PRIVACY & FREE SPEECH

IT'S GOOD FOR BUSINESS

3rd Edition

A Publication of the ACLU of California
Online at ITSGOODFOR.BIZ

In the wake of revelations about widespread government spying, massive data breaches, and increasing online censorship, it's no surprise that privacy and free speech have moved to center stage for many users, policymakers, and investors.

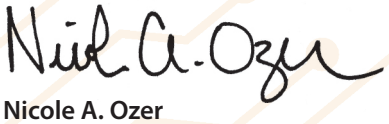
Firsthand experience has taught many companies how decisions about privacy and free speech can impact their business. The failure to take privacy and free speech into account has led to public relations nightmares, costly lawsuits, government investigations, and the loss of users and business partners. Meanwhile, companies taking proactive steps to design user-protective products and business plans have not only avoided these harms but also benefited from positive press and increased customer trust.

Whether your company is a startup or an industry giant, you can protect your users and your bottom line by building privacy and free speech protections into your products and services. This guide gets you started. It walks you through the basic questions you need to address in order to integrate privacy and free speech into your design process. It also provides specific recommendations to help you get started, including dozens of real-life case studies that illustrate how integrating them will help your company thrive.

In the long run, what's good for your users is good for your company. Your users are your greatest asset whether you are selling products, advertising, or data. Meeting, or, better yet, exceeding your users' privacy and free speech expectations can build trust and deepen their relationship with your company and products. Falling short can drive users away, directly affect your company's revenue, and threaten its long-term viability.

This third edition of *Privacy & Free Speech: It's Good for Business* draws from dozens of new case studies to develop specific recommendations that companies of all sizes can implement, including an expanded free speech section addressing issues related to online moderation and censorship. The tools in this guide can help you make the smart, proactive decisions necessary to avoid problems, protect users, and grow your business. Additional resources—including tools to help you produce transparency reports—and continuously-updated content reflecting recent trends and incidents are included in the online version at **itsgoodfor.biz**.

Companies of all sizes face difficult decisions about users' privacy and free speech. Using this guide and sharing it with your colleagues will help your company navigate this thorny terrain and come through with your user base and your reputation intact. Building privacy and free speech protections into your products and services isn't just the right thing to do—it's good for your business, too.



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

CONTENTS

AUTHORS

Matt Cagle, Chris Conley, and Nicole A. Ozer,
Technology and Civil Liberties Project, ACLU of Northern California

CONTRIBUTING WRITERS, THIRD EDITION

Amisha Manek, Eleni Kyriakides, Matthew Callahan

CONTRIBUTING WRITERS, SECOND EDITION

Cliff Helm, Tamar Gubins, Hari O'Connell, Alix McKenna

CONTRIBUTING WRITERS, FIRST EDITION

Christopher Soghoian, Aaron Brauer Rieke, Travis Brandon

DESIGN: Gigi Pandian

PRINTING: Thank you to Inkworks Press for decades of great work

Published by the ACLU of California
Third Edition, January 2016

This publication is supported by the generosity of the ACLU's members and donors and funding from the Digital Trust Foundation

PROMOTING PRIVACY AND FREE SPEECH: A ROADMAP

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

MAKE YOUR PRIVACY PRACTICES STAND OUT

RESPECT YOUR DATA: LIMIT AND PROTECT THE DATA YOU USE

- Do you collect and use only the data you need?
- Do you use data in ways that protect your users?
- Do you collect and store data securely?
- Do you properly handle any sensitive data that you do collect?

PLAN AHEAD: INCORPORATE PRIVACY AND SECURITY FROM START TO FINISH

- Do you have comprehensive privacy and security practices?
- How will you ensure your privacy and security practices are effective?
- How will you protect your users and your company if a breach occurs?

BE TRANSPARENT: GIVE USERS THE ABILITY TO MAKE INFORMED CHOICES

- Do you effectively communicate your privacy practices to your users?
- Do you provide effective notice of data collection?

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

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

GIVE YOUR USERS A PLATFORM TO SPEAK FREELY

ENCOURAGE USERS TO SPEAK FREELY: PROMOTE DIVERSE SPEECH AND SPEAKERS

- Do you encourage users to express themselves as they choose?
- Do you give users control over the content they access and the third-party software they use?
- Do you give users ownership of their speech?

MODERATE CAUTIOUSLY: MINIMIZE YOUR CONTROL OVER USER EXPRESSION

- Do your policies safeguard free expression?
- Is your process fair to users accused of violating your policies?
- Do you apply your policies consistently and fairly?

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

- Do you promote openness and interoperability?
- Do you assert legal control only as a last resort?

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

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

Endnotes available online at **itsgoodfor.biz**

CASE STUDIES

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

Jay-Z App Data Collection "Verges on Parody"
Google Slammed for "Wardriving by Design"
Apple Grilled for Secretly Mapping Customers' Location
Sonic.net Lauded for Reducing Data Retention to Protect Customers
Google Heavily Criticized for Racially-Biased Search Results
Netflix Sued after Sending Not-So-Anonymous User Data to Researchers
AOL Embarrassed by Release of Re-Identifiable Data
CloudFlare Wins Acclaim for Offering Security for Free
Apple Lauded for Encrypting Data by Default
Hookup Apps Grindr and Blendr Slammed for Security Issues
Fitbit Deals with Fireworks after Exposing "Sex Stats"
Blippy Triggers "Nightmare Scenario" by Publishing Credit Card Numbers
MeetMe Pays Up for Hiding That It's Collecting Location Info
Yelp's Collection of Children's Info Gets One-Star Review from the FTC
Uber's "God View" Causes Users to Lose Faith
Facebook Criticized for Poor Internal Security
Citibank Hacked Using "Remarkably Simple Technique"
Lack of Service Provider Oversight Leads to Big Costs for Ad Customers
Target Sued, Accused of Lack of Security Focus after Massive Data Breach
LinkedIn Criticized for Poor Security Practices in Aftermath of Breach
Tesla Accelerates Security Fixes by Cooperating with Researchers
CyberLock Accused of "Abuse of the Legal System" After Threatening Researcher
Uber Hit with Lawsuit for Delayed Notice of Breach
Sony Slammed for "Half-Baked Response" to Security Breach
Spotify's Problem "Isn't Privacy, It's Terrible Communications"
DuckDuckGo Rewarded for Keeping Privacy Simple:
Lookout Gets Shout-Out for Short Form Mobile Privacy Policy Tool
Lenovo Shamed for PCs Secretly Preinstalled with "Nefarious" Adware
Snapchat Investigated for False Claim that Photos "Disappear Forever"
RadioShack Hammered for Unauthorized Sale of Customer Data
Etsy Suffers Privacy "DIY-saster
Verizon's "Supercookie" a "Privacy-Killing Machine"
In-Car Assistance Systems Caught Spying on Drivers
Samsung's "Orwellian" Privacy Policy Invites Allegations of "Smart TV" Spying
Shady Flashlight App Keeps Millions of Users in the Dark
Microsoft in Hot Water After Search of Hotmail Account
Facebook Criticized for Conducting Secret Experiments on Users
Google Buzz Stung for Exposing Private Contact Details
ScanScout Sued After Offering Opt-Out Then Preventing It
Google Faces Record Fines for Bypassing Privacy Settings
Google Praised for Letting Users Order Data "Takeout"
Ashley Madison Angers Users When "Full Delete" Revealed to Be a Fantasy
Netflix Sued for Retaining Records About Former Customers
Apple Draws Attention to New Products by Fighting Centuries-Old Law
Security Firm RSA Faces Backlash for NSA "Backdoor"
Amazon Applauded for Suing to Protect Users
Tech Giants Praised for Supporting Digital Privacy Protections for Californians
Twitter's Resistance to Gag Order Called a "Remarkable Display of Backbone"
Facebook Hailed for Fighting Overbroad Search Warrants
Google Wins "Kudos" for Fighting Demand for Millions of Search Records
Companies Hailed for Issuing Transparency Reports
Tech Giants Praised for Supporting Digital Privacy Protections for Californians
Tech Companies Win Privacy Credibility by Supporting NSA Reforms
Apple Draws Fire for Going "Down the Dark Road of Censorship"
Facebook Called Out for Repeatedly Censoring Drug Policy Reform Discussion
Facebook's "Real Name" Policy Generates Global Outrage
Google Misses Opportunity to Add Pseudonyms to Google+
Instagram Reverses #Curvy Hashtag Ban After User Uproar
Apple Comes Under Fire when Siri Refuses to Provide Abortion Content
League of Legends Praised for Re-Engineering Chat to Reduce Harassment
Twitter's Improved Blocking Tools a Welcome Improvement
Facebook Hailed for Launch of Tor Portal
Apple Accused of "Holding Facetime Hostage"
Instagram's Policy Changes Trigger #instahate:
LinkedIn Pays for Spamming Users' Contact Lists
PayPal Flops as Moral Police
Instagram Receives Worldwide Criticism After Banning Period Photo
Facebook's "Fake Name" Reporting Option Enrages Users
Reddit's "Shadowbanning" Criticized for Leaving Users in the Dark
Facebook Criticized for Censoring ACLU Blog Post About Censorship
Medium Tries to Craft "Human and Practical" Rules for Its Platform
Facebook Faces "Nurse-In" over Breastfeeding Photo Policies
Coca-Cola Slammed for "Homophobic" Promotion
Twitter Triggers "Firestorm of Indignation" After Banning Olympic Journalist
Twitter Use Explodes After Embrace of User-Invented Hashtags
Keurig Faces "Tsunami" of Negative Press for Locking Out Third-Party Pods
Apple Applauded for Removing DRM Controls from Music
Google Forced to Repay Purchasers of Unusable Content
Microsoft Faces "Global Outcry" Over Xbox One DRM
Amazon Forced to Own Up to "Orwellian" Mistake
Katy Perry Ridiculed After Threatening Lawsuit over "Left Shark" Replica
Apple "Bites the Fans that Feed It" by Waging Attack on Bloggers
Sony Embarrassed After Throwing Tantrum Over Leaked Emails
Etsy, YouTube, and Vimeo Commended for Encouraging Informal Resolutions
Google Applauded for Championing First Amendment
Google Cheered for Supporting YouTube Users in Fair Use Fights
WordPress Wins Support for Facing off Against Copyright Abusers
Twitter Gets Public Praise After Standing Up for Political Critics
Avvo Gets Rave Reviews for Protecting Anonymous Speech
Yelp Cheered for Winning Fight to Protect Identities of Reviewers
Google Widely Praised for Opposing Attorney General's Assault on Speech
Facebook Users Like Company's Defense of Free Speech
Websites Thanked by the President for Supporting Net Neutrality
Twitter Commended for "Doing the Right Thing" by Suing for Surveillance Transparency
Companies Praised for "Blackout" to Oppose Laws Undermining Online Speech

MAKE YOUR PRIVACY PRACTICES STAND OUT

The key to developing proper privacy practices is to proactively identify and address potential privacy risks before they happen. By building privacy into your products from the beginning and giving your users the information and tools to protect and control their own personal information, you not only help avoid consequences ranging from scathing media coverage to class action lawsuits, you also make users feel truly invested in your product and build invaluable trust and loyalty.

RESPECT YOUR DATA: LIMIT AND PROTECT THE DATA YOU USE

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

» DO YOU COLLECT AND USE ONLY THE DATA YOU NEED?

Collecting and retaining large amounts of user data—especially if that data has nothing to do with your service—can lead to user mistrust and make your company a target for hackers and legal demands alike. It might even violate your agreement with the platform hosting your app or service. An efficient way to avoid these risks is to collect and retain only the data that you really need for your current product, requesting new data if and when new features require it.

IDENTIFY AND COLLECT THE DATA YOU ACTUALLY NEED.

Your product has a purpose, and that purpose should help you identify the information you actually need. Blindly or willfully grabbing information beyond that can subject your product to bad press, excessive government demands, or even financial penalties. Build trust with your users instead by only collecting information as needed.

85% OF CONSUMERS LIMIT HOW OR WHETHER THEY USE A MOBILE APP BASED ON PRIVACY CONCERNS (2012).[1]

Jay-Z App Data Collection "Verges on Parody": *Jay-Z and Samsung were publicly skewered when their Jay-Z Magna Carta App required so much unnecessary data from users' smartphones that it "verge[d] on parody." The app demanded access to a user's dialed phone numbers, precise GPS location, and details about the user's other apps. This resulted in a complaint with the Federal Trade Commission (FTC) and forced Samsung to publicly defend the app, all of which left press asking: "If Jay-Z wants to know about my phone calls and email accounts, why doesn't he join the National Security Agency?"* [2]

Google Slammed for "Wardriving by Design": *Google found itself in a public relations nightmare when it was revealed in 2010 that the company had captured traffic from private wireless networks. Although the company blamed the mistake on a single engineer, an investigation by the Federal Communications Commission (FCC) revealed that the collection "resulted from a deliberate software design decision" on Google's part. Google was investigated by at least seven countries, has had to defend against multiple class action lawsuits, and paid a $7 million settlement to 38 states and the District of Colombia.*[3]

54% OF MOBILE APP USERS HAVE DECIDED TO NOT INSTALL AN APP WHEN THEY DISCOVERED HOW MUCH PERSONAL INFORMATION THEY WOULD NEED TO SHARE IN ORDER TO USE IT (2012).[4]

Path "Discovered Phoning Home with Your Address Book": *Path came under harsh criticism when a software developer discovered that the company violated its own terms of use by uploading users' entire address books to the cloud. Overwhelming public and press condemnation forced the company to publicly apologize to users and delete the entire collection of user contact information. Path was hit with a class action lawsuit, fined $800,000, and required to conduct annual independent privacy audits for the next 20 years.*[5]

RETAIN DATA ONLY AS LONG AS YOU NEED IT.

Just because you need location information to make your service work doesn't mean you actually need to keep that information. Determine how long you need to keep the data you do collect and delete it once it is no longer necessary to accomplish the purpose for which it was collected. This helps ensure that you're not retaining information that users don't expect you to keep and reduces the potential harm of data breach and other privacy hazards.

Apple Grilled for Secretly Mapping Customers' Location: *Apple was widely criticized, grilled by the Senate and federal agencies, and sued by customers after researchers discovered that iPhones and iPads were collecting and storing a year's worth of unencrypted data about user whereabouts. The company was forced to admit it had erred, reduce location data storage to 7 days or less, stop backing up data on people's computers, and delete information when customers stop using location services.*[6]

Sonic.net Lauded for Reducing Data Retention to Protect Customers: *Sonic.net has been widely lauded for cutting its retention period for user logs down to two weeks. Faced with "a string of legal requests for its users' data," the CEO asked engineers to evaluate the company's actual storage needs to see if reducing data retention could help "protect my customers." The company determined that a two-week retention period was more than adequate to address spam and security issues and properly balanced "an ability to help law enforcement when it's morally right to do so" with protecting users.*[7]

» DO YOU USE DATA IN WAYS THAT PROTECT YOUR USERS?

Failing to consider how you will use the data you collect can undermine the effectiveness of your product and place your users at risk. Limit your use of data to what is necessary to accomplish your product's purpose. Consider the impact of your data-use decisions on both your service and on your users in the real world. Doing so can help you maximize the value of your service while serving your users' best interests online and off.

ENSURE YOU DO NOT USE DATA IN WAYS THAT HARM USERS.

If you aren't careful, making decisions based on data can replicate the biases and discrimination that can exist in the real world, undermining user trust. This is especially true for decisions that impact employment, health, education, lending, or even policing and public safety for users, especially those in vulnerable communities. You can avoid this by carefully scrutinizing the ways in which your data-driven decisions affect your users and taking proactive steps to prevent or counteract these potential harms. Such steps protect the users you have and help attract new ones seeking a fair and equitable service.

Google Heavily Criticized for Racially-Biased Search Results: *Google received a barrage of negative press after an academic study demonstrated that search results for traditionally-black names disproportionately included ads suggestive of a criminal record. The research showed that these names were 25 percent more likely to be served with an arrest-related ad even if the subjects had no criminal record, raising the risk that employers might wrongly assess innocent applicants. Even though both Google and the study itself suggested the results were the innocent product of the company's algorithm, critics attacked the company for its racially-biased results and called the study a "powerful wakeup call."*[8]

MINIMIZE THE LINKS BETWEEN YOUR DATA AND INDIVIDUAL USERS.

Tying identifiable data, including IP addresses or account information, to other records can increase the risk of harm to your users if a breach occurs and, as a result, may make your company more vulnerable to expensive lawsuits and government fines. Explore approaches that effectively mask user identity while preserving the business value of collected information and be particularly careful not to accidentally disclose identifiable data along with other potentially sensitive records.[9]

Netflix Sued After Sending Not-So-Anonymous User Data to Researchers: *In 2009, Netflix faced a flood of criticism, a class action lawsuit, and the loss of user confidence when it released a huge set of improperly anonymized data. While the company took some steps to remove personal identifiers, researchers were able to identify customers by comparing reviews with other online sources. In the aftermath, Netflix was hit with a class action suit filed on behalf of a Netflix customer who was concerned the data would reveal her sexual preference to her intolerant community. After waves of bad press, the case settled out of court for an undisclosed amount.*[10]

» DO YOU COLLECT AND STORE DATA SECURELY?

Your data security practices can make or break your reputation as a company users can trust with their data. Data breaches can be disastrous, leading to lawsuits, fines, and reputational harm. Even small startups should take steps to maintain reasonable security procedures to protect the personal information of users from unauthorized access, destruction, use, modification, or disclosure. The Federal Trade Commission (FTC) and the laws of many states require companies to properly secure user data and impose fines and other enforcement actions for lax security practices.[11]

"BUILDING AND MAINTAINING USER TRUST THROUGH SECURE PRODUCTS IS A CRITICAL FOCUS, AND BY DEFAULT, ALL OF OUR PRODUCTS NEED TO BE SECURE FOR ALL OF OUR USERS AROUND THE GLOBE."
—ALEX STAMOS, FORMER CHIEF SECURITY OFFICER, YAHOO[12]

COLLECT DATA SECURELY.

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

Companies Secure Success with HTTPS by Default: *Since 2010, tech giants including Google, Yahoo, Twitter, Microsoft, and Facebook have received applause for encrypting user connections by default via HTTPS. By moving to HTTPS-by-default, the sites help protect users from monitoring by governments and bad actors. Privacy advocates welcomed Facebook's move to HTTPS as a "huge step forward" while emphasizing that Yahoo's move to encrypt its mail servers was "better late than never."[13]*

CloudFlare Wins Acclaim for Offering Security for Free: *CloudFlare, a major content delivery network, won praise for offering HTTPS encryption for its clients' data by default, for free. In a move widely covered in the press, CloudFlare cofounder and CEO Matthew Prince announced that the company would encrypt its customers' traffic because it was the "right thing to do." The press agreed, describing CloudFlare's business decision as a "present" for the Internet and an "impressive move" that would help the company get more customers by offering great security.[14]*

72% OF CONSUMERS WILL AVOID BUYING FROM COMPANIES THAT THEY BELIEVE DO NOT PROTECT THEIR PERSONAL INFORMATION (2014).[15]

STORE DATA SECURELY.

Data, whether on your servers, laptops, smartphones, or paper, should be secure. Breaches can involve not only high-tech methods such as hacking and phishing but also decidedly low-tech methods such as rooting in dumpsters and stealing from mailboxes. Keep both your physical and network security up to date and use encryption and similar techniques to protect data wherever possible.

Apple Lauded for Encrypting Data by Default: *Apple garnered high marks from its customers and the press when it bucked government opposition and announced that its mobile operating system would automatically encrypt all data stored on the iPhone or iPad. Apple also made encryption easy to use by allowing users to enable it at the same time they set up a password for their device. Commenters described the new feature as a "godsend" that would vastly improve security for the troves of information stored on a modern smartphone, protecting information from both hackers and government surveillance.[16]*

Hookup Apps Grindr and Blendr Slammed for Security Issues: *Location-based dating apps Grindr and Blendr were slammed for failing to protect private accounts with software that was "poorly designed" with "no real security." The apps allow users to seek out like-minded people for dating or socializing, sharing real-time locations and up-to-date profiles complete with pictures. However, research demonstrated that security flaws allowed users to take control of others' profiles, sending pictures and messages on their behalf. Worse yet, it took the apps' parent company a couple of weeks to make fixes even after the flaws were disclosed. Grindr and Blendr's failure to protect their users led to calls for users to delete their accounts despite a public apology from the company's founder and CEO.*[17]

80% OF CONSUMERS ARE MORE LIKELY TO BUY FROM COMPANIES THAT THEY BELIEVE PROTECT THEIR PERSONAL INFORMATION (2014).[18]

» DO YOU PROPERLY HANDLE ANY SENSITIVE DATA THAT YOU DO COLLECT?

Some types of data can be particularly sensitive and require special care. Information such as medical records, financial records, and data concerning children has specific legal requirements that you need to follow. But any data that users consider sensitive should be treated with care, because collecting or disclosing it in ways that your users don't expect or desire creates the potential for user outrage.

CAREFULLY HANDLE ANY DATA THAT YOUR USERS MIGHT CONSIDER SENSITIVE.

Mishaps with information like credit card or financial records, passwords, physical or mental health records, and many other types of sensitive data can have major consequences both for users and your company. Taking special steps to protect this information can protect you and your users from harm.

Fitbit Deals with Fireworks after Exposing "Sex Stats": *Fitbit, an online service that allows users to track their exercise habits, found itself faced with a different set of fireworks during the 2011 Fourth of July weekend when some users discovered that their sexual activity was being broadcast to the public. The company had made all reported data visible to everyone by default without considering the full scope of "exercise data" that it allowed users to include. Although Fitbit "pulled a quickie" by making activity reports private for all new and existing users and even contacting search engines to try to remove results, the damage was already done.*[19]

Blippy Triggers "Nightmare Scenario" by Accidentally Publishing Credit Card Numbers: *In April 2010, Blippy users shared more than they bargained for when a Blippy security flaw turned into a "nightmare scenario" by revealing some users' credit card numbers in search engine results. News of the breach traveled like wildfire and the mood at the startup "quickly went from elation to disbelief to disappointment." Although the company apologized for its mistakes, fixed the problem, hired a chief security officer, and began conducting security audits to prevent future incidents, for many users it was too late. The incident "tainted the service with an aura of mistrust" leading many users to "rush to delete their accounts."* [20]

MeetMe Pays Up for Hiding That It's Collecting Location Info: *MeetMe was met with a barrage of bad press and sued by the City of San Francisco over its collection of location information from teenaged users. The City alleged that MeetMe used a "tangled web of ambiguous and misleading statements" to hide that it was keeping and broadcasting location information on its users. MeetMe was forced to settle the case, pay hundreds of thousands of dollars to the City, and promise to limit the data it revealed about its users.*[21]

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

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

- Any service that deals with electronic communications may be subject to the Electronic Communications Privacy Act.[22]
- Services that are designed for health care providers and related entities may be subject to the Health Insurance Portability and Accountability Act.[23]
- Video content services may be subject to the Video Privacy Protection Act.[24]
- Websites and services that knowingly collect personal information from or that are "directed to children" under 13 may be subject to the Children's Online Privacy Protection Act.[25]
- Other laws may apply if your service handles financial records,[26] consumer credit information,[27] government records,[28] motor vehicle records,[29] or student education records.[30]

"PROTECTING KIDS' PRIVACY ONLINE IS A TOP PRIORITY FOR AMERICA'S PARENTS, AND FOR THE FTC.... A MILLION-DOLLAR PENALTY SHOULD MAKE THAT OBLIGATION CRYSTAL CLEAR."
—DEBORAH PLATT MAJORAS, FORMER FTC CHAIRMAN.[31]

Yelp's Collection of Children's Info Gets One-Star Review from the FTC: *Yelp was investigated by the FTC, fined, and ordered to destroy its records after improperly collecting information from young users. The company had collected information without parental consent, including name, email, and location, from young users of its mobile app even after those users provided a birthday that showed they were under 13. Along with the fine, the FTC also required Yelp to destroy the information it had collected from those users and to submit a report showing how the company would comply with the law.*[32]

PLAN AHEAD: INCORPORATE PRIVACY AND SECURITY FROM START TO FINISH

Thinking about the data you will collect and store while you design your product or service is only one part of "baking in" privacy. You also need processes in place to address issues that might arise in the future. Save time, money, and even your reputation by maintaining privacy and security practices that are holistic, regularly re-evaluated, and prepared for potential data security issues and legal demands.

» DO YOU HAVE COMPREHENSIVE PRIVACY AND SECURITY PRACTICES?

Before your product or service launches, make sure that you have measures in place to protect the data you collect. Many privacy and security fiascos could have been avoided by following well-established best practices. And no matter your company's size, a thorough data security plan can help protect user and proprietary data—and your bottom line as well.

LIMIT AND MONITOR INTERNAL ACCESS TO DATA.

While most businesses imagine shadowy hackers as their biggest security risk, in reality insiders with the ability to access records inappropriately can also pose a significant threat. To minimize this threat, adopt clear rules and technical approaches to prevent inappropriate access, thoroughly train individuals who handle user information in your privacy and security practices, and log and audit data access.

Uber's "God View" Causes Users to Lose Faith: *Uber was hammered with negative press, a #DeleteUber movement, and congressional inquiries after stories emerged that some Uber employees had "God View," allowing them to access ride history and other information about any Uber user. Public outrage over the company's "troubling disregard for customers' privacy" forced Uber to conduct an evaluation of its data privacy program, and in January 2015 it promised to improve its privacy practices based on the firm's recommendations.*[33]

Facebook Criticized for Poor Internal Security: *Users were outraged and the company's reputation was tarnished in 2007 when it came to light that the company had very poor internal security measures. Users demanded change when it was widely reported that the company was not properly safeguarding the private profiles of its users from employee misuse and that employees could view users' private profiles and track which users were viewing particular profiles.*[34]

71% OF EMPLOYEES IN A VARIETY OF FIELDS, INCLUDING SALES AND BUSINESS OPERATIONS, SAID THEY HAVE ACCESS TO DATA THEY SHOULD NOT BE ABLE TO SEE (2014).[35]

KEEP YOUR SYSTEMS AND DATA SECURE FROM OUTSIDE THREATS.

Security breaches can undermine your users' trust and cause them to take their data elsewhere. Many breaches can be prevented by taking steps to protect the systems and data under your direct control. Work with your engineering team and outside experts to implement security best practices such as network activity monitoring, endpoint security for devices that connect with your network, and routine system audits and software updates.[36]

Citibank Hacked Using "Remarkably Simple Technique": *Citibank suffered a major security breach in 2011 and then faced a second wave of criticism for both its lack of preparation and its response to the incident. The company waited three weeks before notifying the 210,000 customers whose data were compromised. Several days later, Citibank announced that, in fact, more than 360,000 accounts had been hacked. When it was revealed that the hackers used a "remarkably simple technique" to exploit a widely recognized vulnerability, critics compared Citibank to a "mansion with a high-tech security system" while "the front door wasn't locked tight."* [37]

PROTECT YOUR ENTIRE DATA ECOSYSTEM.

In addition to securing the data you hold, you need to make sure that your users' data is secure even when it is not on your servers. If third parties are going to have access to your users' data, make sure their privacy and security practices are consistent with your own. Consider how you can formally require third parties to meet your standards and verify compliance with those requirements.

Lack of Service Provider Oversight Leads to Big Costs for Ad Customers: *Large companies such as Best Buy, TiVo, and JPMorgan Chase had millions of their customers' identities and email addresses stolen in 2011 when hackers breached Epsilon, an online marketing provider that was working with the companies. The breach was so large in part because of Epsilon's choice not to segregate the companies' data, something the companies could have required in their contracts with Epsilon. As a result, the companies that worked with Epsilon wound up "paying the price" and were forced to do "damage control" to address the loss of reputation and goodwill.* [38]

» HOW WILL YOU ENSURE YOUR PRIVACY AND SECURITY PRACTICES ARE EFFECTIVE?

As your product line evolves or expands, you will face new challenges related to privacy and security, either because you collect and use more information or because new vulnerabilities and threat models emerge. Even if you can't know exactly what these threats might look like, you can put the pieces into place today to make privacy and security a business priority so that your data and your business are still protected tomorrow.

GROW YOUR PRIVACY AND SECURITY TEAM ALONGSIDE YOUR PRODUCTS.

The assignment of key personnel to oversee privacy and security issues is a great way to proactively address problems and maintain consistent practices throughout a product's lifecycle. For large companies, there might be multiple people whose primary role is to protect privacy and security, including a chief privacy officer and/or chief information security officer, a dedicated privacy group, and specific members of each product team focused on privacy issues. But even two-person startups can benefit by making sure that someone is specifically responsible for thinking about privacy and security issues so that they aren't ignored until it's too late.

Target Sued, Accused of Lack of Security Focus After Massive Data Breach*: Target was hit with a class action lawsuit and widely criticized for its inadequate security practices after hackers stole credit card and sensitive personal information about tens of millions of customers. Target failed to heed several warnings from its security monitoring tools specifically designed to detect an intrusion as information "gushed out of its mainframe." Security officials noted that the company's lack of a Chief Security Officer and "security-oriented culture" rendered it incapable of adequately responding to the incident. As a result, Target's profits and consumer trust dwindled while it incurred lawsuits and costs that "could run into the billions."* [39]

LinkedIn Criticized for Poor Security Practices in Aftermath of Breach: *LinkedIn was heavily criticized after hackers obtained nearly 6.5 million passwords and posted them on the web. Even though LinkedIn immediately acknowledged the leak and attempted to patch up its security, the company was criticized for its previous lax attitude toward security, including its lack of key security personnel, which resulted in the company being unprepared for a preventable attack.*[40]

RE-EVALUATE YOUR PRIVACY AND SECURITY PRACTICES WHEN YOU MAKE MAJOR CHANGES.

Failing to recognize your changing privacy and security needs as your company and products evolve can create new risks for your users and your reputation. Instead, use regular assessments to evaluate and update your privacy and security practices. Assessments should take place before a new product is launched and whenever major changes are implemented.

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

Seeking and accepting advice from outside your company can bring a new perspective to your privacy and security risks, helping you identify and fix potential problems before they impact your users and your business. Consultants and independent researchers can help you identify flaws in your products or your infrastructure and fix them before they lead to a major incident. Work with researchers who responsibly disclose flaws in your product rather than risk a public relations disaster by trying to silence their work.[41]

Tesla Accelerates Security Fixes by Cooperating with Researchers: *Tesla was able to quickly address a vulnerability in the software for one of its cars by cooperating with researchers who discovered the flaw. Even before the bug was known, Tesla implemented a "coordinated disclosure policy" to pay researchers for finding and submitting vulnerabilities. When researchers found a security hole in one of Tesla's cars, Tesla quickly fixed the problem and publicly thanked the researchers by co-presenting with them at a conference. The company enjoyed praise by industry experts and the public for its strong pro-security stance.*[42]

CyberLock Accused of "Abuse of the Legal System" After Threatening Researcher: *Electronic lock maker CyberLock drew harsh criticism for its "abuse of the legal system" when it sent threatening legal letters to a researcher to prevent him from publicly revealing his research about its products. The researcher uncovered security flaws that undermined the protections promised by CyberLock's locks and notified the company of his findings. In response, the company slapped the researcher with threatening legal letters to discourage him from publicly revealing his research, sparking media criticism and outraging members of the security community.*[43]

» HOW WILL YOU PROTECT YOUR USERS AND YOUR COMPANY IF A BREACH OCCURS?

Implementing and following best practices can help you reduce the risk of a data breach—but it cannot eliminate that risk entirely. The best way to mitigate damage from a breach is to be prepared to act immediately to repair the damage to your users and your brand.

PROTECT YOUR USERS BY NOTIFYING THEM AS QUICKLY AS POSSIBLE.

Notifying users in the event of a data breach is required by law in most of the United States.[44] Failing to follow these laws can result in expensive lawsuits. In addition, keeping a breach hidden could result in even more outrage from users and the press. Instead, promptly and thoroughly notify your users to help them prevent identity theft and other harms and to start to repair your relationship with them.

Uber Hit with Lawsuit for Delayed Notice of Breach: *App-based car service Uber was hit with a class action lawsuit after accidentally posting the personal information of about 50,000 drivers and waiting nearly five months to disclose the incident. When Uber did not offer an explanation for the delay, it faced flack for its "unsavory and unprincipled" practices. Moreover, Uber was sued for allegedly violating California law, which requires companies to notify those affected "without unreasonable delay."* [45]

Sony Slammed for "Half-Baked Response" to Security Breach: *Sony "will have a long road ahead to win back the trust of gamers" after a security breach that shut down its PlayStation Network in spring 2011 turned into a major privacy fiasco. The company waited five days before revealing that user data, including passwords, had been compromised and then disclosed weeks later that at least some credit card information had been lost in the incident as well. In the aftermath of the breach, Sony was sued for failing to secure its data and also excoriated by Congress, with Rep. Bono Mack (R-CA) describing its behavior as a "half-hearted, half-baked response [that] is not going to fly in the future."* [46]

TAKE STEPS TO PREVENT FURTHER HARM.

If you suffer a breach, maintaining your customers' good will requires that you do everything in your power to protect them from further harm. Contact law enforcement officials, banks, credit payment processors, and credit agencies to try to head off fraud and other harm. Taking steps such as offering free credit monitoring to any user whose data was exposed can mitigate the damage both to your users and to your reputation. By being forthright about the problem and offering clear guidance and assistance to your users about how they can protect and monitor their own privacy, you will reassure them that you take your business responsibilities—and their privacy—seriously.

BUSINESSES FAIL TO OFFER MITIGATION SERVICES SUCH AS CREDIT MONITORING 29% OF THE TIME IN CASES WHERE IT WOULD BE HELPFUL.
—CALIFORNIA ATTORNEY GENERAL'S 2014 DATA BREACH REPORT [47]

BE TRANSPARENT: GIVE USERS THE ABILITY TO MAKE INFORMED CHOICES

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

» DO YOU EFFECTIVELY COMMUNICATE YOUR PRIVACY PRACTICES TO YOUR USERS?

California law requires any commercial website or mobile app that collects personal information about California residents to post a conspicuous privacy policy.[48] But a privacy policy filled with legal language won't help your users understand how your company actually protects their information. Clearly and effectively communicate your privacy practices to users in order to avoid surprises or misunderstandings that can quickly lead to user backlash, investigations, and lawsuits.

CLEARLY EXPLAIN WHAT DATA YOU COLLECT AND HOW YOU USE IT.

Many privacy fiascos are triggered when users are unpleasantly surprised to learn how a service actually works and how their personal data has been or could be collected and used. You can help avoid surprises that will lead to user backlash by making your privacy practices accessible and easy to understand. Having short-form privacy policies for mobile, Frequently Asked Questions pages, and visual ways of communicating like videos and graphs can also help your users understand your privacy practices.

Spotify's Problem "Isn't Privacy, It's Terrible Communications": *Spotify was widely criticized for the difficult-to-decipher language in an update to its privacy policy released in 2015. Many users were confused by the policy and believed that Spotify wanted to track users "like a jealous ex." Spotify's CEO issued a public apology and rewrote the policy to be clearer, but the public relations damage from the "ridiculous" policy was done.*[49]

DuckDuckGo Rewarded for Keeping Privacy Simple: *Search engine DuckDuckGo reaped the benefits of having clear and privacy-friendly policies written in understandable English. Its privacy policy starts with a clear statement that "DuckDuckGo does not collect or share personal information," followed by an explanation about why users "should care." This policy has been highlighted by the press, helping the company experience a 600 percent increase in traffic in the wake of the 2013 NSA revelations.*[50]

Lookout Gets Shout-Out for Short-Form Mobile Privacy Policy Tool: *Lookout, a mobile privacy and security startup, attracted lots of positive attention for building a tool to help mobile apps produce short-form privacy policies. The company decided to build and release the tool after receiving positive feedback for its own mobile-friendly policy. Lookout was lauded for taking "major steps to empower consumers" that "could change the game on mobile app transparency."* [51]

CLEARLY EXPLAIN HOW INFORMATION IS SHARED WITH OTHERS.

Because many users are particularly concerned about how and whether their data is shared with third parties, making sure that your users understand your data-sharing practices is essential to earn their trust and avoid misunderstandings or backlash. Make it easy for users to understand who can view or access their information, how it can be used, and how your company ensures that it is not misused.

Lenovo Shamed for PCs Secretly Preinstalled with "Nefarious" Adware: *Lenovo was lambasted in the press after security researchers revealed that the PC maker was selling computers secretly preinstalled with "nefarious" adware that not only collected information about users' online activity but also made encrypted web sessions vulnerable to attacks. The adware, from a company called Superfish, posed a sufficiently serious threat that the Department of Homeland Security warned Lenovo customers to remove it immediately. Lenovo's actions not only damaged its reputation, but also exposed it to a class action lawsuit for "compromising user security and privacy."* [52]

80% OF SURVEY RESPONDENTS WANTED MORE REGULATIONS TO PREVENT ORGANIZATIONS FROM REPURPOSING PERSONAL DATA FOR THIRD PARTY USE (2014).[53]

FOLLOW YOUR PRIVACY POLICY.

Your privacy policy is a contract with your users. Failing to live up to your privacy promises may not only anger users but also result in fines and lawsuits. Make sure that your privacy policy is accurate and that everyone who has access to personal data understands and complies with it.

Snapchat Investigated for False Claim that Photos "Disappear Forever": *Snapchat was punished by the FTC for misrepresenting its security and privacy practices, including its fundamental promise that photos and videos "disappear forever" after being viewed. The FTC also accused Snapchat of collecting user geolocation data and data from user address books despite promising not do so in its privacy policy. As part of its settlement with the FTC, Snapchat was forced to agree to independent oversight of its privacy program for 20 years.*[54]

RadioShack Hammered for Unauthorized Sale of Customer Data: *RadioShack was widely condemned when it announced plans to sell tens of millions of customers' data in bankruptcy proceedings even though it had promised not to sell or share any of that information in its privacy policy. The sale was put on hold after the Texas and Tennessee attorneys general filed suit and the FTC requested that RadioShack restrict the use of any data sold given the "potential deceptive nature of the transfer." The press chimed in, calling the company's behavior "obnoxious." The company ultimately was forced to destroy most of the data at issue and require the purchaser to comply with RadioShack's prior privacy promises.*[55]

NOTIFY USERS ABOUT ANY CHANGES BEFORE THEY TAKE EFFECT.

It is more likely that users will embrace new or improved functionality or changes to your privacy practices if they are not surprised. Prominently disclosing meaningful changes in the way your product or service collects data, giving users the opportunity to provide input and express concerns, and obtaining opt-in consent can help prevent controversies for your company.[56]

Etsy Suffers Privacy "DIY-saster": *In early 2011, online marketplace Etsy suffered a "social media DIY-saster" after making shoppers' feedback posts, purchases, and, in some cases, real names publicly visible and searchable without adequately notifying users. Because the company announced the change only on a forum rarely used by buyers, it was accused of refusing to take its users' privacy concerns seriously, leading the incident to be described as "Etsy's privacy Valdez." The online marketplace has since changed its default privacy settings, apologized for its behavior, and acknowledged that it will have to "work hard to regain your trust." For many users, however, this may have been the "last straw."* [57]

IT WOULD TAKE AN AVERAGE AMERICAN UP TO 293 HOURS PER YEAR JUST TO SKIM THE PRIVACY POLICY OF EVERY SITE SHE VISITED (2012).[58]

» DO YOU PROVIDE EFFECTIVE NOTICE OF DATA COLLECTION?

If your company's product includes sensors or otherwise captures data about your users' activities, location, or other attributes, you need to clearly inform users of its capabilities and notify them whenever it is active. Failing to do so can lead to user outrage and legal consequences when users discover that your product has been secretly collecting information about them.

NOTIFY USERS WHENEVER MONITORING IS ACTIVE.

Users should be aware when a device or product is collecting information or when a microphone, camera, or other sensor is turned on. If your product is capable of collecting and transmitting user information surreptitiously, the discovery of those practices can severely erode user trust.

Verizon's "Supercookie" a "Privacy-Killing Machine": *Verizon faced the wrath of consumers, privacy advocates, and the United States Senate for using "supercookies" to track the Internet activity of more than 100 million customers without their knowledge or consent. Described as "privacy-killing machines," supercookies allowed Verizon to monitor customers wherever they went on the Internet, even if they had taken steps to browse anonymously. After months of intense criticism, Verizon finally relented and allowed customers to opt out of the tracking.*[59]

In-Car Assistance Systems Caught Spying on Drivers: *Users who purchased in-car assistance systems they hoped would help them find their stolen cars or get help in an emergency were not happy to learn that these systems could be used to spy on them. Because some of these systems can be remotely activated without alerting the occupants of the vehicle, they have been secretly used by law enforcement to track individuals and silently snoop on their conversations. The press widely reported this undisclosed "feature" of such systems.*[60]

74% OF PEOPLE ARE CONCERNED ABOUT COMPANIES MONITORING THEIR ONLINE ACTIVITIES AND SELLING THAT INFORMATION WITHOUT THEIR EXPLICIT CONSENT (2014).[61]

MAKE USERS AWARE WHEN YOU COLLECT DATA IN UNEXPECTED WAYS.

Today's market of sensor-rich and interconnected devices includes everything from thermostats to cars and is commonly referred to as the "Internet of Things." Many of these devices are able to inconspicuously collect sensitive data about private life, making clear and creative privacy explanations all the more important. Companies that fail to explain how these devices collect and use data may find themselves in hot water.

Samsung's "Orwellian" Privacy Policy Invites Allegations of "Smart TV" Spying: *Samsung faced an FTC complaint as well as a congressional inquiry after reports questioned whether its voice-activated smart TVs might be eavesdropping on users. Users and the press were outraged after noticing that Samsung's "Orwellian" privacy policy suggested that its smart TVs were recording conversations and transmitting that data unencrypted to third parties. In response to the uproar, which included days of negative press coverage and triggered a U.S. senator's inquiry, Samsung updated its privacy policy, but many found the vague modifications insufficient to assuage fears and rebuild consumer trust.[62]*

Shady Flashlight App Keeps Millions of Users in the Dark: *Goldenshores Technologies, makers of the "Brightest Flashlight Free" Android app, faced legal action from the FTC for deceiving users about its data sharing practices. The app failed to disclose in its privacy policy that it was transmitting precise location information and unique device identifiers to advertisers and other third parties. What's worse, the app made a pretense of allowing users to opt out of sharing but then proceeded to share their information anyway. Goldenshores was lambasted in the press and the FTC eventually ordered the app-maker to clarify its practices for users and delete all user information in its possession.[63]*

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

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

» DO YOU IDENTIFY AND RESPECT USER EXPECTATIONS?

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

IDENTIFY AND RESPECT EXISTING USER EXPECTATIONS.

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

Microsoft in Hot Water After Search of Hotmail Account: *Microsoft was roundly criticized for broadly interpreting its own privacy policy to justify searching a Hotmail account for the company's benefit. As part of a search for an insider who had leaked company information, Microsoft scoured the Hotmail inbox of the blogger publishing information on the leaks. The company initially defended its actions when the search became public, claiming its privacy policy authorized the search. After significant backlash from users and the press, Microsoft reversed its position, apologized for its actions, and changed its privacy policy to require the company to refer matters involving Microsoft property to law enforcement.*[64]

Facebook Criticized for Conducting Secret Experiments on Users: *Facebook was lambasted in the press for conducting an "emotional manipulation" study on its users without oversight or user permission. Facebook's experiment involved selectively showing users certain kinds of posts by their friends and determining whether the altered feed affected the users' moods. When the study was revealed, both the press and public railed against the company for treating users like guinea pigs without their informed consent. After weeks of bad press and the scrutiny of scientific groups, Facebook publicly apologized for the move and the company agreed to new procedures designed to protect users in future research.*[65]

USE OPT-IN FOR ANY CHANGES THAT MIGHT CONFLICT WITH USER EXPECTATIONS.

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

Google Buzz Stung for Exposing Private Contact Details: *In early 2010, Google tried to jump on the social networking bandwagon by releasing its own service, Google Buzz. But the biggest buzz about the new service focused on privacy because Google pre-populated "following" lists with frequent chat and email contacts and made that information public by default. Media articles called Buzz a "privacy nightmare" and warned that Buzz "managed to completely overstep the bounds of personal privacy." Within weeks of launch, Google Buzz became the subject of an FTC privacy complaint and a class action lawsuit that resulted in an $8.5 million settlement. Google ultimately axed the entire Buzz service.*[66]

87% OF GLOBAL CONSUMERS THINK THERE SHOULD BE LAWS TO PROHIBIT COMPANIES BUYING AND SELLING DATA WITHOUT OPT-IN CONSENT (2014).[67]

» DO YOU GIVE USERS CONTROL OVER THEIR PERSONAL INFORMATION?

Users want to be in control of how their information is used or shared. Failing to obtain explicit consent to use or share personal information, or making it difficult for users to remove themselves from lists or terminate use of products, risks alienating existing users and discouraging others from joining. Putting your users in control may lead to a far more positive relationship.

"[W]HEN PRIVACY INFORMATION IS MADE MORE SALIENT AND ACCESSIBLE, SOME CONSUMERS ARE WILLING TO PAY A PREMIUM TO PURCHASE FROM PRIVACY PROTECTIVE WEBSITES."
—CARNEGIE MELLON STUDY ON PRIVACY PRACTICES (2011)[68]

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

Although your service may require certain data to function properly, giving users the ability to choose how and whether any other information is collected, used, or shared can increase trust and even use of your service by providing users with the ability to choose the context in which they participate. You can increase user control by providing easy-to-use tools that allow users to understand and select their privacy preferences and by respecting "Do Not Track" browser settings and similar mechanisms that allow your users to communicate their wishes.

ScanScout Sued After Offering Opt-Out Then Preventing It: *In 2011, ScanScout, an online video advertising network, was investigated by the FTC and hit with a class action lawsuit for its deceptive practice of using persistent "supercookies" to track users online. Although ScanScout's privacy policy stated that users could change their browser settings to "opt out" of its information tracking, the company actually used technology designed to prevent users from doing so. ScanScout settled with the FTC by submitting to ongoing oversight of the company's privacy practices.* [69]

Google Faces Record Fines for Bypassing Privacy Settings: *In 2012, Google agreed to pay a record $22.5 million FTC fine*[70] *and was hit with multiple lawsuits for violating its own statements and bypassing privacy settings on Apple's Safari web browser. Although Google had told Safari users that they could use the browser's privacy settings to prevent tracking, the company also deployed code that enabled its own software to bypass these settings. Critics noted that the incident "represents another PR blow" for Google and called for the company to "make a pro-privacy offering to restore your users' trust."* [71]

93% OF U.S. CONSUMERS BELIEVE COMPANIES SHOULD ALWAYS ASK FOR PERMISSION BEFORE USING PERSONAL INFORMATION, AND 72% WANT THE RIGHT TO OPT OUT OF ONLINE TRACKING (2008).[72]

88% OF U.S. CONSUMERS SAID THEY WOULD PREFER TO DETERMINE HOW THEIR DATA CAN BE USED (2015).[73]

ALLOW USERS TO REVIEW, CORRECT, AND EXPORT THEIR OWN DATA.

Allowing users to review and maintain their own records (with appropriate logging and oversight) and export their own data can give them a better understanding of the privacy consequences of their actions. Making it clear that users can modify or export their data and use it as they see fit may encourage users to feel more comfortable with your service and boost your company's reputation in the process. In addition, users are often in the best position to fix mistakes in your data and thus increase its business and market value.

Google Praised for Letting Users Order Data "Takeout": *Google has been widely praised for allowing users to export data from Google services for their own purposes. The service, known as Google Takeout, provides users with a centralized place to export their data from over twenty supported services, including Gmail, Drive, YouTube, and Hangouts. Reporters noted how the export feature both "makes perfect sense from a business perspective" and was "a positive step that'll be beneficial to [Google's] users."* [74]

ALLOW USERS TO DELETE CONTENT OR TERMINATE THEIR ACCOUNT.

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

Ashley Madison Angers Users When "Full Delete" Revealed to Be a Fantasy: *The racy online service Ashley Madison received strong public criticism and was dragged into court after a breach revealed the service retained information about users who had paid the company an additional fee to delete their accounts. Even though Ashley Madison claimed that its $19 "Full Delete" service removed "all information relating to a user's profile and communications activity," a data breach later revealed that it retained a large amount of user information, including the user's birthdate, GPS coordinates, gender, ethnicity, "turn-ons," and more. As a result, Ashley Madison has been accused of misrepresenting the feature in multiple lawsuits and the media.* [75]

Netflix Sued for Retaining Records About Former Customers: *In 2012, Netflix settled a class action lawsuit alleging that it retained records about former customers in violation of the Video Privacy Protection Act. The company ultimately settled the lawsuit by agreeing to pay $9 million and change its policy to permanently de-associate records from accounts that had been inactive for more than 365 days.* [76]

» DO YOU STAND UP FOR YOUR USERS' PRIVACY?

Proactively protecting privacy can reduce burdens on your company and earn your users' trust. Many of the privacy laws in the United States are badly outdated, resulting in a patchwork system of legal protection for privacy riddled with loopholes and gray areas. This uncertainty may subject your company to legally questionable demands for user data, and while fighting back can involve legal costs, it also gives you an opportunity to establish a reputation as a champion of your users' rights.

COMPLY ONLY WITH VALID DEMANDS FOR INFORMATION.

If you suspect that a demand for information is invalid or unenforceable, evaluate your options and consider formal and informal avenues of challenging it. Helping create stronger, clearer privacy laws will make compliance easier in the future, and your users will reward you for fighting for their interests.

Apple Draws Attention to New Products by Fighting Centuries-Old Law: *Apple drew attention to its privacy-friendly practices when it refused to comply with a warrant demanding that it access data on a customer's cell phone. In 2015, Apple received a court order to provide data from an iPhone based on the two-hundred-year-old "All Writs Act." Rather than complying, Apple challenged the order in court. Apple's action earned it—and its new encrypted-by-default iPhones—widespread media attention.*[77]

Security Firm RSA Faces Backlash for NSA "Backdoor": *Prominent security firm RSA faced a massive backlash after reports that it had been paid by the NSA to adopt compromised encryption tools. The story stoked rumors that the spy agency had "backdoor" access to the encrypted communications of the company's customers, severely damaging trust in the RSA brand. Security experts and the press boycotted the company's prestigious annual conference and called for RSA to "come clean."* [78]

Amazon Applauded for Suing to Protect Users: *Amazon was praised for its commitment to protecting the privacy of users in 2010 after refusing a demand to turn over records detailing more than 50 million purchases of North Carolina residents to that state's Department of Revenue. To protect its customers and their ability to "purchase sensitive or unpopular material," the company filed suit against the state agency with the support of the ACLU. After a judge ruled against North Carolina, the state ultimately agreed not to demand the titles or other identifying information about books, movies, and similar material. As a result, Amazon was applauded for defending "the free speech and privacy rights of Amazon.com customers."* [79]

PROMPTLY NOTIFY USERS AND GIVE THEM AN OPPORTUNITY TO RESPOND.

One of the simplest ways to protect your users is by giving them the opportunity to protect themselves. If and when you do receive a demand for information, notify the affected users if possible and inform them that they should explore potential legal options to challenge the demand. And give the user as much time as possible before complying with the demand yourself. Doing so costs very little but still clearly positions you as your users' ally.

Tech Companies Praised for Notifying Users About Data Demands: *Tech companies including Facebook, Apple, Google, and Microsoft won acclaim when they revised their policies to consistently notify users about government demands for their data. The changes were described as proudly "defiant" after the revelations of the NSA, drawing praise from media and privacy advocates alike.*[80]

Twitter's Resistance to Gag Order Called a "Remarkable Display of Backbone": *In January 2011, Twitter was applauded for its "remarkable display of backbone" in standing up for its users' privacy and free speech rights by challenging the secrecy of a demand from the Department of Justice (DOJ). The DOJ obtained a court order requiring Twitter to turn over those records about users associated with WikiLeaks, including contact and credit card information and the identities of other individuals who communicated with those users. The court also issued a "gag order" prohibiting Twitter from telling these users about the demand. However, Twitter fought back against the gag order and won, allowing the company to uphold its promise to notify users of government demands where legally possible.*[81]

DISCLOSE ONLY REQUIRED INFORMATION.

If you are required to turn over user information, make sure you don't turn over more than you must. Turning over months of records when only a single week's worth of data is required or disclosing user transactions outside the scope of the demand can lead to legal liability as well as the loss of user trust.[82] On the other hand, pushing back against overbroad demands can help you limit your own costs and build a reputation for standing up for your users.

Facebook Hailed for Fighting Overbroad Search Warrants: *Facebook was hailed by the media after it "vehemently" opposed a set of warrants from the New York District Attorney's Office demanding information on 381 users, arguing that the warrants were overbroad. Although Facebook ultimately lost its legal battle to prevent disclosure, it was able to persuade the District Attorney to unseal the case, permitting Facebook to notify the affected users. As a result of its efforts, Facebook was applauded for taking a strong stance for user privacy as other companies "rall[ied] behind" the company's stance on the issue.*[83]

Google Wins "Kudos" for Fighting Demand for Millions of Search Records: *Google was praised, and its competitors chastised, when in 2005 the company challenged a subpoena from the federal Department of Justice (DOJ) that demanded every single search query the company had received over a two-month period. Google emerged the victor, with the court holding that the government was only entitled to a limited data set including no personal information. By standing up for privacy, Google reaped a bonanza of positive public and media attention, including favorable comparisons with competitors who "meekly complied" with similar demands.*[84]

PUBLICLY RELEASE A TRANSPARENCY REPORT DETAILING DATA DEMANDS.

Being transparent about how many demands for information you receive and when you comply with these demands, can benefit not only your users but your reputation as well, giving users as much information as possible about information demands from third parties and the steps you have taken in response. The easiest way to accomplish this is by producing a biannual or annual "transparency report" documenting and providing detail about these demands. The ACLU of California has created a set of tools (online at **itsgoodfor.biz/resources**) to help you track and respond to demands for user information and produce your own transparency reports.

Companies Hailed for Issuing Transparency Reports: *Numerous companies, including Apple, Dropbox, Facebook, and Reddit have been applauded for issuing regular transparency reports in the wake of the disclosure of information about NSA spying by Edward Snowden. These reports detail how often the company received and responded to government requests for its users' data. Press described the trend toward issuing such reports as so overwhelming as to become "commonplace for Internet companies," while privacy advocates called the information "invaluable."* [85]

PUSH FOR STRONGER LAWS TO PROTECT USER PRIVACY.

Although privacy issues are increasingly on the radar of the public, press, lawmakers, and regulators, legal protections for online privacy are still badly outdated.[86] This puts user privacy at risk and subjects companies to demands for information that may or may not be legitimate. Joining coalitions with advocates and other companies and supporting efforts to reform privacy law at the state and federal level may not only clarify your own legal obligations, it can also help to establish your reputation as a company invested in protecting your users' privacy.

Tech Giants Praised for Supporting Digital Privacy Protections for Californians: *Technology companies including Facebook, Twitter, Dropbox, and Google were praised for supporting the California Electronic Communications Privacy Act. The law, which was successfully enacted and went into effect in January 2016, requires California law enforcement to get a warrant to gain access to electronic information, including email and text messages, online documents, sensitive metadata, and location information. Press warmly applauded the companies for "taking note of customers' privacy concerns" in uniting behind the effort.*[87]

Tech Companies Win Privacy Credibility by Supporting NSA Reforms: *Technology titans, including Yahoo, Apple, and Microsoft won acclaim for consistently calling for reforms to U.S. surveillance after the Snowden revelations. Through joint public campaigns, the companies demanded limits on domestic and foreign surveillance by the federal government. The USA Freedom Act, one of the reform bills supported by the companies, became law in mid-2015. Legislators seized on the tech companies move as a contribution to "the growing momentum" around reform, and privacy advocates called it a "game changer."* [88]

GIVE YOUR USERS A PLATFORM TO SPEAK FREELY

The Internet is a key catalyst of free expression around the world. As a result, companies that allow users to communicate with their friends and the world at large, express themselves as they see fit, and explore a wide variety of content attract passionate users and investors alike. Giving your users a forum to express their views, free from censorship and other limitations, can create a sense of place and community that enormously benefits your company as well as your users.

ENCOURAGE USERS TO SPEAK FREELY: PROMOTE DIVERSE SPEECH AND SPEAKERS

If your product or service allows users to interact with each other, it is in your best interest to encourage user expression. The more freedom your users have to express themselves freely, the more likely they are to interact deeply with your service, with lasting benefits to everyone involved.

> "The Internet is the most powerful and pervasive platform on the planet.... The Internet has redefined commerce, and... is the ultimate vehicle for free expression.
> —Tom Wheeler, FCC Chairman[89]

» DO YOU ENCOURAGE USERS TO EXPRESS THEMSELVES AS THEY CHOOSE?

Allowing users to express themselves with few limitations helps your product evolve into something that is truly valuable, even if it differs from your original vision. On the other hand, restricting your users' ability to communicate freely may drive them away from your product entirely. Give your users as many choices as possible in how they communicate with each other, and your product may turn into a surprising success story.

ALLOW SPEECH REGARDLESS OF TOPIC OR VIEWPOINT.

To build the widest possible user base, your service should let users discuss the topics they choose and express their own viewpoints. Encouraging debate rather than stifling dissent can produce a vibrant and compelling dialogue that engages existing users and attracts new ones. On the other hand, efforts to censor user speech can generate bad press and outrage users.

Apple Draws Fire for Going "Down the Dark Road of Censorship": *Apple has been accused of "going down a dark and scary road" for rejecting iOS apps that address any topic the company deems "objectionable." In recent years, Apple has rejected games and other apps focused on sweatshops, drone strikes, and the Syrian civil war solely because of the topic itself. In addition, commenters have noted that the policy has a chilling effect on developers and publishers, causing them to self-censor apps related to issues such as gay sexuality before even submitting the app for Apple's approval. As a result, Apple has been loudly criticized for "bar[ring] thoughtful and intelligent political expression" on its platform, leading some developers to abandon the platform entirely.*[90]

Facebook Called Out for Repeatedly Censoring Drug Policy Reform Discussion: *Facebook has repeatedly faced criticism for censoring discussions of marijuana legalization. In 2010 and again in 2012, Facebook blocked ads supporting marijuana legalization voter initiatives and drug policy reform measures. The issue re-emerged in 2015 when the company "permanently deleted" an account for discussing New York's newly-enacted medical marijuana law. The ongoing missteps have undermined Facebook's effort to position itself as a key platform for reaching "a huge potential voter pool" and led to criticism that its handling of the issue "amounts to censorship."* [91]

ALLOW USERS TO SPEAK ANONYMOUSLY OR PSEUDONYMOUSLY.

Many of your users may have important reasons for remaining anonymous or pseudonymous, whether they are domestic violence survivors, transgender people, or whistleblowers reporting an abuse of power. Other users may simply wish to access and share information without fear of harassment or embarrassment. Even if persistent identities are important for your service, allowing users to use pseudonyms can accomplish that while protecting users from harm and encouraging them to participate more deeply.

Facebook's "Real Name" Policy Generates Global Outrage: *Facebook suffered over a year's worth of bad press after advocates began highlighting the harmful effects of its "real name" policy. The policy, which required users to use a name on a government ID, sparked outrage by sending many users into a process resembling a state of "online purgatory," with their accounts disabled until the user submitted identification with a "legal name." The policy had an outsized effect on vulnerable people using non-legal names for privacy and safety reasons, with multiple news outlets highlighting its effect on transgender people, survivors of domestic abuse, and Native Americans. After both online and offline advocacy, including protests at the San Francisco Pride Parade and public pressure from advocacy groups, including the ACLU, Facebook finally committed to changing the policy.* [92]

Google Misses Opportunity to Add Pseudonyms to Google+: *In 2011, Google came under fire for requiring users of its new Google+ service to use their real names, rather than pseudonyms, as identifiers on the service. Critics expressed concern about the loss of online pseudonyms and the especially problematic consequences for people in vulnerable positions. Many users also complained about frequent and unpredictable account deactivation based on the real name policy. Google's initial response, "use your name or don't use the service," was viewed as a lost opportunity to distinguish itself from Facebook. However, continuing pressure ultimately convinced the company to backtrack and promise to allow pseudonyms.* [93]

AVOID ACTIVELY MONITORING USER COMMUNICATIONS.

If your service attempts to profile users by intercepting email, private messages, or other forms of communication, it may not only invade users' privacy but also discourage users from communicating freely on your platform. Encourage your users to freely express themselves by making it clear that you will not monitor their online communications.

» DO YOU GIVE USERS CONTROL OVER THE CONTENT THEY ACCESS AND THE THIRD-PARTY SOFTWARE THEY USE?

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

ALLOW USERS TO ACCESS THE CONTENT THEY CHOOSE.

Your users expect to be able to access the content they want. If they can't do so and don't understand why, they may express their outrage or simply take their business elsewhere. You can avoid this by making content available as a general rule.

Instagram Reverses #Curvy Hashtag Ban After User Uproar: *Instagram found itself at the center of a controversy in 2015 when it banned tons of photos and videos associated with the hashtag #curvy. Although the hashtag had been very popular for posts promoting body positivity and body acceptance, the service banned the term in a misguided attempt to prevent the spread of pornographic images on the site. After alienated and outraged users drew attention to the move with hashtags such as #curvee and #bringcurvyback, Instagram apologized, reversed the hashtag ban, and pledged to be more "thoughtful" in the way it approached user content.*[94]

Apple Comes Under Fire when Siri Refuses to Provide Abortion Content: *Apple came under fire from users and the press in 2011 when it was discovered that Siri, the company's recently-unveiled "intelligent personal assistant," would not provide information about abortion clinics or emergency contraceptives. Siri replied to some inquiries about abortion by saying it "couldn't find any abortion clinics" even if there were multiple hospitals or Planned Parenthood health centers nearby, and to others by directing users to anti-abortion centers. The story received significant attention after it was covered by the* New York Times*, forcing Apple to quickly fix the "glitch" and attempt to reassure users that the omissions were "not intentional."*[95]

ALLOW USERS TO CONTROL THEIR RELATIONSHIPS AND INTERACTIONS WITH OTHERS.

By allowing users to tailor your service to their needs, you help them create an experience that maximizes their enjoyment of your service. Offering tools that enable users to manage the people they interact with can help nurture positive connections and reduce the effects of harmful behavior. Instead of diverting resources on moderators or complicated algorithms, empower users to make their own decisions.

League of Legends Praised for Re-Engineering Chat to Reduce Harassment: *The developer behind the massively popular online multi-player game League of Legends reduced negative user interactions and received public praise after making simple changes to its chat system. Facing a problem of "toxic" and abusive behavior, developer Riot Games came to a simple solution: make the chat feature opt-in for users. According to Riot, a week after the change was made "negative chat saw a decrease by 32.7 percent [and] positive chat went up, by 34.5 percent." Riot was praised for effectively addressing its problems by "creating a simple hurdle to abusive behavior."* [96]

Twitter's Improved Blocking Tools a Welcome Improvement*: In 2014, Twitter was applauded for adding more "civility" to the site when it rolled out a host of tools to empower users themselves to combat harassment. In particular, Twitter improved its blocking feature, making it easier to use and more powerful, so that a blocked user could no longer view the blocker's profile. After previously coming under fire for its handling of online threats, observers called this a move "in the right direction."* [97]

ALLOW USERS TO USE THIRD-PARTY SOFTWARE.

Users consistently express outrage when ISPs, platforms, and similar services interfere with their ability to use third-party software that does not disrupt the functioning of the service. You can avoid controversy and demonstrate your support for your users by giving them the freedom to safely communicate using whatever application or tool they choose.

Facebook Hailed for Launch of Tor Portal: *Facebook was applauded for enhancing user security when it launched its own "Tor hidden service" providing privacy- and security-conscious users an alternative way to reach its service. Facebook connected users running Tor software to a version of the site with extra safeguards for protecting users' identities and their activity on site. Academics and the press embraced the new offering as a "first-of-its-kind" innovation and an "unalloyed good."* [98]

AT&T Accused of "Holding FaceTime Hostage": *AT&T triggered consumer and media outrage when it announced that it would only allow iPhone users to use the video chat app FaceTime on the carrier's cellular data network if the customers purchased a shared data plan. AT&T eventually changed its policy, but only after the company was subjected to a barrage of negative press and customer complaints, with the media accusing the company of "holding FaceTime hostage," "slapping consumers in [the] face over FaceTime," and carrying out "simple extortion."* [99]

» DO YOU GIVE USERS OWNERSHIP OF THEIR SPEECH?

If your product is a platform for user speech, users are likely to react poorly if they feel like they lack ownership of their own speech or lose control of what they say. Ensure that users are in control of their own expression and that you aren't putting words in their mouths without their consent.

GIVE USERS CONTROL OVER HOW THEIR CONTENT IS USED.

Respecting your users' contributions means respecting the legal rights they have in their content and their choices about how to engage with your service. Avoiding an aggressive stance on your ability to reuse users' content and letting your users decide what to say on your service and when to say it may win you more users in the long run.

Instagram's Policy Changes Trigger #instahate: *In late 2012, Instagram ignited a massive user backlash when it released a new privacy policy and terms of use that gave the company and its new owner, Facebook, broad access to user data and photos for commercial use. The policy, which would have allowed Instagram to sell the rights to photos posted to the service, triggered widespread outrage. Critics dubbed it the service's "suicide note" as users threatened to leave en masse. Even celebrity super user Kim Kardashian took to the social network airwaves to call out the company and question the fairness of the new policy. Instagram quickly backpedaled on the offending language, but not in time to avoid losing users to rival companies or to preserve customer goodwill.*[100]

93% OF AMERICANS WANT FULL RIGHTS TO SOME, IF NOT ALL, OF THEIR ONLINE INFORMATION (2014).[101]

CLEARLY DISTINGUISH YOUR OWN SPEECH.

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

LinkedIn Pays for Spamming Users' Contact Lists: *LinkedIn faced a class action lawsuit and the alienation of potential users for spamming contacts of its current users with invitations to join the service. Although LinkedIn did request permission to email these contacts, it failed to inform users that invitations would be sent repeatedly unless the recipient accepted or explicitly declined. LinkedIn ultimately paid $13 million in 2015 to settle a class action lawsuit over the unexpected emails.*[102]

MODERATE CAUTIOUSLY: MINIMIZE YOUR CONTROL OVER USER EXPRESSION

If your product provides a forum for content or communication, consider carefully whether you want to be in the business of policing those forums. If you need to place limits on illegal or other harmful behavior, make sure your policies are as clear and narrow as possible and ensure that there are mechanisms in place to handle disputes with minimal disruption to expression on your service.

» DO YOUR POLICIES SAFEGUARD FREE EXPRESSION?

There are real business costs to restricting user content or communications, both in terms of time and resources and in the impact on users' trust and loyalty. Clear, narrowly-drafted policies that prohibit only illegal speech or harmful behavior can help protect your users' freedom of expression while encouraging engagement with your service.

PROHIBIT ONLY ILLEGAL CONTENT OR SPECIFIC HARMFUL BEHAVIOR.

A sense of community can flourish when users are able to communicate freely. Narrowly tailoring your terms of service or community guidelines to prohibit only illegal content or specific harmful behavior that undermines the purpose of your service will help you limit the time you spend monitoring speech and the risk of being inconsistent or biased in the application of your policies.

PayPal Flops as Moral Police: *In February 2012, PayPal drew criticism from the press and civil liberties groups when it threatened to kick book publishers off its platform unless they removed "offending literature" from their catalogs. Although the company claimed that its policy was merely a shield against legal action, its actions were seen as affecting a broad range of content, some of which was clearly legal. Faced with a barrage of criticism, PayPal narrowed its policy to focus more narrowly on illegal and liability-inducing material.*[103]

CLEARLY SPELL OUT YOUR COMMUNITY'S POLICIES.

Vague prohibitions of "offensive" or "inappropriate" speech leave users uncertain as to what they can and cannot say, which can both chill acceptable speech and drive users to forums with clearer and more speech-friendly policies. On the other hand, clear policies encourage users to contribute rich content and engage with others. As your service changes, reevaluate and improve these policies to maximize speech.

Instagram Receives Worldwide Criticism After Banning Period Photo*: Instagram found itself at the center of an international controversy after it removed a photo posted by the Sikh artist and poet Rupi Kaur. Even though the photo was of a fully dressed woman alone in bed with a period stain on her clothing, Instagram deleted the photo twice for allegedly violating its prohibitions against sexual acts, violence, and nudity. After facing widespread criticism for its decision, Instagram apologized for "wrongly remov[ing]" the content as a violation of its Community Guidelines and reposted the photo.*[104]

MAKE THE PENALTY FIT THE VIOLATION.

If users are subject to extreme penalties for minor violations of your policies even if it's their first time, they may quickly lose interest in engaging with your service. Instead, ensure that consequences are proportionate to the rule violation and designed to keep speech and speakers on your service. Doing so helps you earn the respect and loyalty of all of your users.

» IS YOUR PROCESS FAIR TO USERS ACCUSED OF VIOLATING YOUR POLICIES?

Enforcing your community's policies based on fair processes helps even those accused of breaking them feel heard. Design your process to solicit and address valid concerns and make sure users understand what is happening and how they can respond to or appeal any decisions.

BUILD A REPORTING SYSTEM THAT SAFEGUARDS FREE EXPRESSION.

Allowing users to report policy violations can help you enforce those policies but can also lead to complaints aimed at silencing innocent users. To ensure you receive accurate information and to help you focus your resources on solving meaningful user concerns, encourage users posting complaints to provide details about their concern.

Facebook's "Fake Name" Reporting Option Enrages Users: *Facebook was heavily criticized for maintaining a "fake name" reporting option even as it took steps to move away from its "real name policy." The system was abused to target legitimate users, particularly members of the LGBT community. Targeted users and their communities were "furious" at being trapped in Facebook "purgatory" by a system that enabled rather than prevented abuse.*[105]

INFORM USERS ABOUT POTENTIAL VIOLATIONS OF YOUR POLICIES.

You can help your users better understand your policies and get timely feedback to help you avoid embarrassing mistakes by notifying them when you believe they might have violated your policies. Explain which policies are implicated and any actions you have taken or may take. Communication and transparency helps users better understand your policies and explain their own actions.

Reddit's "Shadowbanning" Criticized for Leaving Users in the Dark*: After being targeted by criticism from its own users, Reddit was forced to backtrack from its practice of "shadowbanning" users who violated its rules. Users who were shadowbanned received no notice and continued to experience reddit in the same manner as before, but none of their actions were visible to other reddit users, resulting in an effective ban from the site. The practice was widely criticized for alienating users, leading reddit to pledge to replace the "confusing" system with a more transparent approach.* [106]

KEEP CONTENT AND USER ACCOUNTS ACTIVE.

Not every user complaint or automated flag you encounter will actually be a violation of your policies. The best way to avoid angry users and the need to publicly apologize for improperly imposing penalties is to wait until you determine whether one of your rules was actually violated before taking any action.

***Facebook Criticized for Censoring ACLU Blog Post About Censorship**: Facebook found itself in the middle of another controversy around online speech when it deleted a blog post that, ironically enough, was about free speech and censorship. The post, which discussed a "kerfluffle" about a partially-nude statue in a public park in Kansas, included a picture of the statue. When the photo was incorrectly identified as a nude picture in violation of Facebook's Community Standards, the service not only removed the blog post but also "unpublished" the ACLU's entire Facebook page. The company ultimately backtracked, claiming that both takedowns were mistakes, but not before the media picked up on the controversy and highlighted Facebook's "history of problems with boobs" and other incidents where it incorrectly or arbitrarily enforced its policies.*[107]

GIVE USERS THE RIGHT TO BE HEARD.

Give your users a chance to be heard by allowing them to make their case, ideally before you make any decision to remove their content or otherwise affect their standing on your service. You might do this by creating a user-to-user informal dispute resolution channel. At a minimum, ensure that any dispute resolution process grants users the right to appeal decisions. With a robust dispute resolution and appeals process, you can help obtain the information to quickly resolve disputes and reduce the risk of incorrect and unfair decisions, all while demonstrating respect of your users' views and experience.

***Medium Tries to Craft "Human and Practical" Policies for Its Platform:** In mid-2015, the blogging site Medium introduced a straightforward set of content policies for posts and comments. The policies are designed to accommodate controversial speech, well-organized, and written in plain English. Notably, Medium states that users who encounter content that may violate a rule will speak with "a real human being" at the company in order to resolve any disputes, a move designed to facilitate fair outcomes and prevent inappropriate removal of speech from the site. Press praised Medium's changes as "setting the tone for the community it wants to foster on its site."* [108]

"We believe that counter-speech, better speech, is one of the best ways to deal with hate speech. That's the balance we're trying to strike."
—Ross LaJeunesse, Google Global Head of Free Expression & International Relations[109]

» DO YOU APPLY YOUR POLICIES CONSISTENTLY AND FAIRLY?

Even the most speech-friendly policies will do little good if they are not consistently and fairly applied. Make sure that everyone responsible for enforcing your policies is on board with your efforts to protect and promote speech by avoiding arbitrary or inequitable enforcement.

ENSURE THAT YOU CONSISTENTLY APPLY YOUR POLICIES.

Having a clear and consistent interpretation of your own policies and ensuring that your reviewers understand and follow them may help your users properly stay within boundaries of acceptable behavior. It can also avoid controversies where similar content is treated differently by different reviewers.

Facebook Faces "Nurse-In" over Breastfeeding Photo Policies: *In February 2012, Facebook offices were the site of "nurse-ins" protesting the social giant's practice of repeatedly taking down photographs of breastfeeding mothers. Although Facebook stated that its current practice was to allow such photos, in practice breastfeeding photos have been removed frequently for containing "nudity," and some mothers' Facebook accounts have even been deactivated. As a result, critics chastised Facebook for not even "playing by their own rules" and told the social network to "stop being total boobs." In response to continued negative press, Facebook explicitly changed its community guidelines in 2014 to allow photos of breastfeeding mothers.* [110]

ENSURE THAT YOUR POLICIES APPLY EQUALLY TO ALL USERS.

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

Coca-Cola Slammed for "Homophobic" Promotion: *Coca-Cola was "slammed by the LGBT community" after users discovered that the company's "Share a Coke" social media campaign banned the words "gay" and "homo." Attempts to create an image of a Coke can with the prohibited words resulted in an "Oops, let's pretend you didn't just try that" message, while words like "straight" and "hetero" were permitted. The company was forced to apologize in the face of "massive pushback," including the loss of "Brand of the Year" honors at multiple diversity events.* [111]

Twitter Triggers "Firestorm of Indignation" After Banning Olympic Journalist: *In 2012, Twitter faced allegations of preferential treatment of NBC, which had partnered with Twitter to promote the Olympics, after it encouraged NBC to complain about journalist Guy Adams' tweets and then immediately suspended his account after NBC complained. Although Twitter quickly apologized and reinstated Adams' account, it still "found itself in a deeply unfamiliar situation: as the subject of one of the firestorms of indignation that characterizes the platform, but which are usually directed at others."* [112]

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

Even if your business model involves selling or otherwise monetizing content, consider the costs and consequences of aggressively asserting your rights to control the use or distribution of that content, whether through legal or technological means. The law gives you tools to enforce rights to your content, but with this power comes the responsibility to use it wisely. Encouraging your customers to use your content or service in new and innovative ways may attract more paying users, while limiting their ability to enjoy your service could drive them to less restrictive competitors.

» DO YOU PROMOTE OPENNESS AND INTEROPERABILITY?

Although it might be tempting to lock down your product or vigorously guard your intellectual property, poorly deployed solutions can hinder your users' ability to use and share your content in beneficial ways and burden you with the obligation of maintaining software and processes for years. You can maximize user engagement and reduce your own burden by encouraging creative uses of your product and using technical or legal limits only where truly necessary.

ENCOURAGE USERS TO CREATIVELY USE YOUR PRODUCTS AND CONTENT.

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

Twitter Use Explodes After Embrace of User-Invented Hashtags: *Twitter started out as a service that would only produce plain text. When Twitter users began using hashtags on the service, Twitter initially resisted calls from users to officially support them. As hashtags continued to become popular, Twitter reversed course and embraced them, leading to an explosion of their use on the service. Today, hashtags—and thus Twitter—are "everywhere" and "impossible to ignore in our society."* [113]

EVALUATE THE IMPACT OF TECHNICAL LIMITS ON YOUR USERS.

Users may be dissuaded from using your product or service if their freedom is constrained by digital rights management (DRM) or other technical limits, especially if there is not enough "breathing space" to allow your customers to customize their own experience. In addition, user trust in your product may erode as customers realize that DRM is interfering with their expectations.

Keurig Faces "Tsunami" of Negative Press for Locking Out Third-Party Pods: *Amid a "negative public relations tsunami," Keurig was forced to roll back a redesign of its coffee maker that prevented competitors' coffee pods from being used with the product. Online reviewers "rebell[ed]" against the change, and customers "voted with their dollars" against it. Keurig sales fell dramatically, leading the company to acknowledge its mistake and reverse its design decision.*[114]

Apple Applauded for Removing DRM from iTunes Music: *Apple was showered with praise from users and the press after it it announced in 2009 that it would no longer impose digital rights management (DRM) on new music bought through its iTunes store. CEO Steve Jobs called the decision to allow the unrestricted copying of music files the "best alternative for consumers." Apple was applauded for its efforts to "help shape the online future of the music business" by ditching a standard that had "never been popular with the public."* [115]

CONSIDER THE FULL COSTS OF TECHNICAL LIMITS.

While the upfront costs of imposing technical limits on your products are fairly obvious and include both financial outlay and development time, the long-term costs can be more difficult to measure. In some situations, you may be forced to choose between maintaining or replacing an outdated system or facing outrage and even lawsuits from users who purchased devices or content that is suddenly unusable.

Google Forced to Repay Purchasers of Unusable Content: *In 2007 Google became the target of public outcry when it tried to close down its video service that incorporated DRM technology. Because users would have been unable to continue to use their previously purchased content once Google terminated the service, Google was forced to fully refund all payments for the service as well as keep the service active for an additional six months.*[116]

ENSURE THAT ANY CONTROLS YOU USE CONFORM TO USER EXPECTATIONS.

Controls that directly interfere with your users' expectations can drive those users away. If you do decide to impose technological limits, make sure you recognize how those limits will affect your users and avoid options that directly interfere with user experience.

Microsoft Faces "Global Outcry" Over Xbox One DRM*: Microsoft was blasted as "gross, despicable, greedy, pathetic, cowardly and out of touch" after it announced a controversial policy that restricted sharing of games and required the console to connect to the Internet every 24 hours for games to work. "Things were looking bad" for Microsoft until the company fully reversed its DRM policies in response to "global outcry" and sluggish sales.*[117]

Amazon Forced to Own Up to "Orwellian" Mistake: *In 2009, Kindle users were furious when they discovered e-Books, including George Orwell's 1984, were removed from their Kindles without notice. Amazon eventually explained that the deleted copies were improperly published in violation of copyright law and Amazon's own licensing agreements, but users were still outraged that Amazon "corrected" the issue in a way that "felt a bit like theft." The massive outcry over the "Orwellian" approach to addressing the problem forced Amazon to change its policy and promise that it would not recall even unauthorized copies in the future.* [118]

» DO YOU ASSERT LEGAL CONTROL ONLY AS A LAST RESORT?

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

USE INFORMAL CHANNELS TO OPEN DISCUSSIONS.

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

CAREFULLY EVALUATE THE LEGAL BASIS FOR YOUR DEMANDS.

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

Katy Perry Ridiculed After Threatening Lawsuit over "Left Shark" Replica: *Katy Perry found herself the subject of press ridicule after her lawyers sent a cease-and-desist letter to a 3D printing service for selling a replica of the Left Shark made popular by its awkward dancing in Perry's Super Bowl XLIX halftime show. The singer (and her lawyers) was slammed for trying to control the spread of a costume that was not protected by copyright. Press accused Perry's team of "desperately" trying to assert control in what amounted to a "show of hubris."* [119]

Apple "Bites the Fans that Feed It" by Waging Attack on Bloggers: *Apple was chastised by Forbes for "biting the fans that feed it" after trying to clamp down on blog posts about rumored upcoming products. A California appeals court shot down Apple's attempt to use legal methods to try to stifle conversation about its next-generation devices, vindicating the rights of online journalists to protect their sources while criticizing Apple for its aggressive use of the civil discovery process.*[120]

CONSIDER THE POTENTIAL CONSEQUENCES OF LEGAL DEMANDS.

In many cases, although you might wish to limit the use or distribution of your intellectual property or other content connected to your company, using legal mechanisms such as copyright takedown demands to attempt to assert control may simply not be effective. Assess the likelihood that your demands will be perceived as attempts to suppress speech, further fanning the flames of interest in the information and resulting in significant damage to your brand as well.

Sony's Internal Emails Widely Disseminated After Tantrum over Leak: *Sony Pictures Entertainment experienced the full force of the "Streisand effect" when its efforts to prevent the publication of emails leaked in a 2014 hack had the result of heightening the public's interest in them. The company's over-the-top reaction, including demands that Twitter and several news organizations delete any information they might obtain, only served to draw more attention to the leaked emails. The effort failed horribly, ultimately leading to a WikiLeaks project that archived the trove of emails and made them searchable for posterity as well as even more negative press for Sony.*[121]

MAKE SURE YOUR DEMANDS ARE COMPLETE AND EASY TO UNDERSTAND.

If you do issue any legal demands, ensure they not only meet any applicable legal requirements but also follow any instructions provided by the host of such content. Provide accurate and up-to-date contact info so recipients can easily contact the person in your company familiar with the demand to resolve or contest it. Facilitating communication about your demand can help repair mistakes and relationships without costly litigation.

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

To gain the respect of users as a champion for their free speech, you need to do more than just allow users to express themselves on your platform or service—you need to affirmatively protect them from third-party attempts to force you to remove their content or reveal their identities. Earning a reputation as a defender of your users' rights can be a valuable way to build trust with your current users and attract new ones.

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

If your company hosts user-generated material, you may find yourself on the receiving end of demands to remove material or even terminate a user's account based on various legal claims. To protect your users and your reputation, develop a procedure to review the demand carefully and ensure that your users' free speech rights are respected. Make sure that process complies with relevant laws, particularly the Digital Millennium Copyright Act (DMCA).[122]

INVOLVE USERS WHEN YOU RECEIVE A DEMAND TO REMOVE THEIR CONTENT.

The simplest way to help your users and boost their loyalty is to notify them promptly and give them a chance to respond to any request or demand to remove their content. Include a copy of the demand and inform the user about her possible responses and your procedure for acting on such notices. Encourage content owners and users to communicate directly and resolve their disputes amicably.

Etsy, YouTube, and Vimeo Commended for Encouraging Informal Resolutions: *Rather than simply providing trademark holders with instructions on how to send formal takedown requests for user-generated content on their sites, Etsy, YouTube, and Vimeo each encourage rights holders and their representatives to contact alleged infringers and attempt to informally resolve a dispute before pursuing legal action. The Electronic Frontier Foundation praised the companies for discouraging unnecessary legal disputes and "giv[ing] users a chance to understand and respond to threats against their own speech if necessary."* [123]

ONLY REMOVE CONTENT THAT YOU ARE REQUIRED TO REMOVE.

Grow your reputation as a defender of user rights by pushing back against illegitimate demands to take down content. If a demand seems overbroad or if you believe that your users have the legal right to say or post what they have done, evaluate your options for pushing back against the demand. And if you do comply with a demand, don't overreact by removing content beyond its scope.

Google Applauded for Championing First Amendment: *Google was praised for "defending freedom" when it refused to comply with an order to remove the controversial "Innocence of Muslims" video from its services. Google ultimately won a decision allowing it to keep the video online, leading "[e]veryone from technology companies to Hollywood to free speech advocates [to] breathe a sigh of relief."* [124]

TAKE YOUR USERS' RIGHTS INTO PROPER ACCOUNT.

Many takedown requests target commentary, criticism, and reporting related to a copyrighted work rather than the use of the copyrighted work itself. Some, but not all, of these uses may fall under the doctrine of fair use, which is a safety valve built into copyright law to help protect freedom of expression. You can win praise and the admiration of your users by finding ways to vindicate your users' rights.

Google Cheered for Supporting YouTube Users in Fair Use Fights: *Google received widespread praise for announcing it would bankroll some users in their legal fights against illegitimate copyright takedown notices of their YouTube videos. Google launched the groundbreaking program in late 2015, stating it would indemnify certain users it had identified as strong examples of fair use for up to $1 million in legal costs. Google was immediately praised by a wide variety of groups, including users, civil rights groups, and the news media, who heralded the move as "a game-changer" and called on other tech companies to follow Google's lead.*[125]

WordPress Wins Support for Facing off Against Copyright Abusers: *WordPress won support when it sued on behalf of a student investigative journalist targeted by an illegitimate censorship demand under the Digital Millennium Copyright Act (DMCA). After the student published an investigative article criticizing the advocacy group known as Straight Pride UK, the group responded by demanding that the post be taken down. WordPress filed suit against the group and won damages for the student for misrepresentation of copyright infringement. Press lauded the move of support as a "welcome" one that would encourage others "to fight back against malicious takedown notices."* [126]

» DO YOU PROTECT YOUR USERS' IDENTITIES?

Your users may have various reasons for keeping their identity private. At times, third parties may try to use legal process such as subpoenas to compel you to disclose their identities. Joining your users in resisting efforts to unmask their identities can earn you the lasting respect of your users, while failing to protect their identities can erode that trust and lead to additional consequences.

GIVE USERS AN OPPORTUNITY TO PROTECT THEIR ANONYMITY.

Build your reputation for respecting anonymity by making sure your users have a chance to defend theirs. If you receive a demand to unmask an anonymous user, immediately notify her and let her know how she might challenge the demand. Give the user as much time as possible to do so before turning over her identifying information.

Twitter Publicly Praised After Standing Up for Political Critics: *In 2010 Twitter was applauded for standing up for two anonymous users who were frequent critics of Pennsylvania Attorney General and gubernatorial candidate Tom Corbett. When Twitter received a subpoena from Pennsylvania prosecutors seeking the identities of the users, it notified the users and gave them a chance to object rather than immediately complying with the demand. The demand was withdrawn after the incident received substantial press coverage and the ACLU intervened. Twitter emerged as one of the heroes of the story for giving its users an opportunity to defend their anonymity.*[127]

DISCLOSE USER INFORMATION ONLY WHERE REQUIRED BY LAW.

Demonstrate that your service is a privacy-protective one and reduce your compliance costs at the same time by resisting illegitimate demands for user information. Thoroughly review any demands for information, identify any that seem overbroad or otherwise questionable, and evaluate your options for pushing back. If you determine you must comply, provide only the information that you are required to disclose.

Avvo Gets Rave Reviews for Protecting Anonymous Speech: *Online lawyer-rating website Avvo was credited with a "landmark" win protecting "your right to anonymity" after it fought a demand to turn over information about a user who had posted a negative review. When Avvo received the demand, it contacted the reviewer, who provided information proving to Avvo's satisfaction that the reviewer had been one of the lawyer's clients. Avvo then challenged the demand in court, ultimately earning recognition for winning "a victory for anonymous commenters."* [128]

Yelp Cheered for Winning Fight to Protect Identities of Reviewers: *Yelp was cheered after it won a public battle to defend the identities of seven users who had been targeted for their reviews. The company went to court to challenge a subpoena from a Virginia-based carpet cleaning company demanding the identities of reviewers who posted negative reviews. Yelp fought the issue for nearly two years before winning in the Virginia Supreme Court, a moment hailed as "a victory for Yelp and its anonymous commenters."* [129]

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

If the law doesn't adequately protect your users' freedom of expression, you can earn their gratitude by working to change the law. Courthouses and legislatures both offer opportunities for you to affect policy and establish yourself as a champion of freedom of expression. Working in coalition with other companies, non-profit advocacy groups, and local law school clinics can provide more bang for the buck if you lack the resources to go it alone.

FIGHT FOR YOUR USERS IN COURT.

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

Google Widely Praised for Opposing Attorney General's Assault on Speech: *Google received accolades from privacy advocates and the press when it fought the Mississippi Attorney General's (AG) 79-page subpoena demanding information allegedly related to illegal materials available through Google's services. Google, along with several non-profit organizations, argued that the AG's subpoena was overbroad and intended to chill speech rather than to further a legitimate investigation. In doing so, Google not only pushed back against an interpretation of the law that would "inevitably" lead to "extraordinary legal costs" for hosting interactive content, it also received widespread attention and praise for standing up for its users' rights.*[130]

Facebook Users Like Company's Defense of Free Speech: *Facebook was praised for defending free speech when it went out of its way to defend the First Amendment rights of its users to use its "Like" feature. When a Facebook user was fired by the Hampton, VA, sheriff's office for "liking" the Facebook page of the current sheriff's election opponent, Facebook joined advocacy groups including the ACLU in arguing that "liking" someone was speech protected by the U.S. Constitution. Facebook's advocacy was widely noted in coverage of the case, earning the company and its stance a "thumbs up" from the media.*[131]

PUSH FOR LAWS AND POLICIES THAT PROTECT FREE SPEECH.

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

Websites Thanked by the President for Supporting Net Neutrality: *Major Internet companies were showered with praise by press and even the U.S. president after coming out in support of net neutrality in 2014 and 2015. Companies advocated for net neutrality in various ways: Mozilla, reddit, Netflix and others altered the home page of their websites to highlight the issue while others, including Google, Twitter, Amazon, and Lyft, released statements in support. After the effort paid off when the FCC voted to approve strong net neutrality rules, the companies even won praise from President Barack Obama, who sent a public handwritten note to Reddit users thanking them for their support.*[132]

OPPOSE LAWS AND POLICIES THAT UNDERMINE FREEDOM OF EXPRESSION.

Your company can also make an impact by opposing laws and policies that would stifle free speech. Taking a stand to fight such laws and policies can protect both your business model and your users' right to freedom of speech.

Twitter Commended for "Doing the Right Thing" by Suing for Surveillance Transparency: *Twitter was commended for challenging government rules preventing it from disclosing basic information about national security requests for user information. When Twitter sued for the ability to reveal how many and what type of national security-related demands it received from the federal government, it was heralded for "doing the right thing" for its users and transparency.*[133]

Companies Praised for "Blackout" to Oppose Laws Undermining Online Speech: *Google, Reddit, Wikimedia, and other online services were widely recognized for standing up for freedom of expression by serving as ringleaders for an online "blackout" in opposition to two highly controversial 2012 Congressional bills, the Stop Online Privacy Act and the Protect Intellectual Property Act. The bills, nominally designed to combat copyright infringement, were described by critics as "damaging free speech, Internet security, and online innovation." After the blackout helped shelve both bills, the press praised the companies for leading the fight and standing up for freedom of expression.*[134]

CONCLUSION

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

We hope the practical tips and case studies in this primer have helped you begin the process of building robust privacy and free speech protections into your services and business so you can properly protect the rights of your users as well as your company's bottom line.

For many additional case studies and resources to help you continue that process, please see the online version of this primer at **itsgoodfor.biz**.


ACLU
AMERICAN CIVIL LIBERTIES UNION
of CALIFORNIA