try to remove results, the damage was already done.



**i-Free Forced to Pull App “Geared Toward Stalkers”:** In 2012, app developer i-Free Innovations was forced to pull its controversial iPhone app “Girls Around Me” from the App Store after heavy criticism of its privacy practices.<sup>121</sup> The app, which used data from Facebook and Foursquare to display the location, picture, and information of nearby women, was shut down by Foursquare<sup>122</sup> amidst outrage that it was “geared towards stalkers” and violated user expectations about the use of personal data.<sup>123</sup>

### REQUIRE USERS TO OPT IN TO ANY CHANGE THAT MAY CONFLICT WITH THEIR EXPECTATIONS.

Although it is important to notify users about any change that impacts their privacy, it is especially important to inform users and obtain their consent when you make a change that directly conflicts with users' current expectations. Users who are not adequately informed and given an opportunity to opt in to a new feature may view the change as a betrayal of their trust.



**Google Buzz Exposes Private Contact Details:** In early 2010, Google tried to jump on the social networking bandwagon by releasing its own service, Google Buzz. But the biggest buzz about the new service focused on privacy because Google pre-populated “following” lists with frequent chat and email contacts and made that information public by default. Media articles called Buzz a “privacy nightmare”<sup>124</sup> and warned that Buzz “managed to completely overstep the bounds of personal privacy.”<sup>125</sup> Within weeks of launch, Google Buzz became the subject of an FTC privacy complaint<sup>126</sup> and a class action lawsuit that resulted in an \$8.5 million settlement.<sup>127</sup> Google ultimately axed the entire Buzz service.<sup>128</sup>

## ➔ DO YOU STAND UP FOR YOUR USERS' PRIVACY?

Going the extra mile to protect privacy can earn your company the valuable trust of your users. Many of the privacy laws in the United States are badly outdated, resulting in a patchwork system of legal protection for privacy riddled with loopholes and grey areas. While this uncertainty may subject your company to legally questionable demands for user data, it also gives you an opportunity to establish a reputation as a champion of your users' rights. As one Chief Privacy Officer put it: "Your customers will hold you to a higher standard than laws will, and the question is, do you pay attention to your customers? Do you care about your customers?"<sup>129</sup>

### COMPLY WITH DEMANDS FOR INFORMATION ONLY WHERE CLEARLY REQUIRED BY LAW.

Reject any demand for user information that lacks legal authority. If the law is uncertain, challenge the legitimacy of a demand for information. Stronger, clearer privacy laws will make compliance easier in the future, and your users will reward you for fighting for their interests.



**Yahoo! Successfully Fights Warrantless Demand:** In 2010 Yahoo! was applauded by users and privacy advocates when it successfully fought a Justice Department demand for access to a user's email without a search warrant.<sup>130</sup> The Justice Department withdrew its request after Yahoo! went to court rather than comply with the demand (and was publicly supported by Google and numerous public interest organizations in a friend-of-the-court brief). As a result, Yahoo! won points with privacy advocates for being committed to protecting the privacy of its users.<sup>131</sup>



**Amazon Sues to Protect Users:** Amazon showed its commitment to protecting the privacy of users in 2010 by refusing to turn over records detailing more than 50 million purchases of North Carolina residents to that state's Department of Revenue.<sup>132</sup> To protect its customers and their ability to "purchase sensitive or unpopular material," the company filed suit against the state agency with the support of the ACLU.<sup>133</sup> The state ultimately agreed not to demand the titles or other identifying information about books, movies, and similar material.<sup>134</sup>



**AT&T, Verizon Accused of Eavesdropping on Users:** In 2006, news broke that these two massive telecommunications companies had been allegedly turning over the private calling records of millions of Americans to the National Security Agency.<sup>135</sup> The companies were caught in a firestorm of bad publicity and hit by a barrage of costly class action lawsuits.<sup>136</sup> The companies faced potentially "crippling" damages in the hundreds of billions of dollars and spent massive amounts on attorney and lobbyist fees to try to sidestep liability.<sup>137</sup>



**Qwest Resists Surveillance Efforts:** Unlike AT&T and Verizon, Qwest resisted the NSA's request for telephone records and received a significant amount of positive media coverage as a result. The *New York Times* described the company as "a gleaming political touchstone and a beacon of consumer protection" and noted that many users had switched to Qwest purely on the basis of its principled stand against government surveillance,<sup>138</sup> the Associated Press declared that Qwest was "squarely on the side of the little guy,"<sup>139</sup> and bloggers created online buttons reading "Qwest: N.S.A.-Free. Who are you with?"<sup>140</sup> As the *New York Times* pointed out: "Companies can't buy that kind of buzz."

## PROMPTLY NOTIFY THE USER AND GIVE HER AN OPPORTUNITY TO RESPOND.

If you do receive a legitimate demand for information, notify the target of that request. Inform the user about any legal options she might have to challenge the demand, such as a motion to quash a subpoena, and give the user as much time as possible to do so before complying with any demand for information.



**Twitter’s “Remarkable Display of Backbone”:** In January 2011, Twitter was widely applauded for its “remarkable display of backbone” in standing up for its users’ privacy and free speech rights by challenging the secrecy of a demand from the Department of Justice (DoJ).<sup>141</sup> Seeking information about Twitter users who were thought to be affiliated with WikiLeaks, the DoJ obtained a court order requiring Twitter to turn over those users’ records—including contact and credit card information and the identities of other individuals who communicated with those users. The court also issued a “gag order” prohibiting Twitter from telling these users about the demand. However, Twitter upheld its promise to notify users of a demand whenever legally possible by fighting back against the order.<sup>142</sup>

## DISCLOSE ONLY REQUIRED INFORMATION.

Companies often hand over far more information than is asked of them—for example, handing over months of call records when law enforcement has only requested a single week or disclosing user transactions that are unrelated to the scope of the request.<sup>143</sup> Excessive disclosure can lead to legal liability for your company and loss of user trust.



**Google Fights Demand for Millions of Search Records:** When Google stood up for the privacy of its users by fighting an overbroad civil subpoena from the government that demanded millions of private search queries, the company reaped a bonanza of positive public and media attention. In the end, the court held that the government was only entitled to 50,000 URLs with no personal information.<sup>144</sup>



**YouTube Wins Battle to Anonymize Data:** As part of an ongoing suit against YouTube/Google for copyright infringement, in 2007 Viacom sought and obtained a discovery order forcing YouTube to disclose all “video-related data from the logging database,” including information identifying the users who watched each video.<sup>145</sup> YouTube continued to fight for the privacy of its users and in 2008 reached an agreement with Viacom to anonymize the identities and IP addresses of non-Google employees in any data conveyed to Viacom.<sup>146</sup>

## PUSH FOR STRONGER LAWS TO PROTECT USER PRIVACY.

Although privacy issues are increasingly on the radar of the public, press, lawmakers, and regulators, legal protections for online privacy are still badly outdated. For example, the Electronic Communications Privacy Act, the federal law intended to protect the privacy of electronic communications and online data, has not been meaningfully updated since its enactment in 1986, before the Web, social media, and other widespread modern technologies even existed.<sup>147</sup>

As the law gets more and more outdated, user privacy is increasingly at risk, and companies are regularly faced with demands for information that may or may not be legitimate. Joining coalitions with advocates and other companies and supporting efforts to reform privacy law at the state and federal level may not only clarify your own legal obligations, it can also help to establish your reputation as a company invested in protecting your users’ privacy.



**Google Protects Readers of Digital Books:** Google helped protect the privacy of its users by supporting the passage of the California Reader Privacy Act.<sup>148</sup> The law, which went into effect in January 2012, ensures that government and third parties can’t demand access to private reading records held by companies without proper justification and creates greater transparency about how often reading records are disclosed.<sup>149</sup>

# GIVE YOUR USERS A PLATFORM TO SPEAK FREELY

The Internet is increasingly seen as a key catalyst of freedom of expression around the world. Simultaneously, companies are realizing that allowing users to express themselves freely is an excellent way to build loyalty. Giving your users a forum to express their views, free from censorship and other limitations, can create a sense of place and community that can enormously benefit your company as well as your users.

## ENCOURAGE USERS TO SPEAK FREELY: ESTABLISH POLICIES THAT PROMOTE SPEECH IN EVERY FORM

If your product allows users to interact with each other, it is in your best interest to encourage user expression. The more freedom your users have to communicate with their friends and the world at large, express themselves as they see fit, and explore a wide variety of content, the more likely they are to interact deeply with your service, with lasting benefits to everyone involved.

### ➔ DO YOU ENCOURAGE USERS TO EXPRESS THEMSELVES AS THEY CHOOSE?

Many successful products evolved in ways their creators never envisioned when users were given the freedom to innovate and utilize the service in different ways rather than adhere to constraints imposed by the service. Give your users as many choices as possible in how they communicate with each other and they may turn your product into a surprising success story.

### PROMOTE SPEECH REGARDLESS OF TOPIC OR VIEWPOINT.

To build the widest possible user base, your service should let users discuss the topics they choose and feel free to express their own viewpoint. Encouraging debate rather than stifling dissent can produce a vibrant and compelling dialogue that engages existing users and attracts new ones, while censoring legitimate speech can generate bad press, outraged users, and governmental intervention.



**Facebook Called Out for Rejecting Drug Policy Reform Ads:** In 2012, Facebook's effort to position itself as a key platform for reaching "a huge potential voter pool"<sup>150</sup> was undermined when its reviewers rejected multiple ads by two separate groups promoting discussion of marijuana legalization and drug policy reform.<sup>151</sup> Although Facebook quickly rescinded the rejection and promised to evaluate its processes for reviewing ads, it still has to address the reputational effects of not initially treating all political content equally.

### ALLOW USERS TO SPEAK ANONYMOUSLY OR PSEUDONYMOUSLY.

The courts have repeatedly affirmed that "protections for anonymous speech are vital to democratic discourse."<sup>152</sup> Many of your users may have important reasons to conceal their identity, whether they are domestic violence survivors, youth questioning their sexual orientation, or whistleblowers reporting an abuse of power. Other users may simply wish to access and share information without fear of harassment or embarrassment. Embracing these users by enabling anonymous or pseudonymous speech can add a deeper dimension to the conversations on your service.



**Google+, Minus Anonymity:** In 2011, Google came under fire for requiring users of its new Google+ service to use their real names, rather than pseudonyms, as identifiers on the service.<sup>153</sup> Critics expressed concern about the loss of online pseudonyms and the especially problematic consequences for people in vulnerable positions. Many users also complained about frequent and unpredictable account deactivation based on the real name policy. Google's initial response, "use your name or don't use the service," was viewed as a lost opportunity to distinguish itself from Facebook. However, continuing pressure ultimately convinced the company to backtrack and promise to allow pseudonyms.<sup>154</sup>

## ▶ DO YOU GIVE USERS CONTROL OVER THE CONTENT THEY ACCESS AND THE TOOLS THEY USE?

Freedom of expression is not just the right to speak freely; it is also the right to obtain information without censorship or restriction. If you prevent your users from accessing content they want to read or see, or if you limit the tools they can use to communicate with each other and the wider world, they may see your product as a hindrance rather than a service.

### ALLOW USERS TO ACCESS CONTENT WITHOUT FILTERING OR CENSORSHIP.

Your users expect to be able to access the content they want. Providing them with the tools to do so, rather than using technology to block access to legitimate content, encourages them to work with your service rather than express their outrage or look for other means of obtaining access to the content.



**Apple Comes Under Fire when Siri Refuses to Provide Abortion Content:** Apple came under fire from users and the press when it was discovered that the new iPhone's "intelligent personal assistant" Siri would not provide information about abortion clinics or emergency contraceptives.<sup>155</sup> Instead of providing the requested information, Siri replied to inquiries by saying it "couldn't find any abortion clinics" despite there being multiple hospitals and Planned Parenthood health centers nearby, or in some cases even by directing users to anti-abortion centers. Although Apple denied allegations of intentionally censoring abortion and contraceptive information and called Siri's response to such inquiries a "glitch," users and the media remained skeptical that the application's performance was entirely a mistake.



**AT&T Faces the Music for Censoring Pearl Jam:** Censoring the political speech of the popular rock band Pearl Jam landed AT&T in hot water in 2007. The company censored several seconds of a live concert broadcast, replacing the lyrics "George Bush, find yourself another home" with silence.<sup>156</sup> Although the company quickly reposted an uncensored version, the damage to its reputation could not be reversed as easily.

### DO NOT DISCRIMINATE AGAINST PARTICULAR TOOLS OR SERVICES.

Users consistently express outrage when ISPs and similar services interfere with their ability to use third-party software. You can avoid controversy and demonstrate your support for your users by giving them the freedom to communicate using whatever application or tool they choose.



**AT&T Accused of “Holding FaceTime Hostage”:** In 2012 AT&T triggered consumer and media outrage when it announced that it would only allow iPhone users to use the video chat app FaceTime on the carrier’s cellular data network if the customers purchased a shared data plan. As a result, the company was subjected to a barrage of negative press and customer complaints, with the media accusing the company of “holding FaceTime hostage,”<sup>157</sup> “slapping consumers in [the] face over FaceTime,”<sup>158</sup> and carrying out “simple extortion.”<sup>159</sup>



**Verizon Pledges Not to Monitor Users:** In late 2007, Verizon received widespread praise when it made a pro-free speech pledge not to monitor its network backbone for peer-to-peer file sharing. The company pledged that it would not “accept the role of network police agency.”<sup>160</sup>

## ➔ DO YOU LET USERS SPEAK FOR THEMSELVES?

Your users may be happy to talk about your service voluntarily, but they are less likely to react well if they are forced to do so. Ensure that users are in control of their own expression and that you aren’t putting words in their mouths without their consent.

### GIVE USERS FULL CONTROL OVER WHAT THEY SAY AND HOW THEIR COMMUNICATIONS ARE USED.

You may want to encourage your users to pitch your service to their friends—but simply doing so on their behalf can backfire, generating resentment and even lawsuits. Letting your users decide what to say about your company and when to say it may win you more users in the long run.



**Socialcam Slammed for “Bullying” Users:** In early 2012, the Facebook app Socialcam was slammed in the press for oversharing potentially embarrassing information, “bullying” people into installing the app, and ignoring stated privacy preferences.<sup>161</sup> The app’s stated purpose was to allow users to share videos on Facebook, but its inadequate controls led to concerns that users might unknowingly share harmful material.<sup>162</sup>

### CLEARLY DISTINGUISH YOUR OWN SPEECH.

Your company is entitled to express its own position. But it is important to make it clear when your company is speaking on its own behalf or simply relaying user expression. Making it easy for users to distinguish between the two can avoid incidents that erode trust in your product and company.



**Tagged Named “World’s Most Annoying Website” for Deceptive Emails:** In 2009, in a misguided attempt to boost membership, social networking site Tagged sent millions of deceptive emails that misled recipients into giving the company access to their contact lists.<sup>163</sup> As users became aware of the deception, Tagged’s reputation and pocketbook both suffered. In addition to being called “the world’s most annoying website” by *Time*,<sup>164</sup> Tagged racked up over \$1.4 million in fines after being sued by at least three states.<sup>165</sup>

## ➔ DO YOU ENCOURAGE YOUR USERS TO SPEAK WITHOUT FEAR OF BEING MONITORED?

If your service attempts to profile users by intercepting and tracking Web searches, email, online downloads, and other activities, it may not only invade users' privacy but also discourage users from communicating freely on your platform. Encourage your users to freely express themselves by making it clear that you will not monitor their online activities.

## MODERATE CAUTIOUSLY: AVOID CENSORING OR REMOVING LEGITIMATE SPEECH

Although promoting most kinds of speech can benefit your product, you may need to place limits on illegal activity or behavior that causes harm to your company or your community of users. Making these policies as clear and narrow as possible and ensuring that there are mechanisms in place to handle disputes with minimal disruption to free expression on your service can help users understand and comply with your code without feeling that their freedom of speech is unreasonably constrained.

## ➔ DO YOUR POLICIES PROTECT YOUR USERS AND YOUR COMPANY WITHOUT DETERRING LEGITIMATE SPEECH?

If your product provides a forum for content or communication, consider carefully whether you want to be in the business of policing those forums. Clear, narrowly-drafted policies that prohibit only illegal or disruptive speech can protect your company as well as your users' freedom of expression.

## PROHIBIT ONLY ACTIONS THAT ARE ILLEGAL OR DISRUPT THE PRIMARY FUNCTION OF YOUR SITE OR SERVICE.

A sense of community can flourish when users are able to communicate freely. Narrowly tailoring your terms of service to prohibit only illegal or disruptive content will help you limit the time you spend monitoring speech as well as the risk of being seen as inconsistent or biased in the application of your rules.



**PayPal Flops as Moral Police:** In February 2012, PayPal told book publishers to remove certain "offending literature" from their catalogs or be removed from online payment processing, drawing criticism from the press and civil liberties groups.<sup>166</sup> Although the company claimed that its policy was merely a shield against legal action, its actions were seen as affecting a broad range of "offensive" content, some of which was clearly legal.<sup>167</sup> Faced with a barrage of criticism, PayPal narrowed its policy to focus more narrowly on illegal and liability-inducing material.<sup>168</sup>



**BART Sparks Controversy by Blocking Cell Service:** The Bay Area Rapid Transit system (BART) sparked a national controversy in 2011 when it shut down cell phone service in advance of a planned protest of a fatal shooting by a BART police officer.<sup>169</sup> The agency's action triggered an outpouring of customer and media outrage and an investigation by the Federal Communications Commission<sup>170</sup> and caused the agency to adopt a new policy to only restrict cell phone access in "extraordinary circumstances" when there is a "strong evidence of imminent unlawful activity."<sup>171</sup>

## CLEARLY SPELL OUT THE CONTENT OR SPEECH THAT IS PROHIBITED AND THE CONSEQUENCES OF VIOLATING YOUR POLICY.

Vague prohibitions of “offensive” or “inappropriate” speech leave users uncertain as to what they can and cannot say, which can both chill acceptable speech and drive users to forums with clearer and more speech-friendly policies.



**Twitter Rethinks Its Code of Conduct:** In 2008, Twitter was dragged into an incident between two of its users as a result of its code of conduct that prohibited “harassing” or “intimidating” tweets.<sup>172</sup> Twitter initially removed a number of tweets that allegedly violated its code, but later reversed course and permitted subsequent tweets rather than comply with requests to ban the offending user from the service. Ultimately, Twitter decided to amend its terms of service and asserted its desire to be “a communication utility, not a mediator of content.”

## ALLOW USERS TO REMEDY OR APPEAL VIOLATIONS.

Unilaterally deleting content or imposing penalties without notice can leave users feeling frustrated and angry. Instead, inform users when they appear to be violating your terms of service, explain exactly what they did that is not allowed, and allow them to appeal that judgment. These actions can both reduce negative feelings about a particular incident and help users understand how to comply with your rules in the future.

### ➔ DO YOU CONSISTENTLY APPLY YOUR POLICIES?

Even the most speech-friendly policies will do little good if they are not consistently applied. Make sure that everyone responsible for moderating or monitoring content is on board with your efforts to protect and promote speech.

## ENSURE THAT YOUR POLICIES FOR REVIEWING CONTENT AND COMPLAINTS PRODUCES CONSISTENT RESULTS.

Having a clear and consistent interpretation of your own policy and ensuring that your reviewers understand and follow it may help your users properly stay within boundaries of acceptable behavior. It can also avoid controversies where content is declared legitimate by some reviewers but nonetheless flagged as inappropriate and removed by others.



**Facebook Faces “Nurse-In” over Breastfeeding Photo Policies:** In February 2012, Facebook offices were the site of “nurse-ins” protesting the social giant’s practice of repeatedly taking down photographs of breastfeeding mothers.<sup>173</sup> Although Facebook stated that its current practice was to allow such photos, in practice breastfeeding photos have been removed frequently for containing “nudity” and some mothers’ Facebook accounts have even been deactivated.<sup>174</sup> As a result, critics chastised Facebook for not even “playing by their own rules” and told the social network to “stop being total boobs.”<sup>175</sup>

## ENSURE THAT YOUR POLICIES APPLY EQUALLY TO ALL USERS.

Users will rightly be unhappy if they believe that some group or perspective is favored on your service. Avoid the appearance of favoritism by ensuring that you apply your policies consistently to all would-be speakers rather than subjecting certain viewpoints to particular scrutiny or catering to objections from certain groups.



**Twitter Bans Olympic Journalist for Heckling:** In 2012, Twitter faced allegations of preferential treatment of NBC, which had partnered with Twitter to promote the Olympics, after it encouraged NBC to complain about journalist Guy Adams’ tweets and then immediately suspended his account after NBC complained.<sup>176</sup> Although Twitter quickly apologized and reinstated Adams’ account, it still “found itself in a deeply unfamiliar situation: as the subject of one of the firestorms of indignation that characterises the platform, but which are usually directed at others.”<sup>177</sup>

## PROMOTE CREATIVITY: LET CUSTOMERS DECIDE HOW TO USE AND DISCUSS YOUR PRODUCT

Even if your business model involves selling or otherwise monetizing content, consider the costs and consequences of aggressively asserting your rights to control the use or distribution of that content, whether through legal or technological means. Encouraging your customers to use your content or service in new and innovative ways may attract more paying customers, while limiting your customers' ability to enjoy your service could drive them to less restrictive competitors.

### ➔ HAVE YOU CONSIDERED THE BENEFITS OF ENCOURAGING THE UNRESTRICTED USE AND DISTRIBUTION OF YOUR CONTENT OR PRODUCT?

Encouraging your fans to express their own creativity may draw more attention to your product and even lead to new strategies for generating revenue. Allowing and encouraging modifications, fan fiction, and other derivative works can support your user community—or even recruit a brand new user base around an adaption of your content or service.



**Fan Mod Pushes 3-Year-Old Video Game up the Charts:** Bohemia Interactive's ARMA II game was released in 2009, but the game achieved its greatest success in 2012 thanks to a zombie-themed modification ("mod") created by one of its players. The "Day-Z" mod "took the PC world by storm," turning the original game into a best seller.<sup>178</sup>

### ➔ DO YOU RESPECT FREE SPEECH IF YOU DO ASSERT CONTROL?

If you determine that you need to take action to prevent unauthorized use or distribution of content or information, ensure that you respect others' freedom of expression while you protect your own rights. Attempting to assert control without considering how the targets of your efforts and the general public might react can backfire badly, especially if your goal is to limit the distribution of sensitive information.

### USE INFORMAL CHANNELS TO OPEN DISCUSSIONS.

Before resorting to, or even threatening, legal action, contact the offending party and explain your concerns. You may be able to reach an amicable solution that serves the interests of both sides instead of winding up in a conflict that may not benefit anyone.

### CAREFULLY EVALUATE THE LEGAL BASIS FOR YOUR DEMANDS.

Do not attempt to control content or information about your company using legal claims that are unlikely to stand up in court. Doing so will not only cost you time and money, it may harm your reputation and even lead to countersuits.



**Apple "Bites the Fans that Feed It":** Apple was chastised by Forbes for "biting the fans that feed it" after trying to clamp down on blog posts about rumored upcoming products.<sup>179</sup> Apple's attempt to use legal methods to try to stifle conversation about its next-generation devices was shot down by the courts as well.<sup>180</sup>



**Viacom Demands Removal of Political Videos:** Downplaying the right to make “fair use” of copyrighted content led to a lawsuit and media firestorm for Viacom. The company sent Digital Millennium Copyright Act (DMCA) letters to YouTube in early 2007 demanding the removal of thousands of video clips that it claimed were infringing on its copyrighted material. Some of the clips taken down, including one produced by MoveOn.org, used copyrighted material for permitted purposes such as political commentary and parody.<sup>181</sup> Viacom conceded that it had erred in issuing the DMCA notice regarding MoveOn’s video and agreed to set up a website and email “hotline” to review any complaints within one business day and reinstate the video if the takedown request was improper.<sup>182</sup> However, many users and online video enthusiasts remain bitter toward the company for its actions.<sup>183</sup>

## MAKE IT EASY FOR RECIPIENTS TO RESPOND TO YOUR DEMANDS.

Give individuals and content hosts a quick and easy way to contest or respond to takedown requests, such as an email hotline. Such a service will allow mistakes and relationships to be repaired without costly litigation. If you send a takedown request to a third party, ask that links to these hotlines be posted in place of any removed content and be sent to the owner or poster of any removed content.

### ➔ HAVE YOU CONSIDERED THE COSTS AND RISKS OF LEGALLY ASSERTING CONTROL OVER YOUR CONTENT OR PRODUCT?

In many cases, although you might wish to limit the use or distribution of your intellectual property, using legal mechanisms to attempt to assert control may simply not be effective. Assess the likelihood of success and the consequences of failure before attempting to use legal or technical means to restrict use.

## CONSIDER THE POTENTIAL CONSEQUENCES OF ATTEMPTING TO REMOVE CONTENT FROM THE INTERNET.

Attempts to suppress speech often backfire, further fanning the flames of interest in the information that you were hoping to remove and resulting in significant damage to brands as well as loss of goodwill. Once information has been leaked to the Internet, it is very difficult to put the genie back into the bottle. Trying to do so may only keep the problem in the spotlight.



**Bank Julius Baer Turns “Secret” Documents into Public Spectacle:** Swiss bank Julius Baer ended up in the free speech hot seat and its leaked corporate documents received widespread attention when it tried to prevent the popular WikiLeaks site from distributing copies of these documents.<sup>184</sup> When the bank was able to obtain an initial court order disabling the WikiLeaks domain name, the incident attracted widespread press attention, the information was republished on many other Internet sites, and the ACLU and a number of other public interest groups opposed the bank’s efforts to squelch speech. Ultimately, the judge recognized the important free speech principles involved and dissolved the injunction, but not before the controversy—and the original documents—were broadcast worldwide.<sup>185</sup>

## ➔ HAVE YOU CAREFULLY CONSIDERED THE IMPLICATIONS OF PLACING TECHNOLOGICAL LIMITS ON YOUR USERS?

Although it might be tempting to use digital rights management (DRM) or filters that identify specific content to guard your intellectual property, poorly-deployed DRM or filters can hinder your users' ability to use and share your content legitimately, and can burden you with the obligation of maintaining your technology for years. Carefully weigh the costs and benefits of these tools and implement them in a way that minimizes the impact on free expression.

### CONSIDER THE LONG-TERM FINANCIAL COSTS.

The upfront costs of DRM are fairly obvious: the financial outlay and time spent on acquisition or implementation. The long-term costs are more difficult to measure. In some situations, you may be forced to choose between maintaining a distribution model or authentication system that you would rather abandon or facing outrage and even lawsuits from users who purchased content that is suddenly unusable. In addition, the administrative costs of maintaining DRM are likely to continue to grow.



**Google Forced to Repay Purchasers of Unusable Content:** In 2007 Google became the target of public outcry when it tried to close down its video service that incorporated DRM technology. Because users would have been unable to continue to use their previously purchased content once Google terminated the service, Google was forced to fully refund all payments for the service as well as keep the service active for an additional six months.<sup>186</sup>

### EVALUATE THE IMPACT ON YOUR USERS.

Users may be dissuaded from using your product or service if their freedom is constrained by DRM, especially if there is not enough "breathing space" to allow your customers to create new content or find new uses of your products or services that you never envisioned. In addition, user trust in your product may erode as customers realize that DRM is interfering with their expectations.

### ENSURE THAT ANY CONTROLS YOU USE CONFORM TO USER EXPECTATIONS.

If you use a filter to restrict the content that users are permitted to post or share, do everything in your power to minimize false positives that lead to blocking or removing legitimate content. Ensure that any automated system only identifies and blocks the desired content and avoids blocking content that may be legitimate.



**Amazon's Orwellian Mistake:** In 2009, Kindle users were furious when they discovered e-Books such as George Orwell's *1984* were removed from their Kindles without notice.<sup>187</sup> Amazon eventually explained that the deleted copies were improperly published in violation of copyright law and Amazon's own licensing agreements, but users were still outraged that Amazon "corrected" the issue in a way that "felt a bit like theft."<sup>188</sup> The lack of proper notice and explanation at the outset and the method of removal sparked a massive outcry and forced Amazon to change its policy and state that it would not "recall" even unauthorized copies.<sup>189</sup>

## SPEAK UP FOR FREE SPEECH: PROTECT YOUR USERS' FREEDOM OF EXPRESSION

To be a true champion of free speech, you need to do more than just allow users to express themselves on your platform or service—you need to affirmatively protect them from third parties that attempt to restrict their freedom of expression. Earning a reputation as a defender of your users' rights is a terrific way to build trust with your current users and recruit more.

### ➔ DO YOU SUPPORT YOUR USERS WHEN YOU RECEIVE DEMANDS TO TAKE DOWN THEIR CONTENT?

If your company hosts user-generated material, you may find yourself on the receiving end of a letter demanding that you remove material or disable a user account because of alleged copyright infringement. To protect your users and your reputation, develop a procedure to review the demand carefully and ensure that your users' free speech rights are respected.

### NOTIFY USERS WHEN A DEMAND TO REMOVE THEIR CONTENT IS RECEIVED.

Notify a user when you receive a request or demand to remove her content by posting information at the location where the content formerly appeared and by directly contacting the content creator. Include a copy of the demand and inform the user about her possible responses and your procedure for acting on such notices. Assist the user in contacting the content owner directly in order to request reconsideration of the demand.

In addition, consider publishing a document similar to Google's Transparency Report that tracks the number of demands you receive to take down or otherwise restrict user data.<sup>190</sup> Doing so can help your users better understand how your process works and what you do to defend their rights.

### ONLY REMOVE CONTENT THAT YOU ARE REQUIRED TO REMOVE.

Ensure that any demand to remove content is legally binding before removing any content. And don't overreact and infringe on protected speech by removing other content posted by the same user, cancel her account, or remove comments posted about a particular content item.

### TAKE YOUR USERS' RIGHTS INTO PROPER ACCOUNT.

Don't take down content that constitutes fair use or that is noncommercial, creative, and transformative in nature. In questionable cases, look for ways to support your users' rights without relinquishing your safe harbor protections. For more information, see [aclunc.org/tech/primer/resources](https://aclunc.org/tech/primer/resources).

### ➔ DO YOU PROTECT THE IDENTITIES OF ANONYMOUS AND PSEUDONYMOUS USERS?

Your users may have various reasons for keeping their identity private. You can encourage anonymous and pseudonymous speech on your service by joining your users in resisting efforts to unmask their identity. Doing so can earn you the lasting respect of your users, while failing to protect their identity can erode that trust and lead to additional consequences.



**Yahoo! Turns Over Dissident Identities to China:** The search engine and email giant was forced to settle multi-million dollar lawsuits,<sup>191</sup> grilled repeatedly during Congressional hearings,<sup>192</sup> and targeted by international protests<sup>193</sup> for turning over identifying information in 2006 about its users to the Chinese government. The Chinese government used these data to link users to pro-democracy activities and to imprison dissidents.

#### DISCLOSE USER INFORMATION ONLY WHERE REQUIRED BY LAW.

Thoroughly review any subpoenas or demands for information, ensure that they comply with proper legal process, and resist inappropriate or overbroad requests. Challenge requests on behalf of your users rather than complying by default, and when you do comply, provide only the information that you are required to disclose.



**Verizon Resists Demand for User Information:** In 2003, the Recording Industry Association of America obtained a subpoena ordering Verizon to reveal the identity of a subscriber who had allegedly used peer-to-peer software to share music online.<sup>194</sup> Verizon refused to comply with the subpoena and ultimately had the subpoena quashed on appeal, garnering praise for its commitment to user rights.<sup>195</sup>

#### GIVE USERS AN OPPORTUNITY TO DEFEND THEIR ANONYMITY.

If you receive a demand to unmask an anonymous user, immediately notify the user and inform her of her right to file a motion to quash the subpoena. Give the user as much time as possible to challenge the subpoena before turning over her identifying information.



**Twitter Stands Up for Political Critics:** In 2010 Twitter was applauded for standing up for two anonymous users who were frequent critics of Pennsylvania Attorney General and gubernatorial candidate Tom Corbett. When Twitter received a subpoena from Pennsylvania prosecutors seeking the identities of the users, it notified the users and gave them a chance to object rather than immediately complying with the demand.<sup>196</sup> The demand was withdrawn after the incident received substantial press coverage and the ACLU intervened.<sup>197</sup> Twitter emerged as one of the heroes of the story for giving its users an opportunity to defend their anonymity.

#### ➔ DO YOU ADVOCATE FOR LAWS THAT PROTECT YOUR USERS' FREEDOM OF EXPRESSION?

If the law doesn't adequately protect your users' freedom of expression, you can earn their gratitude by working to change the law. The courthouse and the legislature both offer opportunities for you to affect policy and establish yourself as a champion of freedom of expression.

#### FIGHT FOR YOUR USERS IN COURT.

When you receive a demand to remove or prohibit content or to disclose the identity of an anonymous user that seems to exceed the boundaries of the law, consider taking the opportunity to stand up for your users in court. The publicity and reputational benefits of doing so may greatly outweigh the costs.



**Facebook “Likes” Free Speech:** In early 2012, a Facebook user was fired by the Hampton, VA sheriff’s office for “liking” the Facebook page of the current sheriff’s election opponent.<sup>198</sup> After a federal district court judge ruled that “liking” something on Facebook was not speech protected by the First Amendment, Facebook submitted a brief to the Court of Appeals arguing otherwise.<sup>199</sup> The ACLU submitted a brief on the user’s behalf as well and joined those applauding Facebook for “support[ing] the free speech rights of its users.”<sup>200</sup>

**PUSH FOR LAWS AND POLICIES THAT PROTECT FREE SPEECH.**

Lawmakers often look to companies for guidance on how they can protect privacy and freedom of expression without hindering innovation. By advocating for strong laws and policies that protect individual rights, you can make it clear that freedom of expression and corporate success are fully compatible and earn the trust and loyalty of users.



**Google Slammed for Its “Betrayal” of Net Neutrality:** Google was pilloried for abruptly changing its position and abandoning support for many of the key tenets of net neutrality in August 2010.<sup>201</sup> Its joint recommendations with Verizon<sup>202</sup> “include[d] some really terrible ideas,”<sup>203</sup> such as excluding cellular networks from nondiscrimination requirements, that undermined Google’s previous reputation as an advocate of net neutrality.<sup>204</sup> Google was excoriated in the media as a “carrier-humping, net neutrality surrender monkey” whose “betrayal” could go down as “one of the most remarkable *volte-faces* in telecommunications policy history.”<sup>205</sup>

**OPPOSE LAWS AND POLICIES THAT UNDERMINE FREEDOM OF EXPRESSION.**

In addition to supporting positive steps, your company can make an impact by opposing laws and policies that would stifle free speech. Taking a stand to fight such laws and policies can protect both your own ability to innovate and thrive as a business and your users’ right to freedom of speech.



**Internet “Blackout” Helps Stop Anti-Piracy Bills:** The battle over two highly controversial 2012 Congressional bills, the Stop Online Privacy Act (SOPA) and the Protect Intellectual Property Act, was heavily influenced by the participation of over 7,000 websites in a “blackout.” The bills, nominally designed to combat copyright infringement, were described by critics as “damaging free speech, Internet security, and online innovation.”<sup>206</sup> Both bills were ultimately shelved, leading to the admiration of Internet users for the sites that stood up for freedom of expression.<sup>207</sup>



**Go Daddy’s Political Position Leads to Boycott:** In 2011, the domain registry company Go Daddy’s support of SOPA led many customers to take their business elsewhere. After losing 37,000 domain registrations in two days, the company ultimately withdrew its support for the bill, but its reversal is unlikely to undo the damage.<sup>208</sup>

SPEAK UP FOR  
FREE SPEECH

# CONCLUSION

Privacy and free speech incidents are now front-page news. This means that your company has the opportunity to be the hero of the story or to face public scorn, customer concern, and expensive lawsuits and government fines.

We hope the practical tips and case studies in this primer have helped you begin the process of building robust privacy and free speech protections into your services and business so you can properly protect the rights of your users and your company's bottom line. For additional resources to help you continue that process, please see the online version of this primer at [aclunc.org/tech/primer](https://aclunc.org/tech/primer) or contact us directly at [dotRights@aclunc.org](mailto:dotRights@aclunc.org).

# APPENDIX: THE LEGAL LANDSCAPE

The purpose of this primer is not to provide legal advice. However, it is important to understand the broad contours of the legal landscape so that you can proactively address areas where your products and business may intersect with free speech and privacy laws, including consulting with attorneys as needed. This appendix is intended to provide a brief survey of relevant laws to get you started. Additional resources, including white papers by the ACLU of Northern California on baking in privacy protections for cloud computing, location-based services, and digital books, can be found online at [aclunc.org/tech/primer/resources](https://aclunc.org/tech/primer/resources).

The laws governing privacy and free speech in the United States are set out in the United States Constitution, state constitutions, federal and state statutes, and regulations and orders by federal and state agencies. Businesses targeting international users may also be subject to the laws and regulations of the nations where their customers or users reside.

## PRIVACY LAWS & REGULATIONS

### CONSTRAINTS ON COLLECTING, USING, AND VOLUNTARILY SHARING INFORMATION

Federal law places restraints on the collection, use, and disclosure of certain forms of information, and the Federal Trade Commission enforces a prohibition against “unfair or deceptive” trade practices that include inaccurate or inadequate notice to users about privacy practices. State law, including several state constitutions, may impose additional restrictions on the collection, use, or disclosure of user information.

#### SECTOR-SPECIFIC FEDERAL PRIVACY LAWS

The United States does not have a comprehensive privacy law that applies to all types of data, users, and services. Instead, there are various laws that apply to specific types of information.

The broadest of these laws is the Electronic Communications Privacy Act (ECPA), which applies to any service that processes or stores electronic communications.<sup>209</sup> ECPA generally requires consent before any user information is voluntarily shared with a third party, and it prohibits unauthorized access to stored communications.

Various other laws apply to specific types of personal information:

- The Health Insurance Portability and Accountability Act applies to many services that are designed for health care providers and related entities.<sup>210</sup>
- The Video Privacy Protection Act applies to services engaged in the rental, sale, or delivery of recorded video content.<sup>211</sup>
- The Children’s Online Privacy Protection Act applies to websites and services that are “directed to children.”<sup>212</sup>
- Other laws may apply to services that handle financial records,<sup>213</sup> consumer credit information,<sup>214</sup> government records,<sup>215</sup> motor vehicle records,<sup>216</sup> or student education records.<sup>217</sup>

## FTC AND FCC REGULATION

The Federal Trade Commission (FTC) is empowered to regulate “unfair or deceptive” practices.<sup>218</sup> The FTC has interpreted this authority to include investigating online actors who fail to comply with their written privacy policies or whose services or policies mislead consumers.<sup>219</sup> In recent years, the FTC has increased its enforcement in the online space, bringing diverse actions against companies, including actions against Google and Facebook for failing to obtain users’ express consent before changing data practices.<sup>220</sup>

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite, and cable throughout the United States. It has been engaged in protecting consumer privacy for decades, beginning with the Communications Act of 1934 which charged the agency with implementing a number of privacy protection provisions.<sup>221</sup> In recent years, the FCC has drafted rules controlling the handling, use, and sharing of Customer Proprietary Network Information and has been exploring privacy issues related to mobile and location-based services.<sup>222</sup>

## STATE LAWS & REGULATIONS

Article I, section 1 of the California Constitution guarantees an “inalienable” right to privacy that is applicable with respect both to the government and private entities,<sup>223</sup> as do the constitutions of nine other states.<sup>224</sup> The Privacy Amendment, overwhelmingly passed by ballot proposition in 1972, was specifically intended to safeguard informational privacy by preventing the expansion of data collection and the potential misuse of that data by both the government and the private sector. State courts in Alaska, Hawaii, Louisiana, and Montana also have held that their state constitutions or common law include a right to information privacy applicable to private actors.<sup>225</sup>

Various states also have specific laws constraining the collection, use, or sharing of certain types of information. For example, California law prohibits publicly posting or displaying social security numbers or embedding them on a card<sup>226</sup> and swiping drivers’ licenses or recording driver’s license information<sup>227</sup> except for very limited circumstances, such as age verification or fraud control.

Other state agencies can also play an important role in defining and enforcing privacy rights. For example, the California Public Utilities Commission has taken an active role in defining privacy requirements for products and services such as smart energy meters.<sup>228</sup> And in 2012 the California Office of the Attorney General announced the creation of a Privacy Enforcement and Protection Unit focused on protecting consumer and individual privacy through enforcement and civil prosecution of state and federal privacy laws.<sup>229</sup>

## EUROPEAN UNION LAWS AND REGULATIONS

International regulators in Europe and elsewhere have also taken an active role in the privacy sphere. Of particular note for many companies are the existing Data Protection Directive and proposed privacy Regulation in the European Union.<sup>230</sup> The Regulation, which could take effect as soon as 2015 and which would apply directly to all EU member states (and thus potentially to all products or services targeting EU residents), demands “explicit” consent before the collection and use of personal information, requires companies to implement “Privacy by Design” and “Privacy by Default,” and provides individuals with the “Right to be Forgotten” and the “Right of Data Portability.”<sup>231</sup>

More detailed information on international laws and regulations is beyond the scope of this document; please consult an attorney to better understand the legal framework in any countries that your product or service is specifically targeting.

## TRANSPARENCY AND REPORTING REQUIREMENTS

Many of the sector-specific laws mentioned above have specific transparency and reporting requirements as well as collection, use, or sharing limitations. In addition, there are various other laws that require transparency in certain circumstances:

### CALIFORNIA ONLINE PRIVACY PROTECTION ACT

The California Online Privacy Protection Act (OPPA) requires that all California companies operating a commercial website post a conspicuous privacy policy on their site and disclose the kinds of personally identifiable data that they collect and share with third parties.<sup>232</sup> Companies must also clearly label their privacy statements, abide by their policies, inform consumers of processes to opt out of data sharing, and publish a date the policy goes into effect.

California Attorney General Kamala Harris has stated that OPPA also applies to mobile apps and has reached an agreement with several major mobile platforms to ensure that all apps include a privacy policy that is available to a potential user before the app is downloaded or installed.<sup>233</sup>

### OTHER STATE LAWS AND REGULATIONS

Various other state laws require notice or reporting under certain circumstances:

- Forty-six states, the District of Columbia, and several territories have laws that require users to be notified if their data is compromised.<sup>234</sup>
- California law empowers consumers to learn how their personal information is shared by companies and encourages companies to adopt simple methods for individuals to opt out of information sharing.<sup>235</sup>
- The California Reader Privacy Act requires companies that sell books or electronic equivalents to produce an annual report detailing the demands for user information received in a given year.<sup>236</sup>

## THIRD PARTY DEMANDS FOR USER INFORMATION

Although many users expect and believe that the letters, diaries, spreadsheets, photographs, videos, and other personal documents and materials that businesses encourage them to store online are as private as those stored in a file cabinet or on their computer's hard drive at home, the legal requirements for the government and third parties to demand access to these documents are uncertain. Courts have long struggled to interpret the U.S. and state constitutions in the light of evolving technology, with Justice Alito pointedly calling for legislative action in the recent Supreme Court case *United States v. Jones*.<sup>237</sup> Privacy laws at both the federal and state level are also becoming rapidly obsolete as technology outpaces the rate of legislative change.

### THE U.S. CONSTITUTION

The Fourth Amendment to the United States Constitution guarantees “[t]he right of the person to be secure . . . against unreasonable searches or seizures.”<sup>238</sup> Generally speaking, when an individual has a “reasonable expectation of privacy,” the government cannot search or seize this information without demonstrating probable cause and obtaining a warrant from a judge.<sup>239</sup> But the exact boundary of that reasonable expectation of privacy, particularly as applied to information collected by technological means and held by third parties, remains an unresolved question.

For example, courts are still addressing the applicability of the “third party doctrine,” which holds that an individual does not possess a reasonable expectation of privacy in records held by a third party, in the modern context. The third party doctrine was originally established in a pair of 1970s Supreme Court cases concerning the privacy of calling and banking records.<sup>240</sup> Modern courts faced with the question of whether the third party doctrine applies to electronic data held by a third party have reached divergent opinions: some courts have held that the contents of an email<sup>241</sup> or a person's location history<sup>242</sup> are constitutionally protected even if held by a third party, while others have held that the third party doctrine negates such protection.<sup>243</sup>

Similarly, courts have only begun to address the question of whether individuals retain a “reasonable expectation of privacy” in information that was at one time publicly available. While a recent Supreme Court case, *United States v. Jones*, did not directly answer that question, a majority of the justices expressed a willingness to consider whether long-term monitoring of a person’s location, even in public, violated the Fourth Amendment.<sup>244</sup> However, other courts have rejected the idea that information made publicly available still retains constitutional protection.<sup>245</sup>

## THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act (ECPA), including the Stored Communications Act, was enacted by Congress in part to address the third party doctrine and ensure that the privacy of electronic communications was safeguarded even if this information were held by a third party.<sup>246</sup> ECPA generally prohibits the voluntary disclosure of user communications and requires third parties to obtain a search warrant or court order to force such disclosure.

However, ECPA was enacted in 1986, and as a result was based on outdated understandings of communications technology. For example, the law was written around the expectation that users would download emails to personal computers and delete copies stored on a central server. In addition, the law did not anticipate new developments such as the collection and use of location information at all. As a result, courts have struggled to apply it to modern technology, frequently reaching different conclusions about the procedural requirements for demands for electronic communications while agreeing only that ECPA is part of “a confusing and uncertain area of the law.”<sup>247</sup>

## STATE CONSTITUTIONS AND LAWS

California is among 11 states that have rejected the third party doctrine and held that their state constitution provides protection for personal data held by third parties. These states use a variety of different standards to determine whether state officials can demand access to personal information held by a third party.<sup>248</sup>

State law, both constitutional and statutory, may place additional limitations on demands for specific types of information. For example, the California Reader Privacy Act requires a government entity to obtain a court order and meet additional criteria in order to compel disclosure of records related to books.<sup>249</sup>

# U.S. FREE SPEECH LAWS & REGULATIONS

## CONSTITUTIONAL PROTECTIONS FOR FREE SPEECH

### THE FIRST AMENDMENT

The First Amendment to the United States Constitution includes the rights of *freedom of speech* and *freedom of the press*.<sup>250</sup> It prevents the government from making any law that restricts either of these freedoms. It is important to note that the First Amendment also guarantees the right to *anonymous speech*, which the Supreme Court has found to be necessary for a democracy.<sup>251</sup>

### STATE CONSTITUTIONS

State constitutions may also provide an explicit right to freedom of expression. For example, Article I, section 2 of the California State Constitution guarantees that “every person may freely speak, write and publish his or her sentiments on all subjects” and that California laws “may not restrain or abridge liberty of speech.”<sup>252</sup> California courts have held that safeguarding free speech is a paramount concern because speech is “a freedom which is the matrix, the indispensable condition, of nearly every other form of freedom.”<sup>253</sup>

Although the First Amendment applies only to government actions that restrict individual rights, courts in California, New Jersey, Colorado, Massachusetts, and Puerto Rico have held that their state constitutional protection for freedom of expression may apply to *private actors* in certain circumstances.<sup>254</sup> For example, Californians enjoy free speech rights on private property, such as shopping malls, that is open to the public.<sup>255</sup> As of August 2012, these courts had not yet considered the implications of these decisions in the context of modern communications technology.

## THE FEDERAL COMMUNICATIONS COMMISSION

The FCC is also actively engaged in safeguarding free speech. In recent years, it has investigated the legality of cell phone disruption by government authorities<sup>256</sup> and drafted net neutrality rules that prohibit non-mobile network providers from blocking and “unreasonably” discriminating against network traffic and also place certain restrictions on discrimination by mobile networks.<sup>257</sup> The net neutrality rules remain in effect as of August 2012, although Verizon has challenged their legality in court.<sup>258</sup>

## COPYRIGHT AND FAIR USE

Because the First Amendment prohibits Congress from making laws that abridge freedom of speech, federal statutes that implicate rights to free expression must have a buffer to safeguard constitutional rights. The federal Copyright Act is a good example.<sup>259</sup> While copyright law provides a set of six exclusive, limited-time rights to copyright holders to serve as an incentive for them to create works, these rights are limited by the fair use doctrine that is delineated in section 107 of the Copyright Act. The fair use doctrine guarantees individuals the right to use copyrighted materials, without seeking a copyright holder’s permission, for activities such as parody, satire, criticism, news reporting, teaching, scholarship, research, and transformative works.<sup>260</sup> Fair use guarantees a “breathing space,” or buffer, that helps to reconcile the tension that would otherwise exist between copyright law and the First Amendment’s guarantee of freedom of expression.

## SAFE HARBORS

The First Amendment does have limits, and some speech—such as obscenity, slander and libel, or the proverbial “shouting ‘fire’ in a crowded theater”—is not constitutionally protected. However, many laws are written to ensure that while a speaker may face consequences for her speech, a platform that hosts her expression is able to protect itself from also being liable. Such “safe harbors” are intended to encourage the creation of platforms for speech by minimizing any requirement for platforms to censor or monitor users in ordinary circumstances.

## CDA SECTION 230

Section 230 of the Communications Decency Act (CDA) states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”<sup>261</sup> This section has been interpreted to immunize services that host user content from liability not only for obscenity (the domain of the broader CDA) but also for defamation and similar torts. However, this immunity may be lost if the provider is an active participant in the creation of the content.<sup>262</sup>

## DMCA SECTION 512

Section 512 of the Digital Millennium Copyright Act (DMCA) provides a service that hosts user-generated content with a safe harbor from liability under the DMCA if it complies with certain requirements.<sup>263</sup> Most notably, to claim safe harbor, a service that receives a DMCA notice-and-takedown letter must remove or block access to any allegedly infringing content.<sup>264</sup> The service may restore access to the content if the user provides a counter-notification asserting that the content is not in fact infringing. Again, this immunity may be lost if the service is aware of the infringing nature of hosted content.

# ENDNOTES

- 1 *Primer*, Dictionary.com, <http://dictionary.reference.com/browse/primer>.
- 2 Molly Wood, *Google Buzz: Privacy Nightmare*, CNet News, Feb. 10, 2010, [http://news.cnet.com/8301-31322\\_3-10451428-256.html](http://news.cnet.com/8301-31322_3-10451428-256.html).
- 3 Nancy Gohring, *EPIC Files Privacy Complaint Against Buzz*, ComputerWorld, Feb. 16, 2010, [http://www.computerworld.com/s/article/9157878/EPIC\\_files\\_privacy\\_complaint\\_against\\_Google\\_Buzz](http://www.computerworld.com/s/article/9157878/EPIC_files_privacy_complaint_against_Google_Buzz).
- 4 Chris Matyszczyk, *Google Gets Buzzed with Class Action Lawsuit*, CNet News, Feb. 17, 2010, [http://news.cnet.com/8301-17852\\_3-10455573-71.html](http://news.cnet.com/8301-17852_3-10455573-71.html).
- 5 Catharine Smith, *Google Buzz Gets the Ax, As Do Others in 'Fall Sweep'*, Huffington Post, Oct. 14, 2011, [http://www.huffingtonpost.com/2011/10/14/google-buzz-igoogole-fall-sweep\\_n\\_1011306.html](http://www.huffingtonpost.com/2011/10/14/google-buzz-igoogole-fall-sweep_n_1011306.html).
- 6 Cyrus Farivar, *Class-Action Lawsuit Forces Netflix Privacy Changes*, ars technica: Law & Disorder, July 30, 2012, <http://arstechnica.com/tech-policy/2012/07/class-action-lawsuit-settlement-forces-netflix-privacy-changes/>.
- 7 Lisa DiCarlo, *Apple Bites the Fans that Feed It*, Forbes, Jan. 7, 2005, [http://www.forbes.com/2005/01/07/cx\\_ld\\_0107apple.html](http://www.forbes.com/2005/01/07/cx_ld_0107apple.html).
- 8 Mark Hosenball, *Case Dismissed? The Secret Lobbying Campaign Your Phone Company Doesn't Want You to Know About*, Daily Beast: Newsweek, Sept. 19, 2007, <http://www.thedailybeast.com/newsweek/2007/09/19/case-dismissed.html>.
- 9 Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery, and Browser Hijacking (2008)*, available at [http://www.freepress.net/sites/default/files/fp-legacy/NebuAd\\_Report.pdf](http://www.freepress.net/sites/default/files/fp-legacy/NebuAd_Report.pdf).
- 10 Tom Cheredar, *Go Daddy Loses Over 37,000 Domains Due to SOPA Stance*, VentureBeat, Dec. 24, 2011, <http://venturebeat.com/2011/12/24/godaddy-domain-loss/>.
- 11 Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, Wash. Post, Nov. 30, 2007, [http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/11/29/AR2007112902503_pf.html).
- 12 Emma Barnett, *Twitter Chief: We Will Protect Our Users from Government*, Telegraph (UK), Oct. 18, 2011, <http://www.telegraph.co.uk/technology/twitter/8833526/Twitter-chief-We-will-protect-our-users-from-Government.html>.
- 13 Tom Zeller Jr., *Qwest Goes from the Goat to the Hero*, N.Y. Times, May 15, 2006, <http://www.nytimes.com/2006/05/15/technology/15link.html>.
- 14 *See Session Transcript: Allison Cerra, Vice President, Communications & Public Affairs; CMO Americas, Alcatel-Lucent*, Argyle Journal Beta, Feb. 13, 2012 (transcript of 2012 CMO Leadership Forum presentation, Jan. 19, 2012).
- 15 Catherine Tucker, *Social Networks, Personalized Advertising, and Privacy Controls* (NEI Institute Working Paper No. 10-07, 2011), Apr. 2011, available at <http://pages.stern.nyu.edu/~atakos/ResearchCamp/ctuckerpaper.pdf>.
- 16 David Navetta and Nicole Friess, *"Privacy by Design": A Key Concern for VS and Start-Ups*, Info. Law Group, May 23, 2011, <http://www.infolawgroup.com/2011/05/articles/privacy-law/privacy-by-design-a-key-concern-for-vcs-and-startups/>.
- 17 TRUSTe, *2012 TRUSTe US Consumer Data Privacy Survey*, <http://www.truste.com/us-consumer-data-privacy-study/>.
- 18 Google Transparency Report, <http://www.google.com/transparencyreport/userdatarequests/>.
- 19 Jan Lauren Boyles et al., *Pew Internet & American Life Project, Privacy and Data Management on Mobile Devices 2* (Sep. 5, 2012), [http://pewinternet.org/~/media/Files/Reports/2012/PIP\\_MobilePrivacyManagement.pdf](http://pewinternet.org/~/media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf).
- 20 *See Calum MacDonald, Google's Street View Site Raises Alarm over Privacy*, Scotland Herald, June 4, 2007, <http://www.heraldscotland.com/google-s-street-view-site-raises-alarm-over-privacy-1.859078>; *Street View Under Fire in Japan*, BBC News, May 14, 2009, <http://news.bbc.co.uk/2/hi/8049490.stm>.
- 21 Robert McMillan, *Lawsuits over Google Wi-Fi Sniffing Pile On*, InfoWorld, June 4, 2010, <http://www.infoworld.com/d/the-industry-standard/lawsuits-over-google-wi-fi-sniffing-pile-135>.
- 22 Chloe Albanesius, *Canada Begins Google Wi-Fi Investigation*, PCMag.com, June 2, 2010, <http://www.pcmag.com/article2/0,2817,2364547,00.asp>; Curt Hopkins, *Australia Latest Country to Investigate Google*, ReadWriteWeb, June 6, 2010, [http://www.readwriteweb.com/archives/australia\\_latest\\_country\\_to\\_investigate\\_google.php](http://www.readwriteweb.com/archives/australia_latest_country_to_investigate_google.php); Peter Sayer, *Google Street View Faces Investigation in France and Italy*, Macworld, May 19, 2010, [http://www.macworld.com/article/1151356/google\\_streetview.html](http://www.macworld.com/article/1151356/google_streetview.html); Kevin J. O'Brien, *Germany Investigates Google's Data Collecting*, N.Y. Times, May 19, 2010, <http://www.nytimes.com/2010/05/20/business/global/20google.html>.
- 23 Alan Eustace, *WiFi Data Collection: An Update*, Google Official Blog, May 14, 2010 (updated June 9, 2010), <http://googleblog.blogspot.co.uk/2010/05/wifi-data-collection-update.html>.
- 24 Mathew J. Schwartz, *Google Street View Pursued Wardriving by Design*, Info. Week, Apr. 30, 2012, <http://www.informationweek.com/security/privacy/google-street-view-pursued-wardriving-by/232901164>.
- 25 Ben Kersey, *Google Street View Privacy Case Reopened in UK*, SlashGear, June 13, 2012, <http://www.slashgear.com/google-street-view-privacy-case-reopened-in-uk-13233683/>.
- 26 Jason D. O'Grady, *Path Discovered Phoning Home with Your Address Book*, ZDNet, Feb. 7, 2012, <http://www.zdnet.com/blog/apple/path-discovered-phoning-home-with-your-address-book/12182>.
- 27 Arum Thampi, *Path Uploads Your Entire iPhone Address Book to Its Servers*, Feb. 8, 2012, <http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html#comment-432202082> (comment of Dave Morin, Co-Founder and CEO of Path); Dave Morin, *We Are Sorry*, Feb. 8, 2012, <http://blog.path.com/post/17274932484/we-are-sorry>.
- 28 Mike Isaac, *Path CEO: "We Thought We Were Doing This Right,"* Gadget Lab, Feb. 8, 2012, <http://www.wired.com/gadgetlab/2012/02/path-dave-morin-explains-data/>.
- 29 Meghan Kelly, *Path, Apple, Facebook Named in Mobile Privacy Class-Action Lawsuit*, VentureBeat, Mar. 17, 2012, <http://venturebeat.com/2012/03/17/apple-address-book-lawsuit/>.
- 30 Alasdair Allan, *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>.

- 31 See Rip Emerson, *The Mobile Privacy Hearings: Senators Prod, Apple and Google Defend*, TechCrunch, May 12, 2011, <http://techcrunch.com/2011/05/12/the-mobile-privacy-hearings-senators-prod-apple-and-google-defend/>; Ed Silverstein, *U.S. Senate to Hold Second Hearing on Mobile Privacy Issues*, TMCnet, May 17, 2011, <http://www.tmcnet.com/topics/articles/175807-us-senate-hold-second-hearing-mobile-privacy-issues.htm>; FCC, *FTC Ask Apple, Google to Visit Forum on Mobile Location*, electronista, May 17, 2011, <http://www.electronista.com/articles/11/05/17/fcc.and.ftc.to.hold.mobile.location.forum/>; Karen Gullo, *Apple Accused in Suit of Tracking iPad, iPhone User Location*, Bloomberg, Apr. 25, 2011, <http://www.bloomberg.com/news/2011-04-25/apple-accused-in-suit-of-tracking-ipad-iphone-user-location-1-.html>.
- 32 Miguel Helft, *Jobs Says Apple Made Mistakes*, N.Y. Times, Apr. 27, 2011, <http://www.nytimes.com/2011/04/28/technology/28apple.html>.
- 33 See Ernesto, *How Long Does Your ISP Store IP-Address Logs?*, TorrentFreak, June 29, 2012, <http://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/>.
- 34 Andy Greenberg, *CEO of Internet Provider Sonic.net: We Delete User Logs After Two Weeks. Your Internet Provider Should, Too.*, Forbes, June 6, 2012, <http://www.forbes.com/sites/andygreenberg/2012/06/22/ceo-of-internet-provider-sonic-net-we-delete-user-logs-after-two-weeks-your-internet-provider-should-too/>.
- 35 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012).
- 36 U.S. Dep't Health & Human Services, *Who Must Comply with HIPAA Privacy Standards*, Dec. 19, 2002, <http://www.hhs.gov/hipaafaq/about/190.html>.
- 37 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012).
- 38 Children's Online Privacy Protect Act of 1998, 15 U.S.C. §§ 6501–6506 (2012).
- 39 Right to Financial Privacy Act, 12 U.S.C. §§ 3401 et seq. (2012); see also Electronic Privacy Information Center, *Right to Financial Privacy Act*, <http://epic.org/privacy/rfpa/>.
- 40 Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81u (2012); see also Electronic Privacy Information Center, *The Fair Credit Reporting Act and the Privacy of Your Credit Report*, <http://epic.org/privacy/fcra/>.
- 41 Privacy Act of 1974, 5 U.S.C. § 552a (2012).
- 42 Drivers Privacy Protection Act, 18 U.S.C. §§ 2721–25 (2012); see also Electronic Privacy Information Center, *The Drivers Privacy Protection Act and the Privacy of Your State Motor Vehicle Record*, <http://epic.org/privacy/drivers/>.
- 43 Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
- 44 Matt Jerzemy, *FTC Urges Apps for Kids Must Disclose Data-Collecting Practices*, Wall St. J.: Digits, Feb. 16, 2012, <http://blogs.wsj.com/digits/2012/02/16/ftc-urges-apps-for-kids-must-disclose-data-collecting-practices/>.
- 45 Press Release, Federal Trade Commission, *Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule*, Aug. 15, 2011, <http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm>.
- 46 Andrew Serwin & Tina Stow, *The Eye of the Beholder: Operationalizing Privacy by Design Through the Power of Consumer Choice* (July 2012), available at [http://www.apcoworldwide.com/content/pdfs/apco\\_privacy\\_study\\_report.pdf](http://www.apcoworldwide.com/content/pdfs/apco_privacy_study_report.pdf).
- 47 Tom Krazit, *How Blippy Users' Credit Cards Got into Google*, CNet News, Apr. 23, 2010, [http://news.cnet.com/8301-30684\\_3-20003332-265.html](http://news.cnet.com/8301-30684_3-20003332-265.html).
- 48 *Blippy Issues, Resolutions, Plan*, Apr. 26, 2010, <http://blog.blippy.com/2010/04/26/blippy-issues-resolutions-plan/>.
- 49 Nicholas Carlson, *Warning: Blippy User's Debit Card Numbers Still Appearing in Google*, Bus. Insider, Apr. 24, 2010, [http://articles.businessinsider.com/2010-04-24/tech/29974853\\_1\\_blippy-card-google-representative](http://articles.businessinsider.com/2010-04-24/tech/29974853_1_blippy-card-google-representative).
- 50 See Electronic Frontier Foundation, *Best Practices for Online Service Providers*, June 2008, <http://www.eff.org/wp/osp>; Alissa Cooper, *A Survey of Query Log Privacy-Enhancing Techniques from a Policy Perspective*, 2(4) ACM TRANS. WEB (Oct. 2008), <http://cdt.org/privacy/10012008acooper.pdf>.
- 51 Michael Arrington, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch, Aug. 6, 2006, <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>.
- 52 Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. Times, Aug. 9, 2006, <http://www.nytimes.com/2006/08/09/technology/09aol.html>.
- 53 Michelle Kessler & Kevin Maney, *AOL's Tech Chief Quits After Breach of Privacy*, USA Today, Aug. 21, 2006, [http://www.usatoday.com/tech/news/Internetprivacy/2006-08-21-aol-privacy-departures\\_x.htm](http://www.usatoday.com/tech/news/Internetprivacy/2006-08-21-aol-privacy-departures_x.htm).
- 54 Ca. Civil Code § 1798.81 (2012).
- 55 Federal Trade Commission, *Protecting Personal Information—A Guide for Business* (2009), <http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/>.
- 56 Jason Fitzpatrick, *Firesheep Sniffs Out Facebook and Other User Credentials on Wi-Fi Hotspots*, LifeHacker, Oct. 25, 2010, <http://lifelifehacker.com/5672313/sniff-out-user-credentials-at-wi-fi-hotspots-with-firesheep>.
- 57 Mathew J. Schwartz, *LinkedIn Users: Change Password Now*, Info. Week, June 6, 2012, <http://www.informationweek.com/security/attacks/linkedin-users-change-password-now/240001623>.
- 58 Nicole Perloth, *Lax Security at LinkedIn Is Laid Bare*, N.Y. Times, June 10, 2012, <http://www.nytimes.com/2012/06/11/technology/linkedin-breach-exposes-light-security-even-at-data-companies.html>.
- 59 KPMG Consumers And Convergence IV, *Convergence Goes Mainstream: Convenience Edges Out Consumer Concern 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>.
- 60 Owen Thomas, *Why Facebook Employees Are Profiling Users*, Valleywag, Oct. 29, 2007, <http://valleywag.com/tech/your-privacy-is-an-illusion/why-facebook-employees-are-profiling-users-316469.php>.
- 61 Chris Morran, *Report: Citi Knew About Credit Card Hack for Weeks Before Going Public*, Consumerist, June 13, 2011, <http://consumerist.com/2011/06/report-citi-knew-about-credit-card-hack-for-weeks-before-going-public.html>.

- 62 Nelson D. Schwartz and Eric Dash, *Thieves Found Citigroup Site an Easy Entry*, N.Y. Times, June 13, 2011, <http://www.nytimes.com/2011/06/14/technology/14security.html>.
- 63 Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Mar. 2012), available at <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.
- 64 David Worthington, *Microsoft Focuses on Security Development Lifecycle*, SD Times, Sept. 25, 2008, <http://www.sdtimes.com/link/32894>.
- 65 David Bank, *Cisco Tries to Squelch Claim About a Flaw in Its Internet Routers*, Wall St. J., July 28, 2005, [http://online.wsj.com/public/article/SB112251394301198260-2zgDRmLtWgPF5vKgFn1qYJBjaGO\\_20050827.html](http://online.wsj.com/public/article/SB112251394301198260-2zgDRmLtWgPF5vKgFn1qYJBjaGO_20050827.html).
- 66 George Ou, *Is Cisco Killing Their Own Reputation?* ZDNet: Real World IT, Aug. 1, 2005, <http://blogs.zdnet.com/Ou/?p=85>.
- 67 National Conference of State Legislatures, *State Security Breach Notification Laws*, <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.
- 68 See *States Demand ChoicePoint Notify ID Theft Victims*, Consumer Affairs, Feb. 17, 2005, [http://www.consumeraffairs.com/news04/2005/choicepoint\\_states.html](http://www.consumeraffairs.com/news04/2005/choicepoint_states.html); Robert Lemos, *ChoicePoint Data Loss May Be Higher Than Reported*, CNet News, Mar. 10, 2005, [http://news.cnet.com/ChoicePoint-data-loss-may-be-higher-than-reported/2100-1029\\_3-5609253.html](http://news.cnet.com/ChoicePoint-data-loss-may-be-higher-than-reported/2100-1029_3-5609253.html) ("At first, the company only notified some 35,000 California residents as required by law in that state. After a public outcry for more information, the company notified 110,000 U.S. citizens whose records were improperly accessed.")
- 69 Audrey Watters, *Almost 1 Month Later, Sony Playstation Network Coming Back on Line*, ReadWriteWeb, May 14, 2011, [http://www.readwriteweb.com/archives/almost\\_1\\_month\\_later\\_sony\\_playstation\\_network\\_comi.php](http://www.readwriteweb.com/archives/almost_1_month_later_sony_playstation_network_comi.php).
- 70 Ian Sherr, *Hackers Breach Second Sony Service*, Wall St. J., May 2, 2011, <http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html>.
- 71 Nate Anderson, *House Hearing Blasts Sony's "Half-Hearted, Half-Baked" Hack Response*, Ars Technica: Law & Disorder, May 4, 2011, <http://arstechnica.com/tech-policy/2011/05/house-hearing-blasts-sonys-half-hearted-half-baked-hack-response/>.
- 72 Erica Ogg, *Sony Sued for Playstation Network Data Breach*, CNet News, Apr. 27, 2011, [http://news.cnet.com/8301-31021\\_3-20057921-260.html](http://news.cnet.com/8301-31021_3-20057921-260.html).
- 73 Ca. Bus. & Prof. Code § 22575 (2012).
- 74 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & Pol'y for Info. Soc. 3, [http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor\\_Formatted\\_Final.pdf](http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf).
- 75 Privacy, <http://duckduckgo.com/privacy.html>.
- 76 Robin Wauters, *Union Square Ventures, Others Invest in Alternative Search Engine DuckDuckGo*, TechCrunch, Oct. 13, 2011, <http://techcrunch.com/2011/10/13/union-square-ventures-invests-in-alternative-search-engine-duckduckgo/>.
- 77 PrivacyVille, <http://company.zynga.com/about/privacy-center/privacyville>.
- 78 Pascal-Emmanuel Gobry, *Zynga's Latest Gimmick Is Actually a Really Good Idea*, Bus Insider, July 8, 2011, <http://www.businessinsider.com/zyngas-latest-gimmick-is-actually-a-really-good-idea-2011-7>.
- 79 See HearUsNow.org, *Consumer Comments to the NTIA on "Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct"*, Apr. 2, 2012, <http://hearusnow.org/document/consumer-comments-to-the-national-telecommunications-and-information-administration-on-multistakeholder-process-to-develop-consumer-data-privacy-codes-of-conduct>.
- 80 See Press Release, State of California Department of Justice Office of the Attorney General, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, Feb. 22, 2012, <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.
- 81 Edward Wyatt, *F.T.C. Charges Myspace with Breaking U.S. Law in Sharing Users' Personal Information*, N.Y. Times, May 8, 2012, <http://www.nytimes.com/2012/05/09/technology/myspace-agrees-to-privacy-controls.html>.
- 82 Joseph Turov et al., *Americans Reject Tailored Advertising and the Three Activities that Enable It* (Sept. 2009), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1478214](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214).
- 83 Google Transparency Report, <http://www.google.com/transparencyreport/>.
- 84 Chris Conley, *Google's New Transparency Tool: A Window into Government Surveillance*, ACLU Blog of Rights, Apr. 20, 2010, <http://www.aclu.org/blog/technology-and-liberty/googles-new-transparency-tool-window-government-surveillance>.
- 85 See Jeremy Kessel, *Twitter Transparency Report*, July 2, 2012, <http://blog.twitter.com/2012/07/twitter-transparency-report.html>.
- 86 Jesus Diaz, *Your Android Phone Is Secretly Recording Everything You Do*, Gizmodo, Nov. 30, 2011, <http://gizmodo.com/5863849/your-android-phone-is-secretly-recording-everything-you-do>.
- 87 Chris Velazco, *Android Researcher Hit with C&D After Dissecting Monitoring Software*, TechCrunch, Nov. 22, 2011, <http://techcrunch.com/2011/11/22/android-researcher-hit-with-cd-after-dissecting-monitoring-software/>.
- 88 David Kravets, *Carrier IQ Admits Holding "Treasure Trove" of Consumer Data, but No Keystrokes*, Wired: Threat Level, Dec. 2, 2011, <http://www.wired.com/threatlevel/2011/12/carrier-iq-data-vacuum/all/1>.
- 89 Andy Greenberg, *And Now, the Lawsuits: Class Actions Hit Carrier IQ, HTC and Samsung*, Forbes, Dec. 2, 2011, <http://www.forbes.com/sites/andygreenberg/2011/12/02/and-now-the-lawsuits-class-actions-hit-carrier-iq-htc-and-samsung/>.
- 90 Andy Greenberg, *Here's The Letter Senator Al Franken Just Sent To Phone 'Rootkit' Firm Carrier IQ*, Forbes, Dec. 1, 2011, <http://www.forbes.com/sites/andygreenberg/2011/12/01/heres-the-letter-senator-al-franken-just-sent-to-phone-rootkit-firm-carrier-iq/>.
- 91 Nate Anderson, *Charter Delays NebuAd Rollout After Outcry*, Ars Technica, June 25, 2008, <http://arstechnica.com/uncategorized/2008/06/charter-delays-nebuad-rollout-after-outcry/>.
- 92 Adam Liptak, *Court Leaves the Door Open for Safety System Wiretaps*, N.Y. Times, Dec. 21, 2003, <http://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html>.
- 93 Drew Grant, *Etsy's Social Media DIY-saster*, Salon, Mar. 15, 2011, [http://www.salon.com/2011/03/15/etsy\\_privacy\\_people\\_search/](http://www.salon.com/2011/03/15/etsy_privacy_people_search/).
- 94 Cory Doctorow, *Etsy's Privacy Valdez: Opt-Out Policy Exposes Users' Real Names and Purchase Histories – Updated*, BoingBoing, Mar. 15, 2011, <http://boingboing.net/2011/03/15/etsys-privacy-valdez.html>.

- 95 Jacqui Cheng, *Etsy Reacts to User Outrage, Makes Changes to Feedback System*, Ars Technica: Ministry of Innovation, Mar. 15, 2011, <http://arstechnica.com/business/2011/03/etsy-reacts-to-user-outrage-makes-changes-to-feedback-system/>.
- 96 Doctorow, *supra* note 94.
- 97 Chris Conley, *Is Facebook Having Another Privacy Disconnect?*, ACLU Blog of Rights, Apr. 21, 2010, <http://www.aclu.org/blog/technology-and-liberty/facebook-having-another-privacy-disconnect>.
- 98 *Angry Facebook Users Rip 'Opt-Out' Privacy for 3rd-Party Sites*, eCreditDaily, Apr. 30, 2010, <http://ecreditdaily.com/2010/03/angry-facebook-users-rip-optout-privacy-3rdparty-sites/>.
- 99 Michael Liedtke, *Facebook's Expansion Triggers Political Backlash*, Sydney Morning Herald (AU), Apr. 27, 2010, <http://news.smh.com.au/breaking-news-technology/facebook-expansion-triggers-political-backlash-20100427-tprc.html>.
- 100 Chris Conley, *Facebook Addresses Several Privacy Problems*, Bytes & Pieces, May 26, 2010, [https://www.aclunc.org/issues/technology/blog/facebook\\_addresses\\_several\\_privacy\\_problems.shtml](https://www.aclunc.org/issues/technology/blog/facebook_addresses_several_privacy_problems.shtml).
- 101 Jim Dalrymple, *Mozilla CEO Criticizes Apple's Stealth Safari Update*, PCWorld, Mar. 22, 2008, [http://www.pcworld.com/article/143752/mozilla\\_ceo\\_criticizes\\_apples\\_stealth\\_safari\\_update.html](http://www.pcworld.com/article/143752/mozilla_ceo_criticizes_apples_stealth_safari_update.html).
- 102 Paul McDougall, *Apple Ends Stealth Safari Installs via Software Update for Windows*, Info. Week, Apr. 18, 2008, <http://www.informationweek.com/news/internet/browsers/showArticle.jhtml?articleID=207400701>.
- 103 Ken Walters, *Online Consumers Willing to Pay for Privacy*, Carnegie Mellon U. Blog, July 7, 2011, <http://www.cmu.edu/news/blog/2011/Summer/paying-for-privacy.shtml>.
- 104 Ca. Civil Code § 1798.83 (2012).
- 105 See Data Liberation Front, <http://www.dataliberation.org/>.
- 106 Frequently Asked Questions, <http://www.dataliberation.org/home/faq>.
- 107 J.R. Raphael, *Meet Google's 'Data Liberation Front'*, PCWorld, Sept. 14, 2009, [http://www.pcworld.com/article/171966/meet\\_google\\_data\\_liberation\\_front.html](http://www.pcworld.com/article/171966/meet_google_data_liberation_front.html).
- 108 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.htm](http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.htm).
- 109 Press Release, Federal Trade Commission, *FTC Accepts Final Settlement with Online Advertiser Scan Scout, Which Allegedly Used Flash Cookies to Track Consumers*, Dec. 21, 2011, <http://www.ftc.gov/opa/2011/12/scanscout.shtml>.
- 110 Matt O'Donnell, *AOL, Brightcove & ScanScout Online Tracking Class Action Lawsuit*, Top Class Actions, Aug. 24, 2011, <http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1334-aol-brightcove-a-scanscout-online-tracking-class-action-lawsuit>.
- 111 Press Release, Federal Trade Comm'n, *Google Will Pay \$22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, Aug. 9, 2012, <http://ftc.gov/opa/2012/08/google.shtml>.
- 112 Peter Pachal, *Google's Safari Tracking: Here Come the Lawsuits*, Mashable, Feb. 22, 2012, <http://mashable.com/2012/02/22/google-sued-over-safari-tracking/>.
- 113 Julia Angwin & Jennifer Valentino-DeVries, *Google's iPhone Tracking*, Wall St. J., Feb. 17, 2012, [online.wsj.com/article\\_email/SB10001424052970204880404577225380456599176-IMyQjAxMTAyMDEwNjExNDYyWj.html](http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-IMyQjAxMTAyMDEwNjExNDYyWj.html).
- 114 David Kravets, *FTC Dings Google \$22.5M in Safari Cookie Flap*, Wired: Threat Level, Aug. 9, 2012, <http://www.wired.com/threatlevel/2012/08/ftc-google-cookie/>; Peter Eckersley et al., *Google Circumvents Safari Privacy Protections—This Is Why We Need Do Not Track*, Deeplinks, Feb. 16, 2012, <https://www.eff.org/deeplinks/2012/02/time-make-amends-google-circumvents-privacy-settings-safari-users>.
- 115 Joseph Turow et al., *Americans Reject Tailored Advertising and the Three Activities that Enable It* (Sept. 2009), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1478214](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214).
- 116 Michael Liedtke, *Netflix Class Action Settlement: Service Pays \$9 Million After Allegations of Privacy Violations*, Huffington Post, Feb. 10, 2012, [http://www.huffingtonpost.com/2012/02/11/netflix-class-action-settlement\\_n\\_1270230.html](http://www.huffingtonpost.com/2012/02/11/netflix-class-action-settlement_n_1270230.html).
- 117 Maria Aspan, *How Sticky Is Membership on Facebook? Just Try Breaking Free*, N.Y. Times, Feb. 11, 2008, <http://www.nytimes.com/2008/02/11/technology/11facebook.html>.
- 118 See, for example, *Delete, Cancel and Terminate Facebook Account and Profile*, My Digital Life, Nov. 4, 2007, <http://www.mydigitallife.info/delete-cancel-and-terminate-facebook-account-and-profile/>.
- 119 See *How Do I Delete My Account*, <https://www.facebook.com/help/?faq=224562897555674>.
- 120 Kashmir Hill, *Fitbit Moves Quickly After Sex Stats Exposed*, Forbes, July 5, 2011, <http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/>.
- 121 Ian Paul, *Girls Around Me App Voluntarily Pulled After Privacy Backlash*, PCWorld, Apr. 2, 2012, [http://www.pcworld.com/article/252996/girls\\_around\\_me\\_app\\_voluntarily\\_pulled\\_after\\_privacy\\_backlash.html](http://www.pcworld.com/article/252996/girls_around_me_app_voluntarily_pulled_after_privacy_backlash.html).
- 122 John Brownlee, *Our Story Got Foursquare to Kill API Access to Creepy Stalking App Girls Around Me [Update: Facebook Responds]*, Cult of Mac, Mar. 30, 2012, <http://www.cultofmac.com/157793/foursquare-kills-api-access-to-creepy-stalking-app-girls-around-me-exclusive/>.
- 123 Melissa Knowles, *Outrage over Alleged Stalker App 'Girls Around Me'*, Yahoo! News: Trending Now, Apr. 4, 2012, <http://news.yahoo.com/blogs/trending-now/outrage-over-alleged-stalker-app-girls-around-180950609.html>.
- 124 Molly Wood, *Google Buzz: Privacy Nightmare*, CNet News, Feb. 10, 2010, [http://news.cnet.com/8301-31322\\_3-10451428-256.html](http://news.cnet.com/8301-31322_3-10451428-256.html).
- 125 Chris Morran, *Google Buzz Makes Private Contact Info Public*, Consumerist, Feb. 11, 2010, <http://consumerist.com/2010/02/google-buzz-makes-private-contact-info-public.html>.
- 126 Nancy Gohring, *EPIC Files Privacy Complaint Against Google Buzz*, ComputerWorld, Feb. 16, 2010, [http://www.computerworld.com/s/article/9157878/EPIC\\_files\\_privacy\\_complaint\\_against\\_Google\\_Buzz](http://www.computerworld.com/s/article/9157878/EPIC_files_privacy_complaint_against_Google_Buzz).
- 127 Tom Krazit, *Google Settles Buzz Lawsuit for \$8.5M*, CNet News, Sept. 3, 2010, [http://news.cnet.com/8301-30684\\_3-20015620-265.html](http://news.cnet.com/8301-30684_3-20015620-265.html).
- 128 Catharine Smith, *Google Buzz Gets the Ax, As Do Others in 'Fall Sweep'*, Huffington Post, Oct. 14, 2011, [http://www.huffingtonpost.com/2011/10/14/google-buzz-igoogole-fall-sweep\\_n\\_1011306.html](http://www.huffingtonpost.com/2011/10/14/google-buzz-igoogole-fall-sweep_n_1011306.html).
- 129 Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on the Books and on the Ground*, 61 Stan. L. Rev. 247, 270 (2011).



- 163 Alina Tugend, *Typing in an E-Mail Address, and Giving Up Your Friends' As Well*, N.Y. Times, June 19, 2009, <http://www.nytimes.com/2009/06/20/technology/internet/20shortcuts.html>.
- 164 Sean Gregory, *Tagged: The World's Most Annoying Website*, Time, June 11, 2009, <http://www.time.com/time/business/article/0,8599,1903810,00.html>.
- 165 Benny Evangelista, *SF District Attorney Tags Tagged.com with \$650,000 Settlement*, S.F. Chron.: Tech Chron., Apr. 4, 2010, <http://blog.sfgate.com/techchron/2010/04/12/sf-district-attorney-tags-tagged-com-with-650000-settlement/>.
- 166 Violet Blue, *PayPal Strong-Arms Indie Ebook Publishers over Erotic Content*, ZDNet: Pulp Tech, Feb. 27, 2012, <http://www.zdnet.com/blog/violetblue/paypal-strong-arms-indie-ebook-publishers-over-erotic-content/1097>.
- 167 See Suw Charman-Anderson, *Credit Card Companies Should Process Payments Not Censor Content*, Forbes, Mar. 9, 2012, <http://www.forbes.com/sites/suwcharmananderson/2012/03/09/credit-card-companies-should-process-payments-not-censor-content/>.
- 168 Nick McCann, *PayPal Narrows Boycott of 'Obscene' Publishers*, Courthouse News Serv., Mar. 14, 2012, <http://www.courthousenews.com/2012/03/14/44701.htm>.
- 169 David Kravets, *San Francisco Subway Shuts Cell Service to Foil Protest; Legal Debate Ignites*, Wired: Threat Level, Aug. 15, 2011, <http://www.wired.com/threatlevel/2011/08/subway-internet-shuttering/>.
- 170 Matthew Lasar, *FCC to Probe San Francisco Subway Cell Phone "Interruption" Policy*, Ars Technica: Law & Disorder, Dec. 2, 2011, <http://arstechnica.com/tech-policy/2011/12/fcc-to-probe-san-francisco-subway-cell-phone-interruption-policy/>.
- 171 Cell Service Interruption Policy, [http://www.bart.gov/docs/final\\_CSIP.pdf](http://www.bart.gov/docs/final_CSIP.pdf).
- 172 Jacqui Cheng, *Twitter's Controversy over Terms of Service (Updated)*, Ars Technica: Law & Disorder, May 26, 2008, <http://arstechnica.com/tech-policy/2008/05/twitters-controversy-over-terms-of-service/>.
- 173 Mikaela Conley, *Breastfeeding Advocates Protest Facebook with Nurse-In*, ABC Good Morning America, Feb. 8, 2012, <http://abcnews.go.com/Health/breastfeeding-advocates-hold-facebook-protest/story?id=15530012#.UDghttZIR1w>.
- 174 Emil Protalinski, *Facebook Clarifies Breastfeeding Photo Policy*, ZDNet: Friending Facebook, Feb. 7, 2012, <http://www.zdnet.com/blog/facebook/facebook-clarifies-breastfeeding-photo-policy/8791>.
- 175 Josh Wolford, *Facebook Continues to Yank Breastfeeding Photos*, WebProNews, Feb. 20, 2012, <http://www.webpronews.com/facebook-continues-to-yank-breastfeeding-photos-2012-02>; Alicia Eler, *Facebook Bans Breast-Feeding Photos*, ReadWriteWeb, Feb. 6, 2012, [http://www.readwriteweb.com/archives/facebook\\_bans\\_breast-feeding\\_photos.php](http://www.readwriteweb.com/archives/facebook_bans_breast-feeding_photos.php).
- 176 Michal Humphrey, *Twitter, Guy Adams, and the Cost of Being a User*, Forbes, July 31, 2012, <http://www.forbes.com/sites/michaellhumphrey/2012/07/31/twitter-guy-adams-and-the-cost-of-being-a-user/>.
- 177 Katie Rogers, *Twitter 'Sorry' for Suspending Guy Adams as NBC Withdraws Complaint*, Guardian (UK), July 31, 2012, <http://www.guardian.co.uk/technology/2012/jul/31/guy-adams-twitter-growing-pains>.
- 178 Giancarlo Valdes, *DayZ: How an ARMA II Mod Took the PC World by Storm*, VentureBeat, June 3, 2012, <http://venturebeat.com/2012/06/03/same-sh-different-dayz-how-a-zombie-mod-took-the-pc-world-by-storm/>.
- 179 Lisa DiCarlo, *Apple Bites the Fans that Feed It*, Forbes, Jan. 7, 2005, [http://www.forbes.com/2005/01/07/cx\\_id\\_0107apple.html](http://www.forbes.com/2005/01/07/cx_id_0107apple.html).
- 180 Electronic Frontier Foundation, *Apple v. Does*, <https://www.eff.org/cases/apple-v-does>.
- 181 Nate Anderson, *DMCA Takedown Backlash: EFF Sues Viacom over Colbert Parody Clip*, Ars Technica, Mar. 22, 2007, <http://arstechnica.com/news.ars/post/20070322-dmca-takedown-backlash-eff-sues-viacom-over-colbert-parody-clip.html>.
- 182 Greg Sandoval, *EFF Takes Viacom to Task over YouTube Takedown*, CNet News, Feb. 15, 2007, [http://www.news.com/2100-1026\\_3-6159548.html](http://www.news.com/2100-1026_3-6159548.html).
- 183 E.g., Hee Haw Marketing, *I Hate You Viacom*, Mar. 13, 2007, [http://heehawmarketing.typepad.com/hee\\_haw\\_marketing/2007/03/i\\_hate\\_you\\_viac.html](http://heehawmarketing.typepad.com/hee_haw_marketing/2007/03/i_hate_you_viac.html).
- 184 Jonathan Glater, *Judge Reverses His Order Disabling Website*, N.Y. Times, Mar. 1, 2008, <http://www.nytimes.com/2008/03/01/us/01wiki.html>.
- 185 Ann Brick, *Free Speech Triumphs in WikiLeaks Case*, Bytes & Pieces, Feb. 29, 2008, [http://www.aclunc.org/issues/technology/blog/free\\_speech\\_triumphs\\_in\\_wikileaks\\_case.shtml](http://www.aclunc.org/issues/technology/blog/free_speech_triumphs_in_wikileaks_case.shtml); Jemima Kiss, *US Judge Reverses Wikileaks Injunction*, Guardian (UK), Mar. 3, 2008, <http://www.guardian.co.uk/technology/2008/mar/03/wikipedia.web20>.
- 186 Clint Boulton, *Google Admits to, Fixes Video Refund Gaffe*, eWeek: Google Watch, Aug. 21, 2007, [http://googlewatch.eweek.com/content/google\\_video/google\\_admits\\_to\\_fixes\\_video\\_refund\\_gaffe.html](http://googlewatch.eweek.com/content/google_video/google_admits_to_fixes_video_refund_gaffe.html).
- 187 Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. Times, July 17, 2009, <http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html>.
- 188 David Pogue, *Some E-Books Are More Equal than Others*, N.Y. Times: Pogue's Posts, July 17, 2009, <http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/>.
- 189 Ina Fried, *Amazon Says It Won't Repeat Kindle Book Recall*, CNet News, July 17, 2009, [http://news.cnet.com/8301-13860\\_3-10290047-56.html](http://news.cnet.com/8301-13860_3-10290047-56.html).
- 190 Google Transparency Report, <http://www.google.com/transparencyreport/>.
- 191 Verne Kopytoff, *Yahoo Settles with Jailed Chinese Journalists*, S.F. Chron., Nov. 14, 2007, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/11/14/BUN4TBJNV.DTL&type=business>.
- 192 Brian Wingfield, *Grilling Yahoo*, Forbes, Nov. 06, 2007, [http://www.forbes.com/home/businessinthebeltway/2007/11/05/china-yahoo-privacy-biz-wash-cx\\_bw\\_1106yahoo.html](http://www.forbes.com/home/businessinthebeltway/2007/11/05/china-yahoo-privacy-biz-wash-cx_bw_1106yahoo.html).
- 193 See UK Journalists Union Calls for Yahoo Boycott, One India News, June 2, 2006, <http://news.oneindia.in/2006/06/02/uk-journalists-union-calls-for-yahoo-boycott-1149264801.html>.
- 194 See Electronic Frontier Foundation, *RIAA v. Verizon Case Archive*, <http://www.eff.org/cases/riaa-v-verizon-case-archive>.
- 195 See, e.g., Press Release, Consumer Action, Verizon v. RIAA Ruling Protects Privacy of Internet Users, [http://www.consumer-action.org/press/articles/verizon\\_vs\\_riaa\\_ruling/](http://www.consumer-action.org/press/articles/verizon_vs_riaa_ruling/).
- 196 John Schwartz, *Twitter Fighting Pennsylvania Subpoena Seeking Names of 2 Tweeters*, N.Y. Times, May 20, 2010, [www.nytimes.com/2010/05/21/technology/21twitter.html](http://www.nytimes.com/2010/05/21/technology/21twitter.html).

- 197 David Kravets, *Pennsylvania AG Dropping Twitter Subpoena*, Wired: Threat Level, May 21, 2010, <http://www.wired.com/threatlevel/2010/05/twitter-subpoena-2/>.
- 198 Doug Gross, *Virginia Deputy Fights His Firing over Facebook 'Like'*, CNN, Aug. 13, 2012, <http://www.cnn.com/2012/08/10/tech/social-media/deputy-fired-facebook-like/index.html>.
- 199 Hayley Tsukayama, *Facebook, ACLU: 'Likes' Are Protected Speech*, Wash. Post, Aug. 8, 2012, [http://www.washingtonpost.com/business/technology/facebook-aclu-likes-are-protected-speech/2012/08/08/d8b0e69a-e14e-11e1-a25e-15067bb31849\\_story.html](http://www.washingtonpost.com/business/technology/facebook-aclu-likes-are-protected-speech/2012/08/08/d8b0e69a-e14e-11e1-a25e-15067bb31849_story.html).
- 200 Josh Bell, *ACLU & Facebook Tell Court That "Like" Is Speech*, ACLU Blog of Rights, Aug. 7, 2012, <http://www.aclu.org/blog/free-speech-technology-and-liberty/aclu-facebook-tell-appeals-court-free-speech>.
- 201 Matthew Lasar, *A Paper Trail of Betrayal: Google's Net Neutrality Collapse*, Ars Technica: Law & Disorder, Aug. 11, 2010, <http://arstechnica.com/tech-policy/2010/08/a-paper-trail-of-betrayal-googles-net-neutrality-collapse/>.
- 202 Verizon-Google Legislative Framework Proposal, [http://static.googleusercontent.com/external\\_content/untrusted\\_dlcp/www.google.com/en/us/googleblogs/pdfs/verizon\\_google\\_legislative\\_framework\\_proposal\\_081010.pdf](http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf).
- 203 Cindy Cohn, *A Review of Verizon and Google's Net Neutrality Proposal*, EFF Deeplinks Blog, Aug. 10, 2010, <https://www.eff.org/deeplinks/2010/08/google-verizon-netneutrality/>.
- 204 See Eric Schmidt, *A Note to Google Users on Net Neutrality*, Google Help Center, 2006, [http://www.google.com/help/netneutrality\\_letter.html](http://www.google.com/help/netneutrality_letter.html).
- 205 Ryan Singel, *Why Google Became a Carrier-Humping Net Neutrality Surrender Monkey (Updated)*, Wired, Aug. 10, 2010, <http://www.wired.com/business/2010/08/why-google-became-a-carrier-humping-net-neutrality-surrender-monkey/>.
- 206 Trevor Timm, *How PIPA and SOPA Violate White House Principles on Free Speech and Innovation*, EFF Deeplinks Blog, Jan. 16, 2012, <https://www.eff.org/deeplinks/2012/01/how-pipa-and-sopa-violate-white-house-principles-supporting-free-speech>.
- 207 *Wikipedia Blackout: 11 Huge Sites Protest SOPA, PIPA on January 18*, Huffington Post, Jan. 18, 2012, [http://www.huffingtonpost.com/2012/01/17/wikipedia-blackout\\_n\\_1212096.html](http://www.huffingtonpost.com/2012/01/17/wikipedia-blackout_n_1212096.html).
- 208 Tom Cheredar, *Not Even a Shift to Full SOPA Opposition Can Stop Go Daddy from Hemorrhaging Customers*, VentureBeat, Dec. 29, 2011, <http://venturebeat.com/2011/12/29/not-even-a-shift-to-full-sopa-opposition-can-stop-go-daddy-from-hemorrhaging-customers/>.
- 209 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012).
- 210 U.S. Dep't of Health & Human Services, *Who Must Comply with HIPAA Privacy Standards*, Dec. 19, 2002, <http://www.hhs.gov/hipaafaq/about/190.html>.
- 211 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2012).
- 212 Children's Online Privacy Protect Act of 1998, 15 U.S.C. §§ 6501–6506 (2012).
- 213 Right to Financial Privacy Act, 12 U.S.C. §§ 3401 *et seq.* (2012); *see also* Electronic Privacy Information Center, *Right to Financial Privacy Act*, <http://epic.org/privacy/rfpa/>.
- 214 Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81u (2012); *see also* Electronic Privacy Information Center, *The Fair Credit Reporting Act and the Privacy of Your Credit Report*, <http://epic.org/privacy/fcra/>.
- 215 Privacy Act of 1974, 5 U.S.C. § 552a (2012).
- 216 Drivers Privacy Protection Act, 18 U.S.C. §§ 2721–25 (2012); *see also* Electronic Privacy Information Center, *The Drivers Privacy Protection Act and the Privacy of Your State Motor Vehicle Record*, <http://epic.org/privacy/drivers/>.
- 217 Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012).
- 218 Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2012).
- 219 *See generally* Prepared Statement of the Federal Trade Commission on the Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission (testimony before the Senate Committee on Commerce, Science, and Transportation), May 9, 2012, *available at* <http://www.ftc.gov/os/testimony/120509privacyprotections.pdf>.
- 220 *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change ii* (Mar. 2012), *available at* <http://ftc.gov/os/2012/03/120326privacyreport.pdf>.
- 221 *See* Federal Comm. Comm'n, *About the FCC*, <http://www.fcc.gov/aboutus.html>.
- 222 *See* Federal Comm. Comm'n, *Location-Based Services: An Overview of Opportunities and Other Considerations* (2012), <http://www.fcc.gov/document/location-based-services-report>.
- 223 *See* Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1 (1994).
- 224 *See* National Conference of State Legislatures, *Privacy Protections in State Constitutions*, <http://www.ncsl.org/issues-research/telecom/privacy-protections-in-state-constitutions.aspx>.
- 225 *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berkeley Tech. L.J. 1085, 1131–44 (2002), *available at* [http://www.btlj.org/data/articles/17\\_03\\_04.pdf](http://www.btlj.org/data/articles/17_03_04.pdf).
- 226 Ca. Civil Code §§ 1798.85–1798.86 (2012).
- 227 Ca. Civil Code § 1798.90.1 (2012).
- 228 *See* eSecurityPlanet Staff, *California Adopts Smart Grid Privacy, Security Rules*, eSecurity Planet, Aug. 5, 2011, <http://www.esecurityplanet.com/headlines/article.php/3938251/California-Adopts-Smart-Grid-Privacy-Security-Rules.htm>.
- 229 Press Release, Ca. Dep't of Justice Office of the Attorney General, Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection United, July 19, 2012, <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection>.
- 230 Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final, *available at* [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf); 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 Authorities 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, COM (2012) 10 final, *available at* [http://ec.europa.eu/home-affairs/doc\\_centre/police/docs/com\\_2012\\_10\\_en.pdf](http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf).

- 231 See Françoise Gilbert, *Proposed EU Data Protection Regulation: A New Framework for 2015?*, Jan. 29, 2012, <http://www.francoisegilbert.com/2012/01/proposed-eu-data-protection-regulation-a-new-framework-for-2015/>.
- 232 Ca. Bus. & Prof. Code § 22575 (2012).
- 233 See Press Release, State of California Department of Justice Office of the Attorney General, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, Feb. 22, 2012, <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.
- 234 National Conference of State Legislatures, *State Security Breach Notification Laws*, <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.
- 235 Ca. Civil Code § 1798.83 (2012).
- 236 Reader Privacy Act, Ca. Civil Code § 1798.90(i) (2012).
- 237 *U.S. v. Jones*, 565 U.S. \_\_ (2012) (Alito, J., concurring in the judgment) (“In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”).
- 238 U.S. Const, amend. IV.
- 239 See *Katz v. U.S.*, 389 U.S. 347 (1967).
- 240 *U.S. v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).
- 241 See, e.g., *U.S. v. Warshak*, 631 F.3d 266 (2010).
- 242 See, e.g., In the Matter of an Application of the United State of America for an Order Authorizing the Release of Historical Cell-Site Information, Case 1:10-mc-00897-NGG-JO (E.D. N.Y. Aug. 22, 2011) (Memorandum & Order).
- 243 See, e.g., *U.S. v. Skinner*, File Name 12a0262p.06 (6th Cir. 2012), available at <http://www.ca6.uscourts.gov/opinions.pdf/12a0262p-06.pdf> (holding that cell site location data and GPS data derived from the operation of a cell phone are not protected by the Fourth Amendment).
- 244 See *U.S. v. Jones*, 565 U.S. \_\_ (2012) (Sotomayor, J., concurring), and *id.* (Alito, J. concurring in judgment).
- 245 See Alex Fitzpatrick, *Judge: Public Tweets Have No ‘Reasonable Expectation of Privacy’*, Mashable, July 3, 2012, <http://mashable.com/2012/07/03/twitter-privacy/>.
- 246 Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22, available at <http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119>; Stored Communications Act, 18 U.S.C. §§ 2701–12, available at <http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121>.
- 247 See Digital Due Process, *About the Issue*, <http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163> (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002)).
- 248 See Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev 373 (2006), available at [http://works.bepress.com/stephen\\_henderson/3](http://works.bepress.com/stephen_henderson/3).
- 249 Reader Privacy Act, Ca. Civil Code § 1798.90(c)–(d) (2012).
- 250 U.S. Const, amend. IV.
- 251 *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334 (1995), available at <http://www.law.cornell.edu/supct/html/93-986.ZO.html>.
- 252 Ca. Const., Art. 1 § 1.
- 253 *Ferlauto v. Hampsher*, 74 Cal.App.4th 1394 (1999), available at <http://jour305.homestead.com/files/ferlauto.pdf>.
- 254 See generally Josh Mulligan, *Finding a Forum in the Simulated City: Mega Malls, Gated Towns, and the Promise of Pruneyard*, 13 Cornell J. L. & Pub. Pol’y 533, 557 (2004).
- 255 See *Pruneyard Shopping Center v. Robins*, 23 Cal.3d 899 (1979).
- 256 Federal Comm. Comm’n, *Commission Seeks Comment on Certain Wireless Service Interruptions*, Mar. 1, 2012, <http://www.fcc.gov/document/commission-seeks-comment-certain-wireless-service-interruptions>
- 257 Declan McCullagh, *FCC Net Neutrality Rules Reach Mobile Apps*, CNet News, Dec. 23, 2010, [http://news.cnet.com/8301-13578\\_3-20026581-38.html](http://news.cnet.com/8301-13578_3-20026581-38.html).
- 258 Timothy B. Lee, *Verizon: Net Neutrality Violates Our Free Speech Rights*, *Ars Technica: Law & Disorder*, July 3, 2012, <http://arstechnica.com/tech-policy/2012/07/verizon-net-neutrality-violates-our-free-speech-rights/>.
- 259 17 U.S.C. §§ 101 *et seq.* (2012).
- 260 See generally Electronic Frontier Foundation, *Fair Use Frequently Asked Questions*, [http://w2.eff.org/IP/eff\\_fair\\_use\\_faq.php](http://w2.eff.org/IP/eff_fair_use_faq.php).
- 261 47 U.S.C. § 230 (2012).
- 262 See Citizen Media Law Project, *Immunity for Online Publishers Under the Communications Decency Act*, <http://www.citmedialaw.org/legal-guide/immunity-online-publishers-under-communications-decency-act>.
- 263 17 U.S.C. § 512 (2012).
- 264 See Citizen Media Law Project, *Protecting Yourself Against Copyright Claims Based on User Content*, <http://www.citmedialaw.org/legal-guide/protecting-yourself-against-copyright-claims-based-user-content>.

“STARTUPS TODAY NEED TO BE PROACTIVE ABOUT PRIVACY ISSUES RATHER THAN DEALING WITH THEM AS AN AFTERTHOUGHT. THIS ACLU PRIMER OF BUSINESS CASE STUDIES AND PRACTICAL TIPS PROVIDES EXCELLENT INSIGHTS WHICH WILL HELP COMPANIES PUT A WELL-CONCEIVED STRATEGY IN PLACE.”

—**RAMAN KHANNA, MANAGING DIRECTOR,  
ONSET VENTURES**

“AS TECHNOLOGY HAS BECOME AN INTEGRAL PART OF MODERN LIFE, IT HAS ALSO COME TO PLAY A CENTRAL ROLE IN SHAPING THE FUTURE OF PRIVACY AND FREE SPEECH. THIS PRIMER INTRODUCES KEY PRIVACY AND FREE SPEECH CONSIDERATIONS FOR DESIGNERS, ENGINEERS, ENTREPRENEURS, AND ANYONE ELSE INVOLVED IN A MODERN TECHNOLOGY BUSINESS.”

—**KEVIN MAHAFFEY, CO-FOUNDER AND CTO,  
LOOKOUT MOBILE SECURITY**

“UNDERSTANDING THE LEGAL LANDSCAPE SURROUNDING PRIVACY AND FREE SPEECH IS IMPERATIVE FOR ANY ENTREPRENEUR BUILDING A DIGITAL MEDIA STARTUP. THE ACLU'S PRIMER IS AN INVALUABLE RESOURCE.”

—**DAVID HORNICK, GENERAL PARTNER,  
AUGUST CAPITAL**

