

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**.



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 government⁵ 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 Commission⁹ and forced to defend against class-action lawsuits¹⁰ 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 Agency's 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 cases¹⁶ 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.