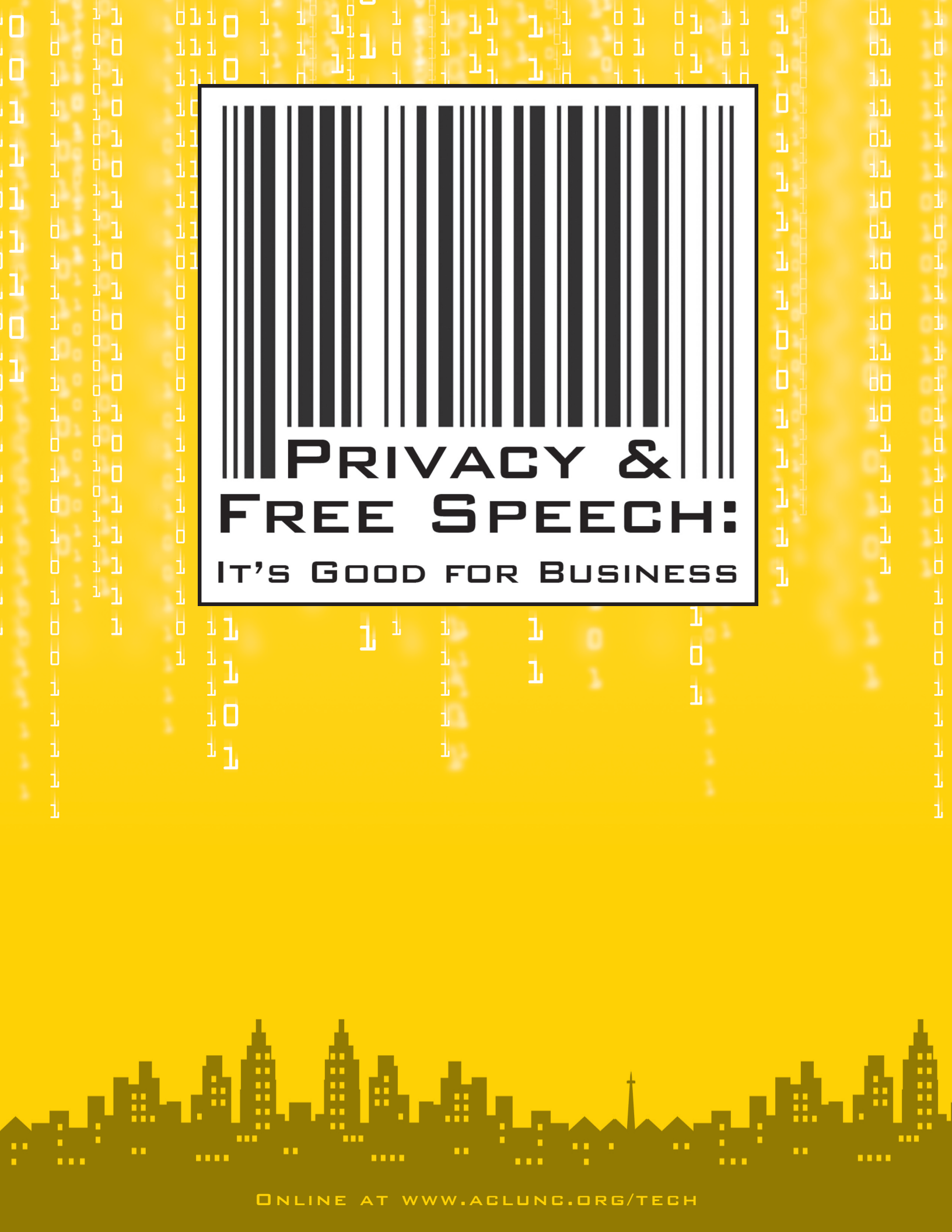
Privacy &
Free Speech:
It's Good for Business
Online at www.aclunc.org/tech

New technology has revolutionized how individuals work and live. It has provided unprecedented access to information, linked people around the world, and given voice to those who might not otherwise be heard. However, technology also can pose risks to your customers' rights, especially their privacy and freedom of expression.

This Guide will help you make smart, proactive decisions about privacy and free speech so you can protect your customers' rights while bolstering the bottom line. Failing to take privacy and free speech into proper account can easily lead to negative press, government investigations and fines, costly lawsuits, and loss of customers and business partners. By making privacy and free speech a priority when developing a new product or business plan, your company can save time and money while enhancing its reputation and building customer loyalty and trust.

Read this Guide now and use it as you develop your next product or business venture. The practical tips and real-life business case studies in this Guide will help you to avoid having millions read about your privacy and free speech mistakes later.

For more information about how your company can build proper privacy and free speech safeguards into your products and business plans, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our Web site and blog at **www.aclunc.org/tech.**

CONTENTS

AUTHOR: Nicole A. Ozer, Technology and Civil Liberties Policy Director, ACLU of Northern California

CONTRIBUTING WRITERS: Chris Conley, Christopher Soghoian, Travis Brandon, Aaron Brauer-Rieke

EDITING: Nancy Adess

DESIGN: Gigi Pandian

PRINTING: Inkworks Press

SPECIAL THANKS to the staff of ACLU National Technology and Liberty Project for editing assistance.

For more information about how your company can build proper privacy and free speech safeguards into your products and business plans, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our Web site and blog at www.aclunc.org/tech.

The ACLU of Northern California wishes to thank the following funders for their support of this publication:
Block v. eBay cy pres fund
California Consumer Protection Foundation
Consumer Privacy Cases cy pres fund
Rose Foundation for Communities and the Environment
The David B. Gold Foundation

Published by the ACLU of Northern California, February 2009

I: OVERVIEW

This Guide has been developed to help companies address user privacy and protection of free speech in a manner that both benefits the company and protects user interests. This section provides an overview of the reasons that companies should be concerned about privacy and free speech issues. The following sections contain specific business tips to aid you in building privacy and free speech into new products and businesses, as well as real-life case studies of companies that have succeeded or failed when they encountered a challenge related to privacy or freedom of speech.

PRIVACY AND FREE SPEECH SAFEGUARDS ARE A GOOD INVESTMENT

Safeguarding your customers' privacy and freedom of speech is not only prudent from a legal standpoint, it is also wise business policy. Protecting user rights can generate immediate results as well as build customer loyalty and trust.

SAFEGUARDS CAN INCREASE USE AND CONSUMER SPENDING

With safeguards in place, consumers are likely to spend more online. One study in 2000 found that consumers would spend a total of $6 billion more annually on the Internet if they did not feel that their privacy was on the line every time they made a transaction.[1] In 2008, a study found that 68% of individuals were "not at all comfortable" with companies that create profiles linking browsing and shopping habits to identity.[2] Other research in 2007 found that customers are willing to pay to protect their privacy and calculated the value at approximately 60 cents more per fifteen-dollar item.[3]

SAFEGUARDS CAN GENERATE POSITIVE PRESS AND CREATE CUSTOMER LOYALTY

Safeguards can also enhance your image and bring customers closer. For example, when **Qwest** refused to join its fellow telephone companies in disclosing customer information to the National Security Agency, the *New York Times* noted the positive public reaction, stating, "Companies can't buy that kind of buzz."[4] When **Google** refused to disclose search records to the United States government[5] and **Yahoo!** refused to cave to pressure from the French government to ban specific materials from its online auctions,[6] they were feted by the press and the public as privacy and free speech heroes.

PRIVACY AND FREE SPEECH MISTAKES HURT BUSINESS

When it comes to protecting your users' privacy and free speech, mistakes can cost you not only money but also your good name.

MISTAKES CAN RESULT IN GOVERNMENT INVESTIGATIONS AND FINES

Government oversight and penalties can hurt. For example, data broker **ChoicePoint**'s insecure data practices cost it $25 million in government fines, legal fees, and costs to notify consumers about a security breach,[7] as well as a rapid 9% dive in stock price.[8] **Comcast** was taken to task by the Federal Communications Commission[9] and forced to defend against class-action lawsuits[10] for interfering with free speech by slowing access for customers using peer-to-peer technologies.

MISTAKES CAN RESULT IN EXPENSIVE LAWSUITS

Several large companies have felt the sting of lawsuits related to their privacy and free speech practices. **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 Agencys massive warrantless wiretapping and data-mining program.[11] **Apple** was slapped with $740,000 in attorney's fees when it tried to expose the identity of individuals who leaked information to bloggers about new products.[12]

MISTAKES CAN RESULT IN LOSS OF REVENUE AND REPUTATION

Free speech and privacy violations can directly affect a company's revenue as well. **Facebook** lost major advertising partners and was the target of online protests from 80,000 of its users for failing to provide proper notice and consent for its Beacon advertising service tying a user's other Internet activities to her Facebook profile.[13] **NebuAd**'s plan to meticulously track all online activity, down to every Web click, and then use this information for targeted advertising went awry when consumers sounded the alarm for online privacy and free speech; in its wake, major partnership agreements crumbled, a Congressional committee investigation was initiated, and the company's founder and chief executive resigned.[14]

FOLLOWING THE LAW IS NOT ENOUGH FOR USERS OR THE BOTTOM LINE

It is imperative to understand and strictly adhere to all federal and state privacy and free speech laws and regulations.[15] But businesses should be aware that the current laws are often unclear; moreover, these laws may not always provide consumers with the level of privacy and free speech protections that they expect and demand.

COMPANIES MAY FIND THEMSELVES CAUGHT BETWEEN DEMANDS FOR INFORMATION AND USERS' EXPECTATIONS OF PRIVACY

Outdated privacy laws can leave companies in an impossible situation, forced to choose between maintaining the trust of users and responding to subpoenas and other demands for information from the government or third parties.

Although many users 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. The "business record" doctrine, which was established in pre-Internet Supreme Court cases[16] and has not been reconsidered in light of the new reality of online communication and commerce, holds that there is no reasonable expectation of privacy, and thus no Fourth Amendment privacy protection, when a user turns over information to a third-party business. Law enforcement officials thus claim that they can demand information about online activities of Internet users without a search warrant, at least without violating the Constitution.

However, other laws, such as the California state constitution and federal and state statutes protecting health records, financial records, electronic communications, video rentals records, and other specific information, provide additional sources of privacy protection for personal information.[17] This patchwork of laws, along with the grey areas in Fourth Amendment doctrine, may leave companies exposed to demands for information whose legal validity is difficult or impossible to determine.

Even where the law is relatively clear, there may be a significant disparity between what users expect and what the law requires. Only companies that develop robust privacy policies that anticipate potential conflict and lay out procedures to safeguard user privacy to the greatest extent possible will meet user expectations during these difficult situations; those that do not risk paying the price by alienating both existing and potential users.

COMPANIES MAY FACE COMPETING DEMANDS TO ENABLE AND LIMIT SPEECH

Consumers have come to rely on the Internet and other new technologies as crucial platforms for the distribution and discussion of news and current events, creative expression, and other socially valuable speech. When a user's political video is removed from a site, when an individual posts an anonymous message and his identity is revealed, or when a company censors information that should be delivered to users, there is often a free speech firestorm regardless of the nuances of what a company is legally required to do. Although its technology may be cutting-edge, a company must be careful to ensure that its business plan and policies do not interfere with long-established free speech expectations.

COMPANIES CAN ACT TO PROTECT THEIR CUSTOMERS AND THEIR OWN INTERESTS

Companies that meekly comply with every request for customer information, whether from the government or a third party, may find themselves subject to a barrage of such requests, which can consume resources while alienating customers. Companies that stand up for their customers' rights to privacy and free speech will earn customer loyalty and may even reduce the administrative burden of dealing with such requests.

Moreover, weak privacy and free speech laws hurt companies that want to build trustworthy services. Companies should push for new laws that will build consumer confidence and protect them from being caught between the privacy interests of customers and government and third-party demands for information.

PROMOTING PRIVACY AND FREE SPEECH IS GOOD BUSINESS

Establishing policies that protect privacy and free speech can be a good way to stand out from your competitors. Protecting your users' rights though legal and other means can generate valuable trust and goodwill that will pay off in the long run. The following sections give you the chance to ask yourself important questions about how your company is currently doing business. Use the tips here to build a solid plan that will save your company money, time, and reputation by properly protecting privacy and free speech.

KEEP USERS INFORMED

- Develop a comprehensive and easy-to-understand privacy policy
- Post your privacy policy prominently on all Web pages
- Always follow your privacy policy
- Alert users and employees to privacy policy changes
- Provide notice and get user consent for software and service updates

PROTECT USERS WHILE GATHERING DATA

- Collect and store only necessary user information
- Aggregate or anonymize user transactional data where appropriate
- Inform users about data collection
- Use "opt-in" processes to collect and share user data
- Have easy, fast, and effective user correction and deletion procedures for user data

PROTECT USER DATA FROM DISCLOSURE

- Ensure proper legal process for disclosures and resist overbroad requests
- Promptly notify users about disclosure requests whenever possible
- Disclose only required information
- Safeguard user data—protect devices and develop data security practices
- Quickly respond, notify, and provide service for data breaches
- Protect users from surreptitious monitoring

PROMOTE FREE SPEECH

- Develop and enforce content-neutral policies
- Protect anonymous speech

AVOID POLICIES AND PRACTICES THAT CHILL FREE SPEECH

- Draft your terms of use and service narrowly to avoid stifling protected speech
- Safeguard product trust by not monitoring and tracking speech
- Respect free speech in takedowns
- Plan for fair use before deploying digital rights management (DRM)

These tips will help you get an edge by building customer loyalty and trust while protecting your company from both litigation and excessive demands for information. In a competitive market, superior privacy and free speech policies might be the difference between success and failure.

II: GETTING AN EDGE: MAKING YOUR PRIVACY PRACTICES STAND OUT

The key to developing outstanding privacy practices is ensuring that users are a part of the process. Informing your users about your products and policies, ensuring that their interests are protected when a data breach occurs or a third party seeks their information, and enabling them to control their own data can give users an ownership stake in your product and build invaluable trust and loyalty.

KEEP USERS INFORMED

DO WE HAVE A REAL "PRIVACY" POLICY?

Every company that operates a commercial Web site in California must post a conspicuous privacy policy on its Web site that discloses the kinds of personally identifiable data that it collects and shares with third parties.[18] But the term "privacy policy" is often misleading. Although consumers expect that privacy policies actually protect consumer privacy,[19] such policies may instead state, in effect, that the company may do as it pleases with whatever information it chooses to collect.

Having a real privacy policy designed to inform users is not just the law, it is also good business. A strong privacy policy can be a marketing tool, attracting users who prefer to do business with a trustworthy company that safeguards their private information.

- **Explain what data you collect.** Do you collect personal information, such as phone numbers, addresses, or Social Security numbers? Do you create a log of users' online histories? Do you collect clickstream data?

- **Explain how data is stored.** How long is each category of data stored? What data is linked to an individual? What data is anonymized and after how long? What data is combined?

89% of consumers in 2006 felt more comfortable giving their personal information to companies that have clear privacy policies.[20]

- **Explain how data will be used or shared.** Do you create a user profile? Do you use it to deliver targeted advertising? Do you sell or share this data? If so, with whom? How do you ensure that this data is not being misused or resold? How can users stop their data from being shared?

- **Explain your processes for responding to data requests by government and third parties.** What data could be requested and disclosed? What standards must the government or third parties meet in order to obtain that data from your company? When and how will you provide notice to users about requests for information? Will you challenge questionable demands on behalf of your users?

- **Explain how users can view and control their own data.** What options do users have to view data? What categories of data can be deleted and how? How quickly is data purged, both online and in archives? What procedures are in place to fix errors?

- **Notify users in advance if your privacy policy is about to change.** Give users the opportunity to terminate use of the system and have existing data deleted or keep using your service but opt out of having their existing data processed under the new policy.

- **Always follow your privacy policy.** Your policy is a contract that you make with your users; failure to follow it can result in the loss of user trust as well as lawsuits by users and action by the Federal Trade Commission and other state and federal agencies.

59% of consumers said they would recommend a business to their family and friends if they believe that it follows its privacy policies.[21]

Do we provide users with notice and get their consent before installing or updating software or features?

Making it as easy as possible for users to install or upgrade their software or use new features can be beneficial, but keeping users in the loop about changes is just as important. Users want to have notice and an opportunity to consent before any significant changes take effect. Both Sony and Google learned the hard way that users do not like their software to contain silent, hidden surprises.

- **Notify users and gain their consent before installing or updating products.** Most users will embrace new or improved functionality as long as they are aware of what they are getting. Giving users choices before making changes will allow them to voice possibly legitimate complaints as well as prevent controversies when new features have unforeseen consequences.

Sony: Shipping CDs with an aggressive digital rights management (DRM) program that installed itself on users' computers without their permission was a big mistake for Sony. The company was targeted by multiple class-action lawsuits and blasted in the media.[22] Sony was forced to recall the CDs and pay millions of dollars in compensation to its users.[23]

- **Activate auto-update only with user consent.** Most users will happily activate a feature that keeps their software up-to-date without requiring any effort on their part—but some will be less than pleased if such updates happen automatically without their knowledge or permission. Avoid dissatisfaction by making auto-update an opt-in process.

Google: The company was pilloried in the press for making millions of its Google toolbar users vulnerable to a malicious software attack because of its toolbar's silent, automatic update mechanism.[24] In 2006, a researcher found a flaw in the toolbar update mechanism of the Firefox browser.[25] But since the Google toolbar software, unlike that used by Yahoo! or Facebook, did not provide notice to and obtain consent from users prior to updating the toolbar, Google toolbar users who used the Firefox browser could not control when the toolbar was updated and faced increased risk.[26]

- **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: When Apple released its Safari 3.1 for Windows 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,"[27] driving Apple to clearly identify Safari as a new product and have users opt in prior to installation.[28]

PROTECT USERS WHILE GATHERING DATA

DO WE COLLECT AND STORE ONLY NECESSARY USER INFORMATION?

As data storage becomes less expensive, it may start to seem as though there is little reason not to collect and retain as much data as possible about your users. However, the apparent ease of accumulating masses of data can hide enormous costs due to user dissatisfaction, security breaches, time-consuming subpoena requests, and privacy and free speech firestorms.

59% OF ADULTS IN A 2008 STUDY HAD REFUSED TO PROVIDE INFORMATION TO A BUSINESS OR COMPANY BECAUSE THEY THOUGHT IT WAS NOT NECESSARY OR TOO PERSONAL.[29]

- **Capture only the data you need for your service or that you are legally required to capture.** AOL reportedly receives more than 1,000 subpoenas *every month* requesting information about its users.[30] Other tech companies may face similar numbers of requests, although they do not reveal exact numbers.[31] An efficient way to avoid these costs is to capture only the data you need for your service. Do you really need an individual's name, address, and phone number? Alternatively, could your company get by just as well with only one of these pieces of identifying information? Or none?

- **Store only necessary data.** Even if you needed to capture identifying information in order to handle a specific transaction, there may be no need to retain it after the transaction is complete. Any data collected should be purged in its entirety after it is no longer necessary. Personally identifying information should rarely be retained for more than a few weeks.

Ask, Google, Microsoft, Yahoo!: Major search engines have started to recognize the importance of limiting data-retention periods for all data.[32] Ask developed the AskEraser, allowing users to conduct online searches without the company logging any information.[33] Microsoft deletes the full IP address, cookies, and any other identifiable user information from its logs after 18 months.[34] Yahoo! is now planning to anonymize all search records after three months.[35] Google now engages in a very limited form of log anonymization after nine months for those using the search engine and not logged into a Google account.[36] After 18 months, the company deletes a portion of the stored IP address and de-identifies the cookie information stored in its logfiles.[37]

DO WE MINIMIZE THE LINKS BETWEEN PERSONAL INFORMATION AND TRANSACTIONAL DATA?

By minimizing the connections between personal information about users and data about the users' activities, companies may be able to achieve desired business goals such as optimizing performance or delivering targeted advertisements and services while cultivating user trust and insulating a company from voluminous legal demands and costly security breaches. Anonymization, aggregation, and similar techniques can help you extract value from your data while protecting your users' privacy.

- **ASSOCIATE USER RECORDS OR PERSONAL INFORMATION WITH TRANSACTIONAL RECORDS ONLY WHERE NECESSARY.**
  Tying identifiable data, including IP addresses or account information, to transactional records invites privacy breaches and lawsuits. Evaluate aggregation and anonymization as tools to protect privacy while preserving the value of collected information.[39]

68% OF CONSUMERS IN 2000 WERE "NOT AT ALL COMFORTABLE" WITH COMPANIES THAT CREATE PROFILES THAT LINK BROWSING AND SHOPPING HABITS TO IDENTITY. THE NUMBERS SPIKED TO 82% WHEN PROFILES INCLUDE INCOME, DRIVER'S LICENSE NUMBERS, CREDIT DATA, OR MEDICAL STATUS.[38]

YOUTUBE: In 2008, YouTube was ordered to turn over records of every video watched by its users, including names and IP addresses, to Viacom, which was suing the company for copyright infringement.[40] Since YouTube collected and maintained "deeply private information" linking individuals and their viewing habits, this information was available when Viacom came calling.[41] Eventually, a compromise was reached and the data was anonymized before being turned over to Viacom.[42] However, this close call resulted in extensive press coverage and outrage by YouTube users and privacy advocates.[43]

AOL: 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.[44] AOL quickly pulled the dataset from its Web site, 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.[45] 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.[46]

Do we give our users control over the services they receive and the information they share?

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.[47]

Failing to ask opt-in permission 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. Follow an ethos of putting the user in control and your relationship with your users may be far more positive.

- **Use opt-in to activate any new services or features.** Users will often happily volunteer to use new features—if they are given the choice. When new features are simply activated without consent, however, backlash can be severe. Overall, giving users a choice can lead to more trust and, ultimately, more users.

- **Use opt-in to initiate or change data collection or sharing.** Users are particularly concerned that their personal information might be shared without their permission. Giving them the choice to share data puts them in control and will mitigate these fears.

88% of Internet users in 2000 wanted businesses to affirmatively ask them for permission, through an opt-in mechanism, each time the business wants to share personal information with anyone else.[48]

94% in 2003 wanted the legal right to know everything that a Web site knows about them.[49]

84% in 2003 believe that a law giving them the right to control how a Web site uses and shares the information collected about them would protect their privacy.[50]

Facebook: The popular social networking site has repeatedly failed to include adequate privacy protections in its new features and has paid with complaints by hundreds of thousands of users,[51] calls for boycotts,[52] legislative proposals for industry regulation, and loss in both reputation and advertising partners.[53] When Facebook announced its new Beacon advertising service in 2007, which tied a user's activity on external Web sites to the user's Facebook profile, the service leaked surprise holiday gifts, engagement plans, and other private information to friends and family.[54] The widespread outrage and negative press forced the company to modify this feature, but not before several large advertisers, including Coca-Cola, Travelocity, and Overstock.com, withdrew from the new program.[55]

Do we give users control over their own accounts and data?

A user who is not confident that she has control over her personal information may be wary of trying new services or products. Refusing to allow users to control their accounts, even when they choose to leave your service, results in poor press and reputational harm. Giving users control over their own data is a better way to address the situation.

- **Allow users to view and control their own data.** Users are often in the best position to fix mistakes in their personal records, and they should have a right to view those records in order to do so. Allowing users to maintain their own records (with appropriate logging and oversight) can increase both user trust and data accuracy.

- **Create a quick and easy process for users to delete records or terminate accounts.** Obviously, you hope that users will remain with your service; but 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.

Online storage and software services, often termed "cloud computing," are growing in popularity. But according to a 2008 study, the underlying message of cloud users to providers is, "Let's keep the data between us." Cloud users do not want their information used in unauthorized ways, and high percentages responded that they were "very concerned" when asked about scenarios in which companies:

- Turn their data over to law enforcement (49%)
- Keep copies of files even after they try to delete them (63%)
- Analyze data in the cloud for targeted advertisements (68%)
- Use cloud documents in marketing campaigns (80%)
- Sell files to others (90%)[56]

Facebook: Facebook users were very unhappy in 2008 when they realized that it was nearly impossible to remove their information from the social network.[57] 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.[58]

PROTECT USER DATA FROM DISCLOSURE

DO WE DISCLOSE USER INFORMATION ONLY WHEN REQUIRED?

Businesses are often asked for user information through legal subpoenas, court orders, and warrants. By having a policy of disclosing user information only when required, your business can help shield itself from liability for illegal disclosure, avoid negative press, gain the trust of users, reduce the administrative costs of compliance, and help set legal precedents that will prevent costly litigation in the future.

- **Comply with demands for information only where required by law.** Reject any demand that lacks legal authority. If the law is uncertain, it is in your best interests, as well as those of your users, to 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.

AT&T, Verizon: 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.[59] The companies were caught in a firestorm of bad publicity and hit by a barrage of costly class action lawsuits.[60] The companies faced potentially "crippling" damages in the hundreds of *billions* of dollars and have spent massive amounts on attorney and lobbyist fees to try to sidestep liability.[61]

Qwest: By resisting the NSA's request for telephone records, Qwest received a significant amount of positive media coverage. The *New York Times* described the company as "a gleaming touchstone and a beacon of consumer protection"[62] and noted that many users had switched to Qwest purely on the basis of its principled stand against government surveillance. The Associated Press declared that Qwest was "squarely on the side of the little guy,"[63] and bloggers created online buttons reading "Qwest—NSA-Free: Who are you with?" As the *New York Times* pointed out, "Companies can't buy that kind of buzz."[64]

- **Promptly notify the user and give the user an opportunity to respond.** If you do receive a legitimate demand for information, notify the target of that request if possible. 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 adequate time (at least 30 days) to do so. Do not comply with the demand until any such challenge is decided.

- **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 them for a single week, or disclosing user transactions that are unrelated to the scope of the request.[65] Excessive disclosures can lead to legal liability for your company and loss of user trust.

Google: 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.[66]

Do we have a solid security plan and take all necessary steps to safeguard user data?

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.[67] The Federal Trade Commission 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.[68] 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.

- **Conduct a risk assessment.** List every type of information that your company collects and stores. Determine which types can be used to identify people individually, such as names, addresses, Social Security numbers, debit/credit card numbers, or account information. For each type of information you collect, evaluate its sensitivity and the procedures that will most effectively safeguard it.

- **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.

- **Store data securely.** Data on your servers, on laptops, or in paper form should all be equally secure. Remember, identity theft can involve high-tech methods such as hacking and phishing, but also decidedly low-tech methods such as rooting in dumpsters and stealing from mailboxes. Make sure that all places where information enters and exits your business are secure.

ChoicePoint: Data broker ChoicePoint paid with its capital, its stock price, and its reputation in 2005 when it failed to secure the personal data of 163,000 individuals and identity thieves obtained this information.[69] As a result of its poor privacy practices and the security breach, the company was slapped with a $15 million fine by the Federal Trade Commission, spent $2 million notifying victims of the breach, and incurred $9.4 million in legal fees.[70] The company's stock price also plunged more than 9%.[71] In the end, ChoicePoint's failure to take sensible precautions to protect its users' privacy ended up costing it more than $25 million, not to mention a lifetime's worth of bad publicity.[72]

- **Protect data with encryption.** Encrypt personally identifiable user data wherever feasible, particularly before storing it on backup tapes and removable storage devices (including employee laptops). In addition to this being a good way to protect your users, it is a great way to protect your company.

- **Limit and monitor access to data.** 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. Log all data access and review these logs regularly.

Facebook: 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.[73] 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.[74]

- **Respond to security risks.** Researchers or members of the public may discover a flaw in your system that could be exploited. If this happens, do not try to silence the criticism. Acknowledge the problem and take prompt action to fix it.

Cisco: 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. The researcher had discovered that the flaw could potentially be exploited by hackers to seize control of a router and monitor, intercept, delete, or misdirect communications.[75] Although the conference and researcher ignored 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.[76]

DO WE HAVE A PLAN TO NOTIFY AND PROTECT USERS IF A SECURITY BREACH OCCURS?

Even with a solid data security plan, data can still be lost or stolen. Forty-four states, the District of Columbia, and Puerto Rico have laws that require businesses to notify users if their data is lost or stolen.[77] Every company and online service that conducts business nationwide needs to know how it will quickly and effectively inform users in the event of a data breach.

ChoicePoint: Being targeted by identity thieves who obtained personal data about 163,000 individuals was bad enough, but ChoicePoint compounded its own injury by initially notifying only victims who happened to live in California, the sole 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.[78]

- **Notify users promptly.** Prompt notification is often crucial to allow users to prevent identity theft and other consequences of data loss before they occur. The costs to your users and the erosion of their trust vastly outweigh any benefits of delaying notification until required by law.

- **Clearly explain what happened.** Let users know what happened to their data, what you are doing to fix the problem, and how they can protect their credit. By being forthright about the problem and offering clear guidance and assistance to your users about how they can protect and monitor their credit, you will reassure them that you take your business responsibilities—and their privacy—seriously. Many users have actually reported feeling more secure once they saw the positive way that a company responded to a data breach.

- **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.

- **Repair your reputation.** Offer free credit monitoring to your users, where appropriate. LexisNexis,[79] Horizon Blue Cross Blue Shield of New Jersey,[80] and the US Department of Agriculture[81] all offered free credit monitoring after data breaches and received favorable press attention for making an effort to redress the harms to their users.

Do we protect users from surreptitious monitoring?

If your company's products utilize Radio Frequency Identification (RFID) tags, sensors (including microphones or cameras), and/or location-aware devices, or if your business plans rely on knowing who somebody is or where they are going, that information may also be very desirable for others, such as law enforcement agencies that want to track individuals surreptitiously. You can take some important steps so that customers are not being forced to choose between your product and their privacy.

- **Inform users about tags, sensors, or location tracking and obtain opt-in consent.** Inform users about the information that your product or service generates or demands, and allow them to choose whether and when to share this information. Allow users to convey partial information, such as a city or zip code, in lieu of complete information, such as a street address or precise longitude and latitude.

- **Notify users whenever a device is active.** Users should be aware when a device or product is actively recording or transmitting information or tracking their location and using or sharing that information. If your product collects or transmits information surreptitiously and that fact is revealed, user trust will be severely affected.

In-Car Assistance Systems: Users who purchased in-car assistance systems thinking that they would be used to help them find their stolen cars and 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.[82]

- **Protect users' personal information.** Prevent hackers, identity thieves, stalkers, and others from accessing data by ensuring that data transmissions are protected through means such as encryption, authentication, and shielding.

HID Corporation: This large manufacturer of Radio Frequency Identification (RFID) technology received a mountain of bad press for trying to silence information about security and privacy vulnerabilities. Researchers built a device for a mere $25 that revealed that many of the company's RFID tags used for building access cards could be read, copied, and cloned from a distance without anyone ever knowing.[83]

- **Educate users.** Let users know about any privacy or security mechanisms and help them understand when and how to employ them. Users of RFID-enabled toll systems in San Francisco are issued a Mylar bag to block RFID transmissions when they are not passing through a toll booth—but the shield bags are not labeled, so many users throw them away. Invest in both technology and communication to protect your users.

- **Minimize data that you collect and store.** Sensor and location information is particularly attractive to law enforcement. Unless you want to become a target for expensive and time-consuming demands for information, do not store sensitive information—or delete the information after the shortest period of time possible. If your company does retain sensor or location information, follow the steps discussed earlier and develop a robust policy to ensure that user information is not disclosed unless truly necessary.

Loopt: The company uses location information to enable mobile device users to find nearby friends, places, or events. But it minimizes the storage of location data tied to personally-identifiable information. Unless a user specifically geo-tags a location, Loopt only maintains the most recent location associated with that user.[84]

III: GETTING AN EDGE: STANDING UP FOR FREE SPEECH

Companies are increasingly realizing that customer loyalty is closely related to that customer's freedom of speech. Giving a customer a forum to express her views, free from censorship and other limitations, can build a sense of place and community that can enormously benefit the company involved.

PROMOTE FREE SPEECH

DOES OUR BUSINESS PROMOTE COMMUNICATIONS REGARDLESS OF METHOD, TOPIC, OR VIEWPOINT?

Speech can be restricted in many ways, such as by censoring politically sensitive messages or slowing down certain types of online traffic. In either case, businesses can easily alienate their user base and run afoul of the law, generating bad press, outraged clients, and governmental intervention. None of this is good for business.

COMCAST: In 2008 cable giant Comcast was taken to task by the Federal Communications Commission (FCC) and members of Congress for interfering with peer-to-peer technologies such as BitTorrent, thereby intruding upon its users' freedom of speech. The widespread press coverage, along with legislative and administrative inquiries, led Comcast to pledge to change its behavior.[85] Nevertheless, the company has been hit with a class-action lawsuit for making false representations about its service and may be paying for its anti-free speech mistake for years to come.[86]

VERIZON: Verizon made a costly mistake in 2007 when it told NARAL Pro-Choice America that the nonprofit could not use the telecommunication company's network to send text messages to people who had requested information updates. The company reversed its decision after receiving a barrage of complaints from activists, members of the media, and legislators.[87] The FCC opened an investigation into the incident, causing senior executives to apologize repeatedly in both written comments and in-person testimony before the agency.[88]

- **Promote free expression through your product or service.** Your product and community of users will grow and benefit if you open your doors to as many potential users as possible.

Yahoo!: Yahoo! became a free speech leader in 2001 when it refused to cave to pressure from the French government to ban the sale of Nazi memorabilia on the Yahoo! auction site. Yahoo!'s principled stand not only helped to guarantee that Americans would be able to read, think, and speak freely in the marketplace of ideas, but also helped set an important precedent for Internet businesses about the need to stand up to conflicting international laws that threaten the rights of users.[89]

AT&T: Censoring the political speech of the popular rock band Pearl Jam landed AT&T in hot water in 2007. The company censored the first few seconds of its Web cast of the group, replacing the lyrics, "George Bush, find yourself another home," with silence. Although the company quickly reposted an uncensored version, the damage to its reputation could not be reversed as easily.[90]

Do we support the rights of our users to speak anonymously?

Millions of users of all ages rely on the Internet every day as an important resource to search for private information and as a forum for discussion and expression.[91] Many choose to do so anonymously or pseudonymously. Whether it be a domestic violence survivor, an LGBT youth, a government whistleblower reporting an abuse of power, or someone who just wants to keep her online activities private, anonymous online speech is vital so individuals can access and share information without fear or embarrassment.

The courts have repeatedly affirmed that "protections for anonymous speech are vital to democratic discourse."[92] In addition, users "who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identities."[93] Have your company do its part by developing a clear policy that helps to safeguard the anonymous speech of users.

- **Disclose user information only where required by law.** Thoroughly review any subpoenas or demands for information, ensuring 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.

Verizon: In 2003, the Recording Industry Association of America (RIAA) obtained a subpoena under the Digital Millennium Copyright Act (DMCA) ordering Verizon to reveal the identity of a subscriber who had allegedly used peer-to-peer software to share music online.[94] Verizon refused to comply with the subpoena, arguing that it raised serious privacy concerns and was not in fact authorized by the DMCA.[95] Verizon succeeded in defeating the subpoena on appeal,[96] garnering praise for its commitment to user privacy.[97]

- **Give users an opportunity to defend their anonymity.** Provide notice, within no more than seven days of receipt of a subpoena, to each user whose personal information is sought, and inform the user of her right to file a motion to quash (fight) the subpoena. Give the user at least thirty days from the time notice is received to file a motion to quash the subpoena.

YouTube/Google: As part of an ongoing suit against YouTube/Google for copyright infringement,[98] 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.[99] YouTube continued to fight for the privacy of its users and in 2008 reached an agreement with Viacom to anonymize the IDs and IP addresses of non-Google employees in any data conveyed to Viacom.[100]

- **Disclose only required information.** Never disclose more information than is requested by a subpoena or other document.

Yahoo!: The search engine and email giant has been forced to settle multi-million-dollar lawsuits,[101] grilled repeatedly during Congressional hearings,[102] rebuked in the press, and targeted by international protests[103] for turning over identifying information in 2006 about its users to the Chinese government. The Chinese government used this data to link users to pro-democracy activities and to imprison dissidents.

AVOID POLICIES AND PRACTICES THAT CHILL FREE SPEECH

ARE OUR TERMS OF SERVICE CLEAR AND SUFFICIENTLY NARROW TO ACCOMPLISH OUR GOALS WITHOUT DETERRING LEGITIMATE SPEECH?

In drafting terms of service, companies that provide a forum for content or communication need to consider carefully whether they want to be in the business of policing those forums. Terms of use that include vague or overbroad prohibitions, such as speech seen as "offensive," may not only deter users by limiting speech, they may put a company in the undesirable position of having to decide whether and how to respond to disputes between users about alleged violations of terms of service.

- **PROHIBIT ONLY CONTENT OR SPEECH THAT IS ILLEGAL OR DISRUPTS THE PRIMARY FUNCTION OF YOUR SITE OR SERVICE.** Terms of use that are narrowly tailored in this manner will help avoid burdensome monitoring of speech and the potential for inconsistent applications and accusations of bias.

- **PROVIDE AN APPEAL MECHANISM.** Give users a way to appeal any alleged violation and resolve disputes over whether a given piece of content violates the terms of service. Give users an opportunity to present their side of the story before imposing consequences.

- **CLEARLY SPELL OUT THE CONSEQUENCES OF VIOLATING TERMS OF SERVICE.** Allow users to remedy violations rather than automatically deleting content or terminating accounts.

TWITTER: "Microblogging" site Twitter was dragged into drama in 2008 because of its overbroad terms of service. By including a clause that "users must not…harass…or intimidate other Twitter users," it was caught in the middle when two users were in conflict. Rather than taking sides, Twitter did the right thing and modified its terms of service. Of course, it could have avoided the problem if it had finely tuned its terms of service in the beginning to avoid overbroad language such as "harass" or "intimidate."[104]

Do we promote free speech or interfere by monitoring online activities?

Businesses that try to build up marketing profiles by intercepting and tracking Web searches, email, online downloads, and other activities through deep packet inspection interfere with an individual's ability to rely on the Internet as a trusted forum for information and discussion. When users are forced to worry about whether or not they can safely use the Internet to ask questions and communicate about health, sexual orientation, religion, politics, or other sensitive topics, companies face the heavy wrath of consumers and the government.[105] According to one technology consultant, "Users have made it very clear that they don't want any part of ISP monitoring regimes that watch everything they do and say on the Internet."[106]

- **Consider the consequences of monitoring user behavior.** If users believe that their activities are being tracked, they are not only less likely to produce content but also less likely to seek it out. Firmly establishing a policy of not monitoring activity can lead to a more robust forum and a more engaged user base.

Verizon: 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."[107]

- **Refrain from monitoring user activity that does not pertain to your service.** Do not use deep packet inspection, third-party cookies, or other methods to obtain information about online activities of users that occur beyond the boundaries of your service.

NebuAd: The data analysis company's deep packet inspection system, designed to track every Web click for targeted online advertising, led to broad consumer outcry, an inquiry into its 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.[108]

- **Clearly inform users about your monitoring practices and obtain opt-in consent.** It is far better to clearly inform customers about monitoring practices and obtain opt-in consent than to keep these practices a secret and risk widespread outrage, negative press, and potential investigations and lawsuits.

Do we respect free speech as we send takedown requests?

When company content ends up online or consumers' online activities push against the boundaries of copyright or trademark law, a company may consider whether to send a takedown notice to another company to remove online information. If your company is considering such a letter, ensure that you respect others' freedom of expression while you protect your own rights.

- **Use informal channels to open discussions.** Attempt to resolve conflicts without litigation or its threat.

- **Ensure that you have a legal basis to demand that content be taken down.** Do not demand takedown of materials that clearly constitute permitted uses of your material, including fair use under copyright law.

Apple: Apple's attempt to clamp down on blog posts about rumored upcoming products was not only a bad legal strategy, according to the judge, but also bad business strategy, according to *Forbes*. The court held that bloggers have the same right to protect the confidentiality of their sources as do offline reporters; Apple was chastised by *Forbes* for "biting the fans that feed it."[109] Its poor decision to disregard free speech cost the company substantial legal fees as well as its sparkling reputation in the blogosphere.[110]

- **Create Web and email "hotlines" where takedown requests can be contested.** Give individuals and content hosts a quick and easy way to contest or respond to takedown requests through an email hotline. Such a service will allow mistakes and relationships to be repaired without costly litigation. If you send a takedown request, 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.

Viacom: Downplaying fair-use rights led to a lawsuit and media firestorm for Viacom. The company sent Digital Millennium Copyright Act (DMCA) cease-and-desist 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, were making fair use of copyrighted material for activities such as political commentary and parody.[111] Viacom conceded that it had erred in issuing the DMCA notice regarding MoveOn's video and agreed to set up a Web site and email "hotline" promising to review any complaints within one business day and reinstate the video if the takedown request was improper.[112] However, many users and online video enthusiasts remain bitter at the company for its actions.[113]

- **Consider the potential consequences of any attempt to remove content from the Internet.** Cease-and-desist letters and the like often backfire, further fanning the flames of interest in the information that you were hoping to remove and resulting in significant damage to brands and loss of goodwill. As one Internet activist has noted, "The Net interprets censorship as damage and routes around it."[114] 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: 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.[115] 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 of Northern California and a number of other public interest groups became involved in the case. Ultimately, the judge recognized the important free speech principles involved and dissolved the injunction,[116] but not before the controversy—and the original data breach—was broadcast worldwide.

Do we have a clear procedure to protect fair use if we receive a takedown letter?

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 targeted content carefully and do not remove content that constitutes fair use. The document, "Fair Use Principles for User Generated Video Content,"[117] provides advice on avoiding missteps by developing a procedure that properly balances intellectual property and fair use rights.

- **Take fair use 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.[118]

- **Minimize impact on protected activities.** Don't overreact and infringe on protected speech by removing other content posted by the same user, canceling someone's account, or removing user comments posted about a particular content item.

- **Incorporate "three strikes" protections for fair use into any automated filters.** Do not use a filtering mechanism to automatically remove, prevent the uploading of, or block access to content unless that automated system is able to verify that the content has previously been removed pursuant to an undisputed Digital Millennium Copyright Act (DMCA) takedown notice or that all of the following "three strikes" against it apply:

1. The video track matches the video track of a copyrighted work submitted by a content owner
2. The audio track matches the audio track of that same copyrighted work
3. Nearly the entirety of the challenged content is composed of or is included in a single copyrighted work

If there is an automated match, give the user an opportunity to dispute the conclusion of an automated filter, and provide human review if requested.

- **Notify users when a takedown letter is received.** Let users know that content has been taken down by posting information at the location where the content formerly appeared and by directly contacting the content creator or uploader. Include a copy of the takedown letter, and inform the user about her right to issue a DMCA counter-notice and your procedure for acting on such notices. Assist the user in contacting the content owner directly in order to request reconsideration of the takedown notice.

Have we carefully considered the ramifications of any use of digital rights management (DRM) tools?

Although it might be tempting to use DRM to guard your intellectual property, you need to weigh the costs and benefits carefully. Google, Microsoft, Virgin Digital, Sony, and Major League Baseball have all made costly mistakes in rolling out DRM.[119]

Google: 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.[120]

- **Consider the long-term financial costs of DRM.** 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. DRM can force your company to choose between maintaining a distribution model or authentication system that you would rather abandon and alienating users who purchased content that is suddenly unusable. In addition, the administrative costs of maintaining DRM are likely to continue to grow.

- **Evaluate the impact of DRM 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.

- **Evaluate the benefits and effectiveness of DRM.** Rather than providing strong protection for intellectual property, DRM often simply presents a speed bump that will quickly be circumvented. With this in mind, your company might benefit more from encouraging broad distribution and creative uses of your property rather than by attempting to retain tighter control.

CONCLUSION

Your most valuable asset is your customer base. As consumers become more aware of the consequences of online activity and are faced with an ever-expanding array of options, they will increasingly demand products that are not only innovative but also protect their privacy and freedom of expression. Designing your products and policies with privacy and free speech in mind will put you ahead of the curve and help you earn the trust and loyalty of your users while protecting your reputation and your bottom line.

The practical tips and real-life case studies in this Guide are intended to help you begin the process of building robust privacy and free speech protections into your products and business plans. To learn more, please contact the Technology and Civil Liberties Program at the ACLU of Northern California and visit our Web site and blog at **www.aclunc.org/tech**.

APPENDIX A: USEFUL SITES AND RESOURCES

ACLU OF NORTHERN CALIFORNIA

Technology and Civil Liberties Program: http://www.aclunc.org/tech

CALIFORNIA OFFICE OF INFORMATION SECURITY & PRIVACY PROTECTION

Office of Privacy Protection: http://www.oispp.ca.gov/consumer_privacy/default.asp

ELECTRONIC FRONTIER FOUNDATION

Best Practices for Online Service Providers: http://www.eff.org/osp
Privacy Page: http://www.eff.org/Privacy

FEDERAL TRADE COMMISSION

Protecting Personal Information: A Guide for Business:
http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity

BUSINESS FOR SOCIAL RESPONSIBILITY

Home page: http://www.bsr.org

BETTER BUSINESS BUREAU

Security & Privacy—Made Simpler: http://www.bbb.org/securityandprivacy
Sample Privacy Notice: https://www.bbbonline.org/privacy/sample_privacy.asp

GLOBAL NETWORK INITIATIVE

Home page: http://www.globalnetworkinitiative.org

APPENDIX B: PRIVACY AND FREE SPEECH: THE LEGAL LANDSCAPE

The purpose of this Guide is not to provide legal advice. However, it is important for business executives to understand the broad contours of the legal landscape so that they can begin to work proactively with their attorneys to address areas where their products and business services may intersect with free speech and privacy laws. 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.

UNITED STATES CONSTITUTION

The First and Fourth Amendments of the United States Constitution embody fundamental American values; namely, that individuals must be able to speak freely in society and that their private lives must be protected from intrusion. Over the years, these constitutional rights have been interpreted and refined by the Supreme Court and other federal courts. These rights inform Americans' expectations about privacy and freedom of expression when they use the Internet and other technologies.

- **Right to Free Expression:** The First Amendment includes the *right of free speech* and *freedom of the press*.[121] 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.[122]

- **No Unreasonable Search and Seizure:** The Fourth Amendment guards against *unreasonable search and seizure* of people and property by the government.[123] Generally speaking, when an individual has a reasonable expectation of privacy—from the content of telephone calls[124] and emails[125] to documents stored on personal computer hard drives[126]—the government cannot search or seize this information without demonstrating probable cause and obtaining a warrant from a judge.

STATE CONSTITUTIONS

Many states, such as California, also include specific guarantees of privacy and free speech in their state constitutions that further augment the federal constitutional rights.

- **Right to Free Expression:** 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."[127] California courts have held that safeguarding free speech from government intrusion is a paramount concern because speech is "a freedom which is the matrix, the indispensable condition, of nearly every other form of freedom."[128]

- **Right to Privacy:** Article I, section 1 of the California Constitution guarantees an "inalienable" right to privacy.[129] 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.[130] Unlike most constitutional provisions, Article I, section 1 applies to private parties as well as to the government.[131]

- **No Unreasonable Search and Seizure:** Article I, section 13 of the California Constitution also protects data privacy by safeguarding citizens from unlawful governmental searches and seizures more expansively than the parallel version of the Fourth Amendment. In contrast to federal courts,[132] the California Supreme Court has held that Californians do not necessarily relinquish the privacy of personal information when they provide information that is necessary to participate in modern life to third parties.[133] Since it is a "fiction" that providing information to companies to engage in necessary activities is voluntary, individuals do not automatically forfeit their reasonable expectation of privacy in their information.

FEDERAL LAWS

In addition to constitutional protections, federal law also includes specific statutory safeguards for both free expression and privacy.

- **Right to Free Expression:** 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 law is a good example. 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.[134] 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. 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.[135]

- **Right to Privacy:** Although the United States does not have a comprehensive, national privacy law, federal law does protect specific types of data or transactions. Separate statutes safeguard the privacy of telephone, email, Voice-over-Internet Protocol (VoIP), and other electronic communications,[136] financial records,[137] consumer credit information,[138] government records,[139] motor vehicle records,[140] student education records,[141] medical and health records,[142] and video rental records.[143]

STATE LAWS

Many state laws further augment federal constitutional and statutory protections, particularly in the area of privacy. California has been on the forefront in crafting legislation that safeguards privacy rights, and its legislation has often been a model for other states to follow.

- **Privacy Policies:** The California Online Privacy Protection Act (OPPA) requires that all California companies operating a commercial Web site post a conspicuous privacy policy on their site and disclose the kinds of personally identifiable data that they collect and share with third parties. 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.[144]

- **Notice and Consent:** California law also 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.[145]

- **Data Breach Reporting:** California law, as well as that of 42 other states, requires companies to notify individuals in the event that their information is lost or stolen as a result of a data breach.[146]

- **Data Use Restrictions:** California law prohibits publicly posting or displaying Social Security numbers or embedding them on a card[147] and swiping drivers' licenses or recording driver's license information except for very limited circumstances, such as age verification or fraud control.[148]

FEDERAL AND STATE AGENCIES

Several federal agencies regulate companies that collect personal information or provide mediums for free speech. For example, the Federal Trade Commission,[149] which serves to safeguard consumer rights and police anticompetitive practices, has become a forum for formal complaints on issues such as net neutrality and privacy policy enforcement. The Federal Communications Commission,[150] which is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable throughout the United States, allocates communication spectrum resources and issues regulations and rulings concerning the manner in which media companies operate the networks through which third parties communicate and share information.[151]

State agencies, such as public utilities commissions, can also play an important role in enforcing privacy rights. Following the National Security Agency spying revelations, several state utilities commissions were forums for formal complaints and investigations into the role of telecommunications providers.[152]

ENDNOTES

1 Jonathan W. Palmer et al., *The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Third-Parties and Privacy Statements*, 5(3) J. Comp.-Mediated Comm. (Mar. 2000), http://jcmc.indiana.edu/vol5/issue3/palmer.html.

2 *Business Week/Harris Poll: A Growing Threat*, Bus. Week, Mar. 2000, http://www.businessweek.com/2000/00_12/b3673010.htm.

3 Candace Lombardi, *Study: Shoppers Will Pay for Privacy*, CNet News, June 7, 2007, http://www.news.com/2100-1029_3-6189380.html.

4 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.

5 Nicole Wong, *Judge Tells DoJ "No" on Search Queries*, Official Google Blog, http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html.

6 Lisa Guernsey, *Court Says France Can't Censor Yahoo Site*, N.Y. Times, Nov. 9, 2001, at C5, http://query.nytimes.com/gst/fullpage.html?res=9402E1D61F39F93AA35752C1A9679C8B63.

7 Arshad Mohammed, *Record Fine for Data Breach*, Wash. Post, Jan. 27, 2006, at D1, http://www.washingtonpost.com/wp-dyn/content/article/2006/01/26/AR2006012600917.html.

8 Tom Zeller Jr., *ChoicePoint Suffers Fall in Share Price*, N.Y. Times, Feb. 23, 2005, http://www.nytimes.com/2005/02/23/business/23point.html.

9 Ann Broache, *FCC Chief Grills Comcast on BitTorrent Blocking*, Cnet News, Feb. 25, 2008, http://news.cnet.com/8301-10784_3-9878330-7.html.

10 David Kravets, *Comcast Makes a Deal with BitTorrent*, Threat Level, Mar. 27, 2008, http://blog.wired.com/27bstroke6/2008/03/comcast-adoptin.html; Rich Fiscus, *New Class Action Lawsuit Against Comcast in Federal Court, afterdawn.com*, July 23, 2008, http://www.afterdawn.com/news/archive/14884.cfm; Austine Modine, *California Sues Comcast over Bit Torrent Throttling*, Register (London), Nov. 15, 2007, http://www.theregister.co.uk/2007/11/15/comcast_sued_over_bittorrent_blockage/.

11 Mark Hosenball & Michael Isikoff, *Case Dismissed?*, Newsweek, Sep. 26, 2007, http://www.newsweek.com/id/41142/.

12 Electronic Frontier Foundation, *Apple v Does*, http://www.eff.org/cases/apple-v-does.

13 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.

14 Nate Anderson, *Charter Delays NebuAd Rollout After Outcry*, Ars Technica, June 5, 2008, http://arstechnica.com/news.ars/post/20080625-charter-delays-nebuad-rollout-after-outcry.html; Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking*, http://www.freepress.net/files/NebuAd_Report.pdf.

15 For example, Article I, section 13 of the California Constitution provides more protection against unlawful searches and seizures than the parallel version of the Fourth Amendment. In contrast to Smith v. Maryland and United States v. Miller, the California Supreme Court has established that people do not relinquish the privacy of personal information by opening accounts with the companies that furnish basic financial and communication services. People v. Chapman, 36 Cal. 3d 98 (1984) (unlisted telephone directory information); People v. Blair, 25 Cal. 3d 640 (1979) (credit card records and motel telephone calls); Burrows v. Superior Court, 13 Cal. 3d 238 (1975) (bank records).

16 Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 535 (1976).

17 For examples of these laws, *see* Appendix B.

18 Cal. Bus. & Prof. Code § 22575–79 (West 2008), http://caselaw.lp.findlaw.com/cacodes/bpc/22575-22579.html. Companies must also clearly mark their privacy statements, abide by their policies, inform consumers of processes to opt out of data sharing, describe company policy when there are material changes to the privacy policy, and publish a date the policy goes into effect.

19 Chris Jay Hoofnagle & Jen King, *What Californians Understand About Privacy Online*, Sep. 3, 2008, http://www.law.berkeley.edu/samuelsonclinic/files/online_report_final.pdf ("A gulf exists between California consumers' understanding of online rules and common business practices.").

20 Better Business Bureau, *Security and Privacy – Made Simpler* (Mar. 2006), http://us.bbb.org/WWWRoot/storage/16/documents/SecurityPrivacyMadeSimpler.pdf.

21 *Id*.

22 *Sony Sued over Controversial CDs*, BBC News, Nov. 22, 2005, http://news.bbc.co.uk/2/hi/technology/4459620.stm.

23 *Associated Press, Sony BMG Tentatively Settles Suits on Spyware*, Dec. 30 2005, http://www.nytimes.com/2005/12/30/technology/30soft.html.

24 Robert McMillian, Researcher: *Don't Trust Google Toolbar*, Network World, May 30, 2007, http://www.networkworld.com/news/2007/053007-researcher-dont-trust-google.html; Lisa Vaas, *Google Prey to Attack Via Firefox Extension Auto Upgrade*, eWeek.com, June 1, 2007, http://www.eweek.com/c/a/Search/Google-Prey-to-Attack-Via-Firefox-Extension-AutoUpgrade/; Ryan Naraine, *Remote Vulnerability in High-Profile Firefox Extensions (Update)*, Zero Day, May 30, 2007, http://blogs.zdnet.com/security/?p=245.

25 Christopher Soghoian, *A Remote Vulnerability in Firefox Extensions*, Slight Paranoia, May 30, 2007, http://paranoia.dubfire.net/2007/05/remote-vulnerability-in-firefox.html.

26 Ryan Singel, *Google, Yahoo, Facebook Extensions Put Millions of Firefox Users At Risk*, Threat Level, May 29, 2007, http://blog.wired.com/27bstroke6/2007/05/google_yahoo_fa.html.

27 Jim Dalrymple, *Mozilla CEO Criticizes Apple's Stealth Safari Update*, Macworld, Mar. 22, 2008, http://www.pcworld.com/article/id,143752-page,1-c,mozilla/article.html.

28 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.

29 Susannah Fox, *Fast, Mobile Internet Access Adds to Privacy Problems*, Feb. 14, 2008, http://pewresearch.org/pubs/735/mobile-broadband-privacy.

30 Fred von Lohmann, *Subpoenas and Your Privacy*, Deeplinks, Feb. 4, 2006, http://www.eff.org/deeplinks/archives/004385.php.

31 *Google's Half-Hearted Commitment to Transparency*, Threat Level, May 05, 2006, http://blog.wired.com/27bstroke6/2006/05/googles_halfhea.html.

32 Brad Stone, *The Most Privacy-Friendly Search Engine on the Web Is…*, N.Y. Times, July 23, 2007, http://bits.blogs.nytimes.com/2007/07/23/the-most-privacy-friendly-search-engine-on-the-web-is/.

33 Miguel Helft, *Ask.com Puts a Bet on Privacy*, N.Y. Times, Dec. 11, 2007, http://www.nytimes.com/2007/12/11/technology/11ask.html?fta=y.

34 Microsoft Press Pass, *Microsoft Announces Enhanced Privacy Protections for Users*, July 22, 2007, http://www.microsoft.com/presspass/press/2007/jul07/07-22EnhancedPrivacyPrinciplesPR.mspx.

35 Miguel Helft, *Yahoo Limits Retention of Search Records to Three Months*, N.Y. Times, Dec. 17, 2008, at B3,

http://www.nytimes.com/2008/12/18/technology/internet/18yahoo.html.

36 Peter Fleischer et al., *Another Step to Protect User Privacy*, Google Public Policy Blog, Sep. 9, 2008, http://googlepublicpolicy.blogspot.com/2008/09/another-step-to-protect-user-privacy.html; Christopher Soghoian, *Debunking Google's Log Anonymization Propaganda*, Surveillance State, Sep. 11, 2008, http://news.cnet.com/8301-13739_3-10038963-46.html.

37 Ryan Singel, *Under Scrutiny, Search Engines Start to Embrace Privacy; Will ISPs Be Next?* Threat Level, July 23, 2007, http://blog.wired.com/27bstroke6/2007/07/under-scrutinty.html.

38 *Business Week/Harris Poll: A Growing Threat*, Bus. Week, Mar. 2000, http://www.businessweek.com/2000/00_12/b3673010.htm.

39 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.

40 Ryan Singel, *Judge Orders YouTube to Give All User Histories to Viacom*, Threat Level, July 2, 2008, http://blog.wired.com/27bstroke6/2008/07/judge-orders-yo.html.

41 Kurt Opsahl, *Court Ruling Will Expose Viewing Habits of YouTube Users*, Deeplinks, July 2, 2008, http://www.eff.org/deeplinks/2008/07/court-ruling-will-expose-viewing-habits-youtube-us.

42 Barry Collins and Reuters, *Google Wins Agreement to Anonymize YouTube Logs*, PC Pro, July 15, 2008, http://www.pcpro.co.uk/news/212226/google-wins-agreement-to-anonymise-youtube-logs.html.

43 Miguel Helft, *Google Told to Turn over User Data of YouTube*, N.Y. Times, July 4, 2008, http://www.nytimes.com/2008/07/04/technology/04youtube.html.

44 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/.

45 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.

46 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.

47 Ca. Civil Code §§ 1798.83–.84.

48 *Business Week/Harris Poll: A Growing Threat*, Bus. Week, Mar. 2000, http://www.businessweek.com/2000/00_12/b3673010.htm.

49 Joseph Turow, Americans & Online Privacy: The System is Broken 18 (2003).

50 *Id*. at 18, 30.

51 Sam Bhagwat, *Many Miffed over Facebook Feeds*, Stan. Daily, Sep. 19, 2006, http://daily.stanford.edu/article/2006/9/19/manyMiffedOverFacebookFeeds.

52 A Day Without Facebook, http://daywithoutfacebook.blogspot.com/.

53 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.

54 Charlene Li, *Close Encounter with Facebook Beacon*, groundswell, Nov. 21, 2007, http://blogs.forrester.com/charleneli/2007/11/close-encounter.html.

55 Nakashima, *supra* note 53.

56 Pew Internet & American Life Project, Data Memo: Use of Cloud Computing Applications and Services, 5, Sep.

2008, http://www.pewinternet.org/pdfs/PIP_Cloud.Memo.pdf.

57 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.

58 *My Digital Life, Delete, Cancel and Terminate Facebook Profile*, Nov. 11, 2007, http://www.mydigitallife.info/2007/11/04/delete-cancel-and-terminate-facebook-account-and-profile/.

59 Leslie Cauley, *NSA Has Massive Database of Americans' Phone Records*, USA Today, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

60 Electronic Frontier Foundation, *NSA Multi-District Litigation: Documents Relating to All Cases and Dismissed Cases*, http://www.eff.org/cases/att.

61 Mark Hosenball & Michael Isikoff, *Case Dismissed?*, Newsweek, Sep. 26, 2007, http://www.newsweek.com/id/41142/.

62 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.

63 Catherine Tsai, *Ex-Qwest CEO Balked at Request for Records*, Associated Press, May 12, 2006, http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2006/05/12/national/a124748D59.DTL.

64 Zeller, *supra* note 62.

65 Eric Lichtblau, *F.B.I. Gained Unauthorized Access to E-Mail*, N.Y. Times, Feb. 17, 2008, http://www.nytimes.com/2008/02/17/washington/17fisa.html.

66 Nicole Wong, *Judge Tells DoJ "No" on Search Queries*, Official Google Blog, http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html.

67 Ca. Civil Code. § 1798.81, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

68 Federal Trade Commission, Protecting Personal Information—A Guide for Business, http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/.

69 Jon Brodlin, *ChoicePoint Details Data Breach Lessons*, Network World, June 11, 2007, http://www.pcworld.com/article/132795/choicepoint_details_data_breach_lessons.html.

70 Bob Sullivan, *ChoicePoint to Pay $15 Million over Data Breach*, MSNBC, Jan. 26 2006, http://www.msnbc.msn.com/id/11030692/.

71 Tom Zeller, Jr., *ChoicePoint Suffers Fall in Share Price*, N.Y. Times, Feb. 23, 2005, http://nytimes.com/2005/02/23/business/23point.html.

72 Arshad Mohammed, *Record Fine for Data Breach*, Wash. Post, Jan. 27, 2006, at D1, http://www.washingtonpost.com/wp-dyn/content/article/2006/01/26/AR2006012600917.html.

73 E.g., Megan McCarthy, *How Facebook Employees Break Into Your Profile*, Megan McCarthy, Valleywag, Nov. 6, 2007, http://valleywag.com/tech/your-privacy-is-an-illusion/how-facebook-employees-break-into-your-profile-319630.php; Nicholas Carson, *Facebook Employees Meddling With Profiles*, Valleywag, Oct. 29, 2007, http://valleywag.com/tech/rumormonger/facebook-employees-meddling-with-profiles-316105.php; Megan McCarthy, *Facebook Employee Used Login as Dating Tool*, Valleywag, Oct. 29, 2007, http://valleywag.com/tech/your-privacy-is-an-illusion/facebook-employee-used-login-as-dating-tool-316454.php.

74 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.

75 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/SB112251394301198260-2zgDRmLtWgPF5vKgFn1qYJBjaG0_20050827.html.

76 George Ou, *Is Cisco Killing Their Own Reputation?* ZDNet, Aug. 1, 2005, http://blogs.zdnet.com/Ou/?p=85.

77 National Conference of State Legislatures, *State Security Breach Notification Laws*, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

78 *States Demand ChoicePoint Notify ID Theft Victims*, Consumer Affairs, Feb. 17, 2005, 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 ("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.").

79 Jonathan Krim, *LexisNexis Data Breach Bigger Than Estimated*, Wash. Post, Apr. 13, 2005, at E1, http://www.washingtonpost.com/wp-dyn/articles/A45756-2005Apr12.html.

80 Marianne Kolbasuk-McGee, *Laptop Stolen with Personal Data on 300,000 Health Insurance Clients*, Info. Week, Jan. 30, 2008, http://www.informationweek.com/news/security/showArticle.jhtml?articleID=206100526.

81 *USDA Data Breach: 150,000 at Risk*, CNNMoney.com, Apr. 20, 2007, http://money.cnn.com/2007/04/20/technology/credit_monitoring/index.htm.

82 Adam Liptak, *Court Leaves the Door Open for Safety System Wiretaps*, N.Y. Times, Dec. 21, 2003, http://query.nytimes.com/gst/fullpage.html?res=9A0CE5DD133FF932A15751C1A9659C8B63.

83 Nicole Ozer, *BlackHat Presenters Threatened with Patent Suit for Exposing RFID Vulnerabilities*, Bytes and Pieces, Feb. 27, 2007, http://www.aclunc.org/issues/technology/blog/blackhat_presenters_threatened_with_patent_suit_for_exposing_rfid_vulnerabilities.shtml.

84 Loopt, *Privacy Notice,* https://app.loopt.com/loopt/privacyNotice.aspx.

85 Ann Broache, *FCC Chief Grills Comcast on BitTorrent Blocking*, Cnet News, Feb. 25, 2008, http://news.cnet.com/8301-10784_3-9878330-7.html; Ryan Paul, *FCC to Investigate Comcast BitTorrent Blocking*, Ars Technica, Jan. 8, 2008, http://arstechnica.com/news.ars/post/20080108-fcc-to-investigate-comcast-bittorrent-blocking.html; Christopher Soghoian, *Congressman to Comcast: Stop Interfering with BitTorrent*, Surveillance State, Oct. 25, 2007, http://www.news.com/8301-10784_3-9804158-7.html.

86 *See* David Kravets, *Comcast Makes a Deal with BitTorrent*, Threat Level, Mar. 27, 2008, http://blog.wired.com/27bstroke6/2008/03/comcast-adoptin.html; Rich Fiscus, *New Class Action Lawsuit Against Comcast in Federal Court*, afterdawn.com, July 23, 2008, http://www.afterdawn.com/news/archive/14884.cfm; Austine Modine, *California Sues Comcast over Bit Torrent Throttling*, Register (London), Nov. 15, 2007, http://www.theregister.co.uk/2007/11/15/comcast_sued_over_bittorrent_blockage/.

87 Adam Liptak, *Verizon Blocks Messages of Abortion Rights Group*, N.Y. Times, Sep. 27, 2007, http://www.nytimes.com/2007/09/27/us/27verizon.html.

88 Ryan Paul, *FCC Moves Closer to Ruling on SMS Censorship Issue*, Ars Technica, Apr. 11, 2007, http://arstechnica.com/news.ars/post/20080411-fcc-to-examine-sms-short-code-censorship.html.

89 Lisa Guernsey, *Court Says France Can't Censor Yahoo Site*, N.Y. Times, Nov. 9, 2001, at C5, http://query.nytimes.com/gst/fullpage.html?res=9402E1D61F39F93AA35752C1A9679C8B63.

90 Nate Anderson, *Pearl Jam Censored by AT&T, Calls for a Neutral 'Net*, Ars Technica, Aug 09, 2007, http://arstechnica.com/news.ars/post/20070809-pearl-jam-censored-by-att-calls-for-a-neutral-net.html.

91 Pew Internet & American Life Project, Data Memo: Use of Cloud Computing Applications and Services 5, Sep. 2008, http://www.pewinternet.org/pdfs/PIP_Cloud.Memo.pdf. According to this memo, 73% of Americans now use the Internet.

92 NAACP v. Alabama, 357 U.S. 449 (1958) (forbidding the state of Alabama from compelling the NAACP to disclose its membership lists).

93 Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

94 Electronic Frontier Foundation, RIAA v. Verizon Case Archive, http://www.eff.org/cases/riaa-v-verizon-case-archive.

95 Verizon, RIAA v. Verizon: It's About Privacy, Not Piracy, http://newscenter.verizon.com/kit/riaa/vz.html.

96 RIAA v. Verizon Internet Services, 351 F.3d 1229 (D.C. Cir. 2003).

97 *Verizon v. RIAA Ruling Protects Privacy of Internet Users*, Consumer Action, http://www.consumer-action.org/press/articles/verizon_vs_riaa_ruling/.

98 Anne Broache & Greg Sandoval, *Viacom Sues Google over YouTube Clips*, CNet News, Mar. 13, 2007, http://news.cnet.com/Viacom-sues-Google-over-YouTube-clips/2100-1030_3-6166668.html.

99 Viacom v. YouTube, 07-CV-2103, slip op. at 11–14 (S.D.N.Y. July 1, 2008), http://beckermanlegal.com/Documents/viacom_youtube_080702DecisionDiscoveryRulings.pdf.

100 Saul Hansell, *One Subpoena Is All It Takes to Reveal Your Online Life*, N.Y. Times, July 7, 2008, http://bits.blogs.nytimes.com/2008/07/07/the-privacy-risk-from-the-courts/; Stipulation Regarding July 1, 2008 Opinion and Order, Viacom v. YouTube, 07-CV-2103, http://www.docstoc.com/docs/953234/YOUTUBE-V-VIACOM-STIPULATION-REGARDING-JULY-1-2008-ORDER.

101 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.

102 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.

103 *UK Journalists Union Calls for Yahoo Boycott*, oneindia, June 02, 2006, http://news.oneindia.in/2006/06/02/uk-journalists-union-calls-for-yahoo-boycott-1149264801.html.

104 Jacqui Cheng, *Twitter's Controversy over Terms of Service*, Ars Technica, May 26, 2008, http://arstechnica.com/news.ars/post/20080526-twitters-controversy-over-terms-of-service.html.

105 Electronic Privacy Information Center, *Deep Packet Inspection and Privacy*, http://epic.org/privacy/dpi/.

106 Ellen Nakashima, *NebuAd Halts Plans for Web Tracking*, Wash. Post, Sep. 4, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/09/03/AR2008090303566.html.

107 Peter Svensson, *Verizon to Speed Up, Not Police, Internet Traffic*, MSNBC, Mar. 14, 2008, http://www.msnbc.msn.com/id/23630791/.

108 Id.; Nate Anderson, *Charter Delays NebuAd Rollout After Outcry*, Ars Technica, June 5, 2008, http://arstechnica.com/news.ars/post/20080625-charter-delays-nebuad-rollout-after-outcry.html; Robert M. Topolski, *NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking*, http://www.freepress.net/files/NebuAd_Report.pdf.

109 Lisa DiCarlo, *Apple Bites the Fans That Feed It*, Forbes, Jan. 7, 2005, http://www.forbes.com/technology/2005/01/07/cx_ld_0107apple.html.

110 Electronic Frontier Foundation, *Apple v. Does*, http://www.eff.org/cases/apple-v-does.

111 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.

112 Greg Sandoval, *EFF Takes Viacom to Task over YouTube Takedown*, Cnet News, Feb. 15, 2007, http://www.news.com/2100-1026_3-6159548.html.

113 Hee Haw Marketing, *I Hate You Viacom*, Mar. 13, 2007, http://heehawmarketing.typepad.com/hee_haw_marketing/2007/03/i_hate_you_viac.html.

114 John Gilmore, *John Gilmore, Entrepreneur and Civil Libertarian*, http://www.toad.com/gnu/.

115 Jonathan Glater, *Judge Reverses His Order Disabling Website*, N.Y. Times, Mar. 1, 2008, http://www.nytimes.com/2008/03/01/us/01wiki.html

116 Ann Brick, *Free Speech Triumphs in Wikileaks Case*, Bytes and Pieces, Feb. 29, 2008, http://www.aclunc.org/issues/technology/blog/free_speech_triumphs_in_wikileaks_case.shtml; Jemima Kiss, US Judge Reverses Wikileaks Injunction, Guardian, Mar. 3, 2008, http://www.guardian.co.uk/technology/2008/mar/03/wikipedia.web20.

117 *Fair Use Principles for User-Generated Video Content*, http://www.eff.org/files/UGC_Fair_Use_Best_Practices_0.pdf.

118 "Safe harbor" refers to legal protection that shields a company from civil or criminal liability as long as it complies with certain requirements. For more information about safe harbors for technology products, *see* Appendix B.

119 Steve O'Hear, *Five Companies that Sold Customers Down the DRM-Filled River*, Last 100, Apr. 27, 2008, http://www.last100.com/2008/04/27/five-companies-that-sold-customers-down-the-drm-filled-river/.

120 Clint Boulton, *Google Admits to, Fixes Video Refund Gaffe*, Google Watch, Aug. 21, 2007, http://googlewatch.eweek.com/content/google_video/google_admits_to_fixes_video_refund_gaffe.html.

121 U.S. Const. amend. I.

122 McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

123 U.S. Const. amend. IV.

124 Katz v. United States, 389 U.S. 347 (1967).

125 Warshak v. United States, 490 F.3d 55 (6th Cir. 2007), vacated, No. 06-4092 (6th Cir. Oct. 9, 2007).

126 United States v. Barth, 26 F.Supp.2d 929 (W.D. Tex. 1998).

127 Ca. Const. art 1, § 2, http://www.leginfo.ca.gov/.const/.article_1.

128 Ferlauto v. Hamsher, 74 Cal. App. 4th 1394, 1399 (1999).

129 Ca. Const. art 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

130 Ballot Proposition 11 stated: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us." Cal. Sec'y of State, Proposed Amendments to Constitution for the Nov. 7, 1972 Election 27 (1972), http://library.uchastings.edu/ballot_pdf/1972g.pdf.

131 Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1 (1994).

132 Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 535 (1976).

133 People v. Chapman, 36 Cal. 3d 98 (1984) (affirming a right to privacy in unlisted telephone directory information); People v. Blair, 25 Cal. 3d 640 (1979) (credit card records and motel telephone calls); Burrows v. Superior Court, 13 Cal. 3d 238 (1975) (bank records).

134 U.S. Copyright Office, *Fair Use*, revised July 2006, http://www.copyright.gov/fls/fl102.html.

135 Campbell v. Acuff-Rose Music, 510 U.S. 569, 579 (1994).

136 Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq., 2701 et seq., 3121–27 (2008).

137 Right to Financial Privacy Act, 12 U.S.C. §§ 3401 et seq. *See* Electronic Privacy Information Center, *Right to Financial Privacy Act*, http://epic.org/privacy/rfpa/.

138 Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81u. *See* Electronic Privacy Information Center, *The Fair Credit Reporting Act and the Privacy of Your Credit Report*, http://epic.org/privacy/fcra/.

139 Privacy Act of 1974, 5 U.S.C. § 552a, available at http://www.justice.gov/oip/privstat.htm.

140 Drivers Privacy Protection Act, 18 U.S.C. §§ 2721 – 25. *See* Electronic Privacy Information Center, *The Drivers Privacy Protection Act and the Privacy of Your State Motor Vehicle Record*, http://epic.org/privacy/drivers/.

141 Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

142 Electronic Privacy information Center, *Medical Privacy*, http://epic.org/privacy/medical/.

143 Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2008).

144 California Online Privacy Protection Act, Ca. Bus. & Prof. Code §§ 22575–79 (2008), http://caselaw.lp.findlaw.com/cacodes/bpc/22575-22579.html.

145 Ca. Civ. Code §§ 1798.83–.84.

146 Tanya Forsheit, *More Breach Notification Laws—42 States and Counting*, Privacy Law Blog, Apr. 7, 2008, http://privacylaw.proskauer.com/2008/04/articles/security-breach-notification-l/more-breach-notification-laws-42-states-and-counting/.

147 Ca. Civ. Code §§ 1798.85–.86.

148 Ca. Civ. Code § 1798.90.1, http://www.dmv.ca.gov/pubs/vctop/appndxa/civil/civ1798_90_1.htm

149 Federal Trade Commission, http://www.ftc.gov/index.shtml.

150 Federal Communications Commission, *About the FCC*, http://www.fcc.gov/aboutus.html.

151 For example, the FCC recently ruled that Comcast violated the Commission's net neutrality rules by throttling a specific file-sharing application, BitTorrent. Declan McCullagh, *FCC Formally Rules Comcast's Throttling of BitTorrent Was Illegal*, CNet News, Aug. 1, 2008, http://news.cnet.com/8301-13578_3-10004508-38.html.

152 American Civil Liberties Union, *Safe and Free Surveillance*, http://www.aclu.org/safefree/spying/.

Advance Praise

"Startups seeking a way to distinguish themselves in today's tough climate would do well to follow the advice in this primer. The case studies show that ignoring privacy and free speech concerns can do serious damage to a company's customer base, while implementing these tips can help build successful relationships. I consider this primer a must-read for all the companies in our portfolio."

—Omar Mencin, Managing Director,
San Jose Incubator Program

"**Privacy and Free Speech** is both a compelling read and a treasure trove of best practices. Ripped from the headlines stories provide practical advice to help companies bake privacy and free speech safeguards into the technical design process and build corporate understanding of why good privacy and free speech policies matter to the bottom line."

—Deirdre Mulligan, Assistant Professor,
School of Information, UC Berkeley

"This primer makes it clear why privacy is good for business and deftly shows the specific steps companies can take to develop strong data privacy practices. The ACLU of Northern California has created a great tool to help companies achieve effective privacy by design -- building privacy considerations into the product development life cycle early and often, so it's not an afterthought."

—Brian Knapp, Chief Operating Officer,
Loopt, Inc.

ACLUNC.ORG/TECH