Managing Users' Rights Responsibly – A Guide for Early-Stage Companies

Dalia Ritvo, BERKMAN CENTER FOR INTERNET AND SOCIETY
Vivek Krishnamurthy, BERKMAN CENTER FOR INTERNET AND SOCIETY
Sarah Altschuller, *Corporate Social Responsibility Practice*, FOLEY HOAG LLP

TABLE OF CONTENTS

Introduction

"The web is now a public resource on which people, businesses, communities and governments depend. It is vital to democracy and now more critical to free expression than any other medium. It stores and allows us to share our ideas, music, images and cultures. It is an incredibly intimate reflection of our interests, priorities, disagreements and values. That makes the web worth protecting."

-- Sir Tim Berners-Lee, Inventor of the World Wide Web

"In this technological era, people are increasingly reliant on digital media in their political, economic and social lives. It is fundamental that the human rights they hold offline should also be protected online."

-- Navi Pillay, U.N. High Commissioner for Human Rights

As online services play an increasingly important role in every aspect of our lives, companies are being forced to make difficult legal decisions about the free speech and privacy rights of their users. Consequently, both established and early-stage companies must understand the relevant laws about collecting, storing, processing, and disclosing information on behalf of their customers—both to maintain customer trust and avoid lawsuits and public relations debacles. This guide provides the tools and information your company needs to respect the privacy, security, free expression, and intellectual property rights of your users.

Why do these issues demand your attention?

Most of the things on your "to do" list need to be done *right now*, including raising capital, shepherding product development, and implementing marketing strategies. Developing policies and procedures to protect and respect the rights of your users may not be at the top of your list of concerns. Nevertheless, smart, early-stage investments in protecting user privacy and freedom of expression can pay dividends for many years to come. This investment will help inspire trust and confidence among both customers and investors. This will propel growth and protect your company against legal and reputational risks that can derail your plans.

Ultimately, developing strategies to protect user rights in a responsible way will help your company accomplish the following:

- Generate positive press that attracts users, customers, investors, and employees;
- Develop scalable internal processes that will serve your company as it grows; and
- Ensure that your company has the tools necessary to avoid making bad decisions -- that may result in legal liability, public embarrassment, or a loss of customers -- in response to difficult requests.

What are the risks of inaction?

User expectations as to how companies should manage and protect their content and personal data (including metadata) have never been higher -- especially following Edward Snowden's revelations on the scope and scale of U.S. government surveillance. For a small company, one misstep can put you out of business.

The risks are especially great as people around the world use technology platforms to communicate ideas, strategies, and demands for political change. Large companies may be able to weather the public relations storm resulting from a failure to protect users' interests when responding to a government request or a takedown

notice. Smaller companies, however, can lose their customer base as a result of one significant controversy. While Yahoo!'s reputation has now recovered from the lawsuits and adverse publicity that resulted from its Chinese subsidiary's compliance with Chinese law enforcement requests that eventually resulted in the arrest of pro-democracy activists, Google's Buzz social network never recovered from a furor over its privacy practices at the time of its launch and ended up being shuttered within two years.

Furthermore, investors and employees alike are paying attention to corporate policies on users' rights. Investors prefer to support companies that avoid litigation and negative publicity, while employees prefer to work for companies that care about the rights of their customers. There is no reason why your company shouldn't share in the accolades accorded to companies like Dropbox and Wordpress[1] for taking strong public stands to protect user rights. Investing time and resources in policy and process development in the short term will generate long-term value for your company.

How will this guide help?

This guide provides a succinct overview of the challenges your company may face when third parties seek to access or suppress information relating to your customers. It also outlines practical steps that you can take right now to address those challenges. Specifically, each of the chapters in this guide provides:

- An initial summary of the key challenges faced by companies, including requests for content-restriction, demands for user data, and evolving expectations and requirements with regard to user privacy;
- A description of the nature of the challenge, the relevant legal requirements, and the associated risks to your company,
- Guidance on steps that you can take in the short, medium, and long term to address the identified challenges; and
- Suggested resources for further information and guidance.

This first edition of our guide covers only the laws of the United States and focuses primarily on federal law. We hope to expand our coverage in subsequent editions of this guide to include the laws of key international and U.S. state jurisdictions. In the interim, and as discussed further in Chapter 1, be aware that your company is potentially subject to the laws of every jurisdiction in which it operates. Consequently, you should obtain competent local legal advice before you expand beyond your home market.

Last, but not least, who are we?

This guide represents a joint effort between Foley Hoag LLP and the Cyberlaw Clinic at Harvard University's Berkman Center for Internet & Society.

Foley Hoag LLP is a law firm with offices in Boston, Washington, D.C., New York, and Paris. With leading practices in corporate social responsibility, security and data privacy, and intellectual property, Foley Hoag's attorneys are well positioned to advise the leaders of emerging technology companies on the development of policies and procedures to mitigate legal, reputational, and operational risks. Foley Hoag is also an accredited independent assessor for the Global Network Initiative,[2] a multi-stakeholder organization that provides guidance to information and communications technology companies seeking to respect, protect, and advance user rights to freedom of expression and privacy.

[1] Both companies earned perfect five star ratings from the Electronic Frontier Foundation in 2015 for their efforts to protect user data from unlawful government intrusion. Electronic Frontier Foundation, Who Has Your Back, (2015), *available at* https://www.eff.org/who-has-your-back-government-data-requests-2015.

[2] To learn more about the Global Network Initiative, visit: https://globalnetworkinitiative.org/

The Berkman Center for Internet & Society is Harvard's university-wide center dedicated to the exploration, study, and development of cyberspace. The center draws upon a vast network of faculty, students, entrepreneurs, lawyers, and virtual architects to diagnose both the opportunities and the challenges of cyberspace, particularly with regard to the need for legal structures. This guide is a product of the Harvard Law School's Cyberlaw Clinic, which is based at the Berkman Center. The Cyberlaw Clinic engages Harvard Law students in a wide range of real-world litigation, licensing, client counseling, advocacy, and legislative projects and cases, covering a broad spectrum of Internet, new technology, and intellectual property legal issues. Clients include individuals, small startups, nonprofit organizations, internal Berkman Center projects, groups of law professors, and government entities.

Special thanks to Benjamin Guthrie and Rebecca Gerome at Foley Hoag for their help in pulling this together, as well as the following Cyberlaw Clinic students: Derrick Davis, Chien-Fei Li, Esther Lim, Mark Quien, Kerry Maeve Sheehan, Ajay Sundar, and Martha Vega Gonzalez for all of their hard work on this project.

CHAPTER 1:
Jurisdiction: What Laws Apply?

A vital first step in responsibly managing the rights of your users is to understand what laws apply to your company and to the data that your users have entrusted you to manage. Such an understanding does not guarantee that your company will do right by your users, but it is critical to appreciating the risks to user rights that might be posed by offering specific products in different markets around the world.

Whose Laws?

One of the most difficult questions facing technology companies that wish to operate responsibly is the question of whose laws they must follow.

Jurisdiction is the term lawyers use to describe the power of a government and its courts to apply and enforce its laws against an individual or a company. The advent of the Internet has introduced considerable confusion into the law of jurisdiction.

In the old days, jurisdiction was based on whether an individual or a company was physically present within a particular territory. This hard and fast rule began to give way in the era of the travelling salesman, when courts decided that it was fair to exercise jurisdiction over businesses that conducted more than an occasional transaction in a given place.

Courts in the United States and around the world have been struggling to adapt these rules to the borderless Internet, where start-ups can acquire millions of users around the world in a matter of weeks, and vast quantities of data are stored with cloud providers that operate across national borders. Adding to the complications are the fact that judges are not always particularly tech-savvy, as reflected in jurisdictional decisions turning on such factors as whether a website contains interactive elements or banner ads localized to a browser's IP address.

The rules around when and how online business activities give rise to jurisdiction in a particular place are still very much in flux. Within the United States, however, three basic principles govern when different state governments may be able to assert their jurisdiction against your company:

- First, governments and courts will possess jurisdiction over your company in any U.S. state where you have a permanent physical presence, such as offices, employees, or servers.
- Second, governments and courts will also possess jurisdiction over your company in whatever state in which you are incorporated as a business.
- Third, there is a point beyond which your activities in any given state will become substantial enough that the state government and its courts will be able to exercise jurisdiction over you in relation to those activities — regardless of whether you have a physical presence in the state. Where this point lies is difficult to delineate in the abstract, as courts weigh a variety of factors in making this determination, but legal counsel can advise you on this.

As for the law of jurisdiction beyond the United States, each country has its own rules. Some countries' courts may only exercise jurisdiction over companies with a physical presence within the country's borders, while others may do so when a company transacts a large volume of business with the country's residents from afar. Since foreign laws governing access to user data or the removal of user-generated content can be very different from U.S. laws, your company should think very carefully before it establishes a physical presence in any other country

— including placing data on servers located in another country for backup or performance reasons. Consulting with a local lawyer who is knowledgeable regarding such issues is a vital first step for any business to take when establishing a physical presence in another country, as an on-the-ground presence makes it immeasurably easier for foreign governments and courts to enforce their laws against your company.

What Data?

Once your company has identified whose laws it must follow, you must then determine what laws regulate your business within each of those jurisdictions. In the context of protecting user rights, the critical question to ask is what kinds of data your company is collecting and storing either from or on behalf of your users. This is important for at least two reasons.

First, the risks to the rights of your customers vary significantly depending on the kind of data your company maintains on its servers. Data concerning the intimate details of a customer's personal life is obviously more sensitive than a customer's reviews of the products and services your company offers, for example.

Second, and equally importantly, different kinds of data are subject to varying degrees of regulatory protection in the United States and foreign jurisdictions. Health, financial, and educational data are all protected by federal laws in the United States, while personally identifying information such as an individual's date of birth is subject to heightened protections in most U.S. states and many foreign jurisdictions as well.

Thinking carefully about the kinds of data your company collects — and whether it needs to collect such data in the first place — arms your company with the information you need to manage the specific user rights challenges that are discussed in the next three chapters of this guide.

CHAPTER 2:
Content Takedown Requests

There are many reasons why a company that provides online services might receive a request to remove content hosted on its websites or services. Individuals, corporations, and even government agencies may ask companies to remove content based on a claim that the content:

- Is illegal, such as child pornography (everywhere) or hate speech (in most non-U.S. democracies);
- Infringes on existing copyright or trademark rights;
- Violates someone's publicity, privacy or other related rights; or
- Is defamatory.

These requests are generally known as "takedown requests." Different laws apply to the varying types of takedown requests, and a few statutes offer "safe harbors" that insulate online service providers ("OSPs") from liability arising out of content uploaded by users if the OSP has followed certain procedures. This chapter introduces the different types of content takedown requests a company might receive, and the legal structures that drive these requests, including the instances in which the law provides safe harbor.

As of February 2016, Google reported that it had received requests to remove over 76 million individual web addresses in the previous month. These requests were submitted by 6,780 copyright owners and 3,263 reporting organizations.

Google reported that it had received 3,467 requests from governments to remove 34,299 items during the six-month period ending June 2015.

One challenge for OSPs is managing the volume of takedown requests. Individuals, organizations and governments seeking to suppress speech and civil liberties take advantage of the fact that many OSPs don't carefully scrutinize the takedown requests they receive by submitting requests that don't comply with the law. OSPs run the risk of public relations fiascos, and more importantly, of losing the trust of their customers, in responding to such requests. For example, Google came under fire in 2009 when it removed an MSNBC news report critical of an anti-gay-rights group's ad from YouTube after the group claimed that its copyright had been violated. Similarly, in 2013, the Electronic Frontier Foundation inducted the artist known again as Prince into its "Takedown Hall of Shame" for his use of copyright takedown procedures against content that did not infringe upon his copyrights.

To avoid unwarranted suppression of user content, your company should establish policies and procedures to guide your response when a takedown request ultimately arrives, and you should provide all relevant personnel with appropriate training in these procedures. Having clear policies in place communicates to your users that you are serious about respecting everyone's rights while helping your company avoid the negative consequences of an *ad hoc* response to an illegitimate request. This chapter provides an overview of the laws that cover takedown requests and the types of policies and procedures that will help you respond appropriately.

Copyright Takedown Requests

The Law

Copyright bestows authors with exclusive property-like interests in their expressive works. Much of the content posted on the Internet, including computer programs, pictures, photographs, sounds, videos, and so forth, is protected by copyright. The protections that copyright affords authors are not absolute, however. For example, facts, ideas, and concepts cannot themselves be copyrighted, although the particular words used to express them are protected by copyright. Similarly, the "fair use" doctrine allows reasonable portions of a copyrighted work to be reproduced for purposes such as criticism, comment, news reporting, teaching, scholarship, and research.

The Digital Millennium Copyright Act of 1998 (the "DMCA"), provides OSPs, such as search engines, websites, cloud computing service providers, and other similar type of providers, with safe harbor protections against copyright infringement claims arising out of content uploaded, transmitted or posted on their services by third parties or individuals, so long as the OSP:

1. Does not know that the content is infringing, or is unaware of any facts that would indicate the content is infringing; and
2. Removes the content "expeditiously" upon receiving a takedown notice from a rights holder.

In 2008, the activist group The Yes Men set up a website parodying the U.S. Chamber of Commerce and staged a press conference posing as the Chamber of Commerce where they announced that the Chamber of Commerce would stop its aggressive lobbying against climate change legislation. The Chamber of Commerce sent a takedown notice to Hurricane Electric, the parody site's upstream service provider, alleging that the site's use of the Chamber of Commerce's images, logos, and website design violated the Chamber's intellectual property rights. Hurricane Electric responded by taking down The Yes Men's site as well as many others hosted by May First/People Link ("May First"), the site's direct service provider. May First immediately mirrored the parody site on a different network to preserve access to The Yes Men's political message. Had May First responded by taking down the parody site entirely, it would have silenced speech that is protected by the First Amendment and contributed to the abuse of trademark law. Following the takedown notice, the Chamber of Commerce filed suit against the Yes Men in federal court alleging trademark infringement. After The Yes Men, represented by the Electronic Frontier Foundation and Davis Wright Tremaine, LLP, moved to dismiss the lawsuit on First Amendment grounds, the Chamber of Commerce withdrew its lawsuit.

This statute is intended to insulate OSPs from copyright liability stemming from content that is posted or uploaded by an OSP's customers or users.

The "safe harbor" protections are so called because they are not automatic. To take advantage of these protections, a company must "enter" the safe harbor by taking the following steps:

1. Designate a copyright agent to receive DMCA takedown notices, and register the agent with the U.S. Copyright Office.
2. Adopt policies regarding copyright infringement and repeat infringers, and communicate those policies to the public. These policies must not interfere with anti-circumvention measures, such as Digital Rights Management (DRM) software, put in place by rights holders to protect their copyrighted works.
3. Comply with legitimate notice-and-takedown measures by quickly removing or blocking access to alleged infringing materials.

Once you have met these requirements, you can implement your "notice and takedown" process pursuant to the DMCA. In order for a takedown notice to be valid under the DMCA, the takedown notice must be delivered in writing and **must** include the following elements:

1. A physical or electronic signature of a person authorized to act on behalf of the copyright holder;
2. Identification of the copyrighted work the individual claims is being infringed;
3. Information that is reasonably sufficient to allow the OSP to contact the complaining party, such as an address, phone number or email address;
4. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
5. A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Your company may reject any DMCA takedown notice that does not contain all of these elements.

In considering how best to review and respond to DMCA takedown notices, your company should consider the potential for the process to be abused in order to stifle political and social commentary. One specific challenge to be aware of is the potential for public authorities to utilize the DMCA process, potentially through third-party proxies. Developing internal guidelines to ensure that potentially abusive requests receive appropriate internal review can help mitigate the potential that your company will contribute to the stifling of legitimate expression.

Action Items

- ❑ Register a copyright agent with the U.S. Copyright Office. Instructions on how to do this can be found at: http://www.copyright.gov/onlinesp/
- ❑ Draft and publish a policy statement describing how you plan to address DMCA takedown requests that includes a process on how your company will identify and treat repeat infringers. In creating the policy, consider how takedown requests will be assessed to avoid taking down content that is non-infringing under fair use, and what process you might use to allow your users to counter a notice.
- ❑ Create internal guidelines and an escalation process to ensure that takedown requests that may not be accurate or that may misidentify infringing material receive an extra level of review by senior company personnel or external advisors, such as your legal counsel, a local law school clinic, or staff attorneys with organizations such as the Cyberlaw Clinic at the Berkman Center, the Electronic Frontier Foundation and the ACLU.
- ❑ Provide training to personnel who will be responsible for takedown notices on elements that need to be included in a takedown notice, and reject all notices that don't meet statutory requirements.
- ❑ Create a system to track your company's handling of takedown requests that includes the ability to flag individuals who repeatedly post infringing material.

Resources

Statutes

- Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512 ("Limitations on liability relating to material online")

Other References

- Digital Media Law Project, Protecting Yourself Against Copyright Claims Based on User Content, *available at* http://www.dmlp.org/legal-guide/protecting-yourself-against-copyright-claims-based-user-content
- Electronic Frontier Foundation, DMCA, *available at* https://www.eff.org/issues/dmca

Trademark Takedown Requests

The Law

The purpose of trademark law is to protect consumers against confusion in the marketplace. Trademark law accomplishes this by granting robust rights to trademark owners to prevent others from using an owner's mark or a mark that is "confusingly similar" in order to ensure that consumers can identify the source of a product or service.

A trademark is a word, name, symbol, phrase, design or other device used to identify and distinguish the source of particular goods and services. Trademarks can be text- or design-based and can include logos, slogans, particular sounds, domain names, colors, or the look and feel of a website.

Trademarks may appear in user-generated content in a variety of forms including: artistic expressions; commentary and reporting; domain names; advertisements; hashtags; search keywords; and website metadata. Many uses of trademarks in user-generated content are legal so long as they don't cause confusion in the marketplace. For example, the use of trademarks in product reviews, comparison advertising, news reporting, and in non-commercial uses generally does not constitute trademark infringement.

Trademark law provides no explicit process by which OSPs can insulate themselves from liability, but recent case law indicates that OSPs that implement notice and takedown procedures similar to those required under the DMCA might avoid liability for third party content that is transmitted or uploaded to their services. Specifically, even if you exert some control and monitoring over user content or user access to the service, your company is unlikely to be held liable for infringement based on user-generated content if:

> *To prove infringement, a trademark owner must show that it owns a valid trademark and that the allegedly infringing user used the mark or a similar mark in connection with the sale, offering for sale, distribution, or advertising of goods and services in a way likely to, or that in fact did, cause confusion among consumers as to the source or sponsorship of the user's goods or services.* Rosetta Stone Ltd. v. Google, Inc., *676 F.3d 144, 152 (4th Cir. 2012). If the use of the mark is not likely to cause confusion, there is no trademark infringement.*

1. Your company is unaware of the specific instances of trademark infringement; and
2. Your company promptly removes content specifically identified as infringing a trademark.

If your company receives and ignores repeated valid takedown notices, you do risk liability. To that end, in order to avoid liability for contributory trademark infringement you should:

1. Adopt a policy on how to handle trademark infringement and repeat infringers, and communicate those policies to the public; and
2. Comply with legitimate notice-and-takedown measures by quickly removing or blocking access to potentially infringing materials for which you have received a valid takedown notice.

As part of your policy, you should specify what information trademark holders must include in a takedown notice in order for the notice to be valid. Pursuant to relevant case law, a valid takedown request must identify each instance of infringement on the OSP's service.

In addition, although it is not legally required under case law, it is best practice to require rights holders to include the following in their takedown notices:

1. Information that is reasonably sufficient to allow you to contact the complaining party, such as an address, phone number or email address;
2. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the trademark owner, its agent, or the law;
3. A statement identifying the source of the infringement (*e.g.*, the use is causing or likely to cause consumer confusion, or the use is causing dilution or tarnishment of the rights holder's trademark); and
4. A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Action Items

- ❑ Draft a customer-facing policy describing how you plan to address trademark takedown requests. This policy may include a clear notice and takedown process similar to those required under the DMCA, but at minimum, it should comply with relevant case law. The policy should also include information on how your company will respond to users who repeatedly post infringing content, as well as a counter-notice process for users to respond to takedown requests associated with their content.
- ❑ Create an internal escalation process to ensure that takedown requests that may not be accurate, or that may misidentify infringing material receive an extra level of review by senior company personnel or external legal advisors.
- ❑ Provide training to personnel who will be responsible for responding to trademark takedown notices regarding the elements that must be included in such a notice, to ensure that your company will reject all notices that don't meet these requirements.
- ❑ Create a flagging system to identify individuals who repeatedly post infringing content.
- ❑ Create and draft a disclaimer for your site that states you are not affiliated with the trademark owners represented on your site through your own content, or that of your users, and encourage your users to adopt similar disclaimers in their content and to provide links to the official site of the trademark owner when confusion is possible.

Resources

Statutes

- Section 45 of the Lanham Act, 15 U.S.C. § 1127

Case Law

- *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010)
- *Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.*, 658 F.3d 936 (9th Cir. 2011)

Other References

- Digital Media Law Project: Trademark, *available at* http://www.dmlp.org/legal-guide/trademark
- Electronic Frontier Foundation, Internet Law Treatise, "Trademark," *available at* https://ilt.eff.org/index.php/Trademark:_General

Takedown Requests for Defamation and Other Harmful Content

In order to protect free speech online, Congress passed the Communications Decency Act ("CDA") in 1996. Section 230 of the CDA grants broad immunity to OSPs for information and content posted on their sites that is generated by a third party.

Businesses operating online will most frequently encounter Section 230 when addressing takedown requests for content that is not illegal per se, but that is defamatory or in violation of an individual's rights to privacy and publicity. Section 230 does not provide immunity for all content appearing on an OSP's services. For example, no immunity may exist when an OSP has solicited or paid for the content. That said, Section 230 provides OSPs with strong protection against liability for statements made by third parties through their sites or services.

> *In 2004, Gordon Roy Parker, a self-described Internet publisher, sued Google for defamation, invasion of privacy, and negligence, among other claims, based on an excerpt of his publication posted on a USENET discussion board, and on search results provided by Google that lead to websites that hosted content criticizing Parker. The court rejected Parker's defamation, invasion of privacy and negligence claims based on Google's immunity under the CDA Section 230. Had Google responded by removing the negative statements about Parker, it would have silenced critical discussion about Parker and his writings, and impinged on the free speech rights of its users.* Parker v. Google, Inc., *242 F. App'x 833, 838 (3d Cir. 2007).*

OSPs naturally want to avoid having their services used to stalk, harass or damage the reputations of other businesses, organizations or individuals. In fact, most OSPs' terms of use explicitly prohibit this type of behavior. OSPs are rarely in a position, however, to determine whether statements made by their users or customers are defamatory or otherwise actionable in a civil lawsuit. Further, there is a strong possibility that protected speech might be silenced through an OSP's response to such takedown requests, as people often file defamation or harassment claims to silence those with whom they disagree. The intent of Section 230 is to help companies avoid making arbitrary decisions that could ultimately silence speech protected under the First Amendment to the U.S. Constitution.

The protection offered by Section 230 is especially important as people continue to rely on online services to organize for social change and to communicate grievances related to government and public policy. To that end, you should think about how Section 230 will play into your takedown policies and practices, taking into account the free speech implications of taking down content based on potentially unfounded claims.

The Law

Subject to certain exceptions, Section 230 insulates OSPs from any liability stemming from content posted or uploaded by third parties through the OSP's services. Courts have held that this immunity exists even when OSPs exercise control over whether the offending material is published or removed, and when they edit the material (so long as the edits do not alter the meaning of the content). When an OSP plays an active role in specifically soliciting the harmful content, however, Section 230 may not apply.

Unlike the DMCA or trademark law, Section 230 does not require OSPs to remove content in response to takedown requests rooted in defamation or other similar claims. Further, instead of designating certain types of content as protected, Section 230 excludes obscene materials and child pornography from protection against liability, and explicitly states that it is not intended to have any effect on federal criminal law, federal and state communication privacy and intellectual property laws, and any other state law that is consistent with its provisions.

Accordingly, if your service hosts user generated content, you generally will not be obligated to take down any content, unless it violates criminal law or the takedown notice complies with the requirements under intellectual property law. To that end, in creating policies on how to handle user generated content, you should take into account the need to protect free speech and an exchange of ideas before arbitrarily removing content based on a grievance by an individual user.

Action Items

- ❑ Create and draft an external policy describing what rules apply to user-generated content that is not specifically prohibited by law. This policy should include how you plan to moderate content, if at all, and under what circumstances you may remove or block access to content based on the material or statements made within the content.
- ❑ Provide training to personnel who will be responsible for moderating content and responding to requests for content to be removed.
- ❑ Create an internal escalation process to ensure that content that is flagged as harmful or unlawful receives an extra level of review by senior company personnel to determine whether or not the content should be taken down. This process should match the policies disclosed to users and customers.

Resources

Statutes

- Section 230 of the Communications Decency Act, 47 U.S.C. § 230

Case Law

- *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003) (finding that Section 230 precluded liability for Internet dating site on claims of defamation, negligence, invasion of privacy, and misappropriation of the right of publicity)
- *Doe v. MySpace, Inc.*, 528 F.3d 413, 422 (5th Cir. 2008) (finding MySpace not liable for negligence and gross negligence based on a failure to prevent a 13 year old from lying about her age on the site, where she eventually met an adult who later sexually assaulted her)
- *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.,* 519 F.3d 666, 671 (7th Cir. 2008) (finding Craigslist not liable for violation of the Fair Housing Act based on user ads)
- *Noah v. AOL Time Warner, Inc.,* 261 F. Supp. 2d 532, 538 (E.D. Va. 2003) aff'd *Noah v. AOL-Time Warner, Inc.*, No. 03-1770, 2004 WL 602711 (4th Cir. Mar. 24, 2004) (finding AOL not liable for violation of Title II of the Civil Rights Act based on harassing comments by users)
- *F.T.C. v. Accusearch Inc.*, 570 F.3d 1187, 1199 (10th Cir. 2009) (upholding liability for an OSP that solicited requests for confidential information, paid researchers to obtain it, and made it publicly available)
- *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1165 (9th Cir. 2008) (finding a roommate matching website liable for violation of the Fair Housing Act when the site produced the discriminatory content by posting a questionnaire with a dropdown menu of unlawful answers)

Other References

- DMLP, Immunity for Online Publishers under the Communications Decency Act, *available at* http://www.dmlp.org/legal-guide/immunity-online-publishers-under-communications-decency-act
- Harvard Law Review, Badging: Section 230 Immunity in a Web 2.0 World, *available at* http://cdn.harvardlawreview.org/wp-content/uploads/pdfs/badging.pdf

Child Pornography Takedown Requests

While adult pornographic material is generally protected in the United States by the First Amendment, that protection does not extend to child pornography. Possession and distribution of child pornography is prohibited by law. For this reason, it is extremely important to properly respond to takedown notices regarding content containing child pornography.

The Law

The Child Protection and Sexual Predator Act of 1998 prohibits the knowing possession or transmission of any visual depiction of a person under 18 years of age engaging in sexually explicit conduct. The law defines sexually explicit conduct as any actual or simulated sex act, or the "lascivious" exhibition of the genitals or pubic area.

Defining whether specific material is lascivious or not may be difficult depending on the nature of the content. For instance, under the statute, it may be unclear whether a picture taken by a mother of her infant in the bathtub as qualifies child pornography. Similarly, it is unclear whether a black and white photograph of nude babies would constitute exploitation of children or art protected by the First Amendment.

Most courts apply a flexible multi-factor test to determine whether content is lascivious and will consider all or some of the following six factors in the context of the overall image and age of the subject: (1) whether the focal point of the image the subject's genitalia or pubic area; (2) whether the setting of the image is sexually suggestive; (3) whether the subject is depicted in an unnatural pose or in inappropriate attire considering the age of the child; (4) whether the subject is fully or partially clothed, or nude; (5) whether the image suggests sexual coyness or willingness to engage in sexual activity; and (6) whether the image is intended or designed to elicit a sexual response in the viewer. United States v. Dost, *636 F. Supp. 828, 832 (S.D. Cal. 1986), aff'd sub nom.,* United States v. Wiegand, *812 F.2d 1239, 1244 (9th Cir. 1987).*

Navigating legal requirements while also respecting users' rights to free expression can be difficult. Many companies adopt qualified prohibitions against nudity, while expressly prohibiting any sexualized depictions of minors. For example, Facebook's Community Standards state that:

> We remove content that threatens or promotes sexual violence or exploitation. This includes the sexual exploitation of minors and sexual assault. To protect victims and survivors, we also remove photographs or videos depicting incidents of sexual violence and images shared in revenge or without permission from the people in the images.

Despite the ambiguities in the law, failing to identify content that violates the law can create direct liability for an OSP and increase the potential for extraordinary crimes against children, including human trafficking, forced prostitution, and other human rights violations. In addition, an OSP can incur direct liability if it fails to remove this type of content in response to a takedown request. Section 2258A of the Act requires that online service providers who know about violations of child protection statutes report those violations to the CyberTipline of the National Center for Missing and Exploited Children (http://www.missingkids.com/cybertipline/), with substantial fines for not doing so. Accordingly, it is prudent for you to take a conservative approach with regard to this type of content to ensure the protection of children online.

Action Items

- ❑ Develop a clear public-facing policy that notifies your users what types of content are prohibited and allowed, and how the company will respond to users that violate this policy.
- ❑ If you identify content that violates the law and/or your corporate policy, remove the offending image or links immediately.

- ❑ If you determine that a user is posting child pornography, you should terminate the user's account and report the offender to appropriate authorities. While there is no legal requirement for OSPs to seek out content containing child pornography, many providers do so in order to minimize public relations or compliance problems. Consider whether your company should proactively monitor for this type of content depending on the services that you offer.

- ❑ Consider, based on your service offering, whether you need to implement practices and policies for the protection of children.

- ❑ Create an internal escalation process to ensure that your legal team is notified whenever potential child pornography has been identified either internally or by a third party.

Resources

Statutes

- Child Protection and Sexual Predator Act of 1998, 18 U.S.C. § 2252

Other References

- Department of Justice: Child Exploitation & Obscenity Section, *available at* http://www.justice.gov/criminal/ceos/subjectareas/childporn.html
- E-Commerce and Internet Law 49.10[1] (2012-2013 update)
- Electronic Frontier Foundation, Legal Guide for Bloggers, "Adult Material", *available at* https://www.eff.org/issues/bloggers/legal/adult
- Thorn, Sound Practice Guide to Fight Child Sexual Exploitation Online (August 2014), *available at* https://www.wearethorn.org/sound-practices-guide-stopping-child-abuse/

CHAPTER 3:
Government Requests for User Data

Data generated by your users can be an important source of evidence for law enforcement officials seeking to investigate individuals, groups, or activities. Governments are increasingly seeking disclosures from companies regarding specific user accounts and/or communications.

If your company hasn't already received a law enforcement request for user data, it is likely only a matter of time before it does.

GOVERNMENT REQUESTS FOR USER DATA

In the first half of 2015, Google received 35,365 requests for user data from governments around the world, while Microsoft received 35,228 requests in the same period. Smaller, earlier-stage companies regularly receive such requests as well, albeit in smaller numbers. For example, in the first half of 2015, Dropbox received 406 requests for user information from U.S. law enforcement officials and 7 requests from non-U.S. authorities.

Key Concepts and Considerations

You should consider the following concepts in thinking about how your company will respond to government requests:

Jurisdiction

As discussed in Chapter 1, requests for user information may come from law enforcement officials within or outside the United States. How you structure your company and its operations, including where you locate your personnel and equipment, may impact where you may be subject to enforceable requests, and the number of requests that you can expect to receive.

If you deliver services or store data outside the U.S., you may be subject to requests by non-U.S. officials for user data. That said, simply allowing your services to be accessed by users outside the U.S. does not necessarily subject your company to the laws of foreign countries. To know how and when you need to respond to foreign government requests for information, you need to identify which countries may assert jurisdiction over data held by your company.[3]

In thinking about jurisdiction, you should consider the following questions:

- Do you know the full list of countries whose governments can make valid requests of your company and enforce them against employees or equipment you may have on the ground there?
- Do you understand what constitutes a valid request for user data in each country where your company may face an enforceable government demand?
- Have you investigated the extent to which the relevant government(s) are known to issue requests that are illegitimate, overbroad, or abusive?
- If you work with third party service providers that store or process data on behalf of your company, do you understand where they do so, and what laws might apply to them?

[3] It is outside the scope of this guide to provide information regarding the legal regimes of all of the countries in which your company may be subject to requests. You should seek advice from legal counsel with knowledge as to the legal requirements in each country in which your company may be subject to law enforcement requests.

Types of Data

What types of data does your company generate?

You should review your operations and the services you provide to users, and should determine what types of data may be subject to law enforcement requests.

Law enforcement officials may make requests for the **content** of user communications or accounts, or for **non-content** data regarding these accounts, including users' names and addresses, the dates and times of communications, and users' IP addresses. The law affords greater protections when content is being sought, when compared to non-content data.

Companies are generating new types of data with every new product and service they offer. Often, it is not clear whether new kinds of data are content or non-content, so your company may need to make initial judgments on how you will treat such information. The table below illustrates how certain kinds of data have been categorized by courts in the United States:

NON-CONTENT DATA	CONTENT DATA
• Basic subscriber information (name, username, address) • Email header fields • Transactional log information (including IP address, session length, etc.)	• Text of an email • Contents of a file stored "in the cloud" • Information exchanged during a Skype, Google Hangouts, or FaceTime conversation

Users' Rights and Maintaining Trust

Many law enforcement requests are made for legitimate reasons in accordance with relevant legal standards. Governments are by no means immune, however, from making requests for user data that are unlawful, illegitimate, or both. *Such requests can impact and even violate the rights of your users, including their internationally recognized rights to privacy, free expression, and fair judicial process.*

The importance of thoughtfully managing your company's responses to unlawful or illegitimate requests is now greater than ever, in view of the continuing public concerns over the scope and extent of government surveillance activities around the world. As some companies have learned the hard way, failing to respond to such requests in an appropriate manner can result in serious consequences for your users. This, in turn, may expose your company to bad publicity and legal liability. A poorly considered response may also undermine the user trust that is a critical asset for any company, so taking steps to protect this trust in your responses to government requests is good for your users and good for your business.

THE CASE OF YAHOO! AND SHI TAO

One of the highest-profile examples of the perils around disclosing user data to a government involves Yahoo!, which was sued after its Chinese subsidiary disclosed account data that Chinese law enforcement used to arrest and imprison a political dissident.

Specifically, in 2004, the company responded to a request from the Beijing State Security Bureau for data from an account that was used to send emails regarding government press restrictions during the fifteenth anniversary of the 1989 Tiananmen Square protests. The account belonged to Chinese journalist Shi Tao, who was arrested and sentenced to ten years' imprisonment for "providing state secrets to foreign entities." After serving eight-and-a-half years, Shi Tao was released from prison in September 2013.

Statutory Authority for Government Requests

This section provides an overview of the law governing how and when U.S. state and federal agencies can request user data. It includes an overview of jurisdictional considerations and the primary statutes that govern these requests.

While the statutes summarized below provide the authority for law enforcement requests, their application is always subject to the protection against unreasonable searches and seizures enshrined in the Fourth Amendment to the U.S. Constitution (see text box).

FOURTH AMENDMENT TO THE U.S. CONSTITUTION

The Fourth Amendment provides that all people in the United States have a constitutional right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure…"

In the physical world, this means that the government cannot search a person's house or property without a warrant issued by a judge (save for certain exceptional circumstances). In the digital world, whether or not the government needs a warrant to search a particular kind of data depends on whether a person has a "reasonable expectation of privacy" in that information. Courts have held that individuals don't have a reasonable expectation of privacy in information that they share with third parties. Therefore, no warrant is required to search an individual's bank records, because these are "shared" and routinely viewed by bank employees. Courts are still grappling with when this "third party doctrine" applies to searches of data stored with third-party online service companies, such as webmail and cloud storage providers.

The Electronic Communications Privacy Act (ECPA) is the most important federal law governing searches of digital information. ECPA includes there component statutes: the Stored Communications Act, the Wiretap Act, and the Pen/Trap Statute – each of which are discussed in turn, below.

The Stored Communications Act

The Stored Communications Act (SCA) is the primary statute defining when U.S. law enforcement may compel a company to disclose information relating to electronic communications, or information stored in the cloud. It protects user privacy by restricting companies from disclosing content or non-content data to the government, unless the company is properly served with a warrant, court order, or subpoena.

Enacted in 1986, the SCA is significantly out of date and not always easy to apply to new technological situations. Apart from the difficulties associated with categorizing new kinds of data as content or non-content, a further problem arises from the SCA's division of online services into two categories:

- *Electronic Communications Services (ECS)* are those providing customers with the ability to send or receive electronic communications.
- *Remote Computing Services (RCS*) are those providing customers with data storage or processing services.

The distinction between ECSs and RCSs generally turns on how long a company stores information on behalf of its customers. A company is providing an ECS when it only stores communications temporarily for transmission purposes. By contrast, any service that stores customer communications or files for an extended period is likely an RCS. Courts have found that companies like Facebook and Google provide both ECS ("message delivery") and RCS ("message storage") services.

Content Data from ECS Providers

The SCA requires law enforcement to obtain a **warrant** to compel an ECS provider to disclose the content of unopened electronic communications, such as emails, that have been stored for 180 days or less.

The text of the SCA treats the contents of electronic communications stored with an ECS provider for more than 180 days according to the standards applied to RCS providers. That said, one federal appellate court has ruled that a warrant is required for law enforcement to access the content of user communications stored on an ECS provider's servers for any length of time. *United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010). Consequently, many ECS providers now follow the "Warshak Rule" and require law enforcement to get a warrant before they will hand over any communications content data.

Content Data from RCS Providers

Under the SCA, law enforcement may obtain content data from RCS providers with either a **warrant**, a **court order,** or an **administrative subpoena** (see below for further explanations as to the differences between these documents).

As noted above, ECS providers that store communications content for more than 180 days may be treated as RCS providers. If you provide email, text or other electronic communications services, you should be aware of how long you store these communications, and for what purpose, to determine the appropriate method for law enforcement to obtain content data stored on your servers.

Non-Content Data

Under the SCA, law enforcement may request ECS or RCS providers to disclose non-content data through either a **warrant** or a **court order**.

Non-content data, also known as metadata, includes:

- Email addresses;
- Usernames;
- Server logs;
- File sizes; and
- IP addresses.

Since the SCA did not anticipate many of the types of communication services that are in use today, this list should be viewed as illustrative. Different courts may well reach different conclusions as to whether a given piece of data is content or non-content.

Certain types of non-content data, commonly referred to as "subscriber information," may be requested through an **administrative subpoena,** including:

- Names;
- Addresses;
- Local and long distance telephone connection records, or records of session times and durations;
- Length of service (including start date) and types of service utilized;
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and types of payment for services (including any credit card or bank account number).

COMPANIES THAT OBSERVE THE "WARSHAK RULE"

In 2015, the Electronic Frontier Foundation publicly recognized the following companies for requiring a search warrant for the disclosure of the contents of stored user communications: Adobe, Amazon, Apple, AT&T, Comcast, Credo Mobile, Dropbox, Facebook, Google, LinkedIn, Lookout, Microsoft, Pinterest, Reddit, Slack, Snapchat, Sonic.net, Spideroak, Tumblr, Twitter, Verizon, Wickr, Wikimedia Foundation, Wordpress, and Yahoo!

The Wiretap Act

The Wiretap Act is a component statute of ECPA governing when the content of phone calls, emails, and other electronic communications may be intercepted in real time. As a default rule, ECPA bans anyone from intercepting or recording the content of such communications without the consent of at least one party to the communication. (Note, however, that 12 states have their own wiretapping laws requiring the consent of all parties to a communication before it may be lawfully recorded.)

The Wiretap Act requires law enforcement to get a **warrant** to conduct a real-time intercept (save for two exceptions, detailed below). If your company is asked to assist law enforcement in conducting a real-time intercept, you will be reimbursed for your expenses and granted immunity from criminal prosecution and civil liability relating to your assistance. You must not, however, publicly disclose the fact that a real-time intercept is taking place, or else you will be subject to significant penalties.

The first exception to the warrant requirement is for emergencies. If law enforcement reasonably determines that an intercept is required to respond to an emergency involving: (1) immediate danger of death or serious injury to any person; (2) a conspiracy against national security interests; or (3) an organized criminal conspiracy, it may conduct an emergency wiretap for up to 48 hours before obtaining a court order. In such circumstances, you will receive a written certification from a prosecutor or a law enforcement officer stating that no court order is required to conduct an intercept in view of the emergency.

The second exception to the warrant requirement is for foreign intelligence gathering. Such intercepts are not subject to the provisions of the Wiretap Act, but are instead governed by the separate Foreign Intelligence Surveillance Act, which is discussed elsewhere in this chapter.

The Pen/Trap Statute

The Pen/Trap Statute governs the real-time interception by law enforcement of a category of non-content information known as "dialing, routing, addressing, and signaling" information. Examples of such information include: the phone number of an incoming or outgoing call as it is placed or received, the destination of an email as it is being sent, or the IP address of a website as the user loads it in their browser.

The Pen/Trap Statute requires law enforcement to obtain a **court order** before intercepting non-content communications data in real time. It provides companies with legal immunity and monetary compensation when they assist law enforcement in intercepting and capturing such information, and it also bars companies from disclosing the existence of an intercept subject to penalties.

The Pen/Trap Statute contains an emergency exception that permits intercepts for up to 48 hours without a court order. The only difference with the Wiretap Act's emergency provisions is that the Pen/Trap Statute also recognizes an ongoing attack against government, financial, or commercial computer systems as additional emergency situations.

THE WIRETAP ACT AND THE PEN/TRAP STATUTE

Both the Wiretap Act and the Pen/Trap Statute permit communications providers to conduct real-time intercepts for certain purposes. For example, "record[ing] the fact that a wire or electronic communication was completed or initiated," such as by capturing the date, time, duration, origin, and destination of a communication, is permitted under both statutes. So too is the interception of content and non-content information when it is needed to protect the provider's rights and property, such as in detecting billing fraud.

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

While the Wiretap Act and the Pen/Trap Statute require service providers to assist law enforcement in carrying out real-time intercepts to the best of their abilities, a federal statute called the Communications Assistance for Law Enforcement Act (CALEA) requires "telecommunications carriers" to build certain technical capabilities into their networks to facilitate government wiretapping. There is uncertainty as to what constitutes a "telecommunications carrier" within the meaning of this statute. Landline and mobile phone operators clearly fit the definition, but in 2006, a federal appeals court confused matters by ruling that VoIP telephony providers such as Vonage are subject to CALEA. Some companies have taken the position that their application-based VoIP services are not subject to CALEA, but your company should seek advice on CALEA compliance if you are considering including voice or video chat functionality in a product.

Requests from Non-U.S. Law Enforcement Officials

If law enforcement officials from outside the United States wish to access content data stored in the United States, they must seek the assistance of the U.S. Government in obtaining it. They may do so by invoking the provisions of a Mutual Legal Assistance Treaty (MLAT), or issuing "letters rogatory" directed at the U.S. government. The U.S. Department of Justice reviews all such requests and will obtain the requested information on behalf of the foreign government so long as the request satisfies ECPA and all other relevant U.S. legal requirements.

By contrast, if foreign law enforcement officials seek non-content data stored in the U.S., a company is free to disclose such data if it wishes, though it is not required to do so. Most large tech companies have policies in place to scrutinize and evaluate such requests in deciding whether to comply with them.

If you receive a request from foreign law enforcement, you should consult with an attorney to understand your obligations under U.S. law and the law of the requesting country. You should also understand whether or not you are permitted to inform the user that a request has been made, regardless of whether you will ultimately be disclosing any information to a government as a result.

National Security and Foreign Intelligence Investigations

Revelations regarding the U.S. government's ability to conduct surveillance for foreign intelligence purposes have sparked a continuing debate on the appropriate balance between civil liberties and national security. This section describes some of the key statutory provisions that govern when U.S. officials can seek data from companies when conducting such investigations.

National Security Letters

The USA FREEDOM Act authorizes the Federal Bureau of Investigation (FBI) to issue a specific type of administrative subpoena, known as a **national security letter**, for subscriber information or electronic communication transaction records in connection with certain national security investigations.

Specifically, the FBI may request that you provide the name, address, length of service, and billing records of a "person or entity" if the FBI certifies in writing that those records are relevant to an authorized investigation into "international terrorism or clandestine intelligence activities." Companies are obligated to comply with these requests.

If you receive a national security letter, you are generally prohibited from disclosing to anyone that the FBI has sought or obtained access to information. You may only inform those people at your company whose assistance is required in order to respond to the request. You may also inform outside attorneys whom you consult regarding the request.

"Tangible Things"

The USA Freedom Act also allows the U.S. government to seek a **court order** from the Foreign Intelligence Surveillance Court (FISA Court) requiring a company to produce "tangible things"—such as records and documents—for investigations involving foreign intelligence or to protect against international terrorism.

"Tangible things" are presumed to be relevant to an investigation if the FBI demonstrates that they pertain to:

1. A foreign power or an agent of a foreign power;
2. The activities of a suspected agent of a foreign power who is the subject of an authorized investigation; or
3. An individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation.

In using the "tangible things" provision, the government must limit any given request by using selection terms that specifically identify a person, account, address, personal device, or some other similar specific identifier. Following reforms in 2015, the government can no longer use the "tangible things" provision to engage in the bulk collection of records pertaining to large numbers of individuals, as it did prior to the Snowden revelations.

Requests made under the business records provision of FISA are subject to the same non-disclosure provisions as national security letters.

Section 702 Orders

Section 702 of the FISA Amendments Act of 2008 provides the Attorney General and the Director of National Intelligence with authorization to conduct secret investigations of foreign nationals located outside the United States if they can show the FISA Court that the foreign intelligence is "important to the national security of the United States."

The FISA Court must authorize such investigations. After such authorization is provided, the Attorney General and the Director of National Intelligence may request such information through specialized directives.

NOTE RE: INVESTIGATIONS PURSUANT TO EXECUTIVE ORDER 12,333

Executive Order 12,333 was originally signed by President Ronald Reagan in 1981 and has been subsequently modified several times. This Executive Order provides authority to U.S. intelligence agencies, including the National Security Agency (NSA) and the Central Intelligence Agency (CIA), to conduct surveillance of foreigners outside the United States.

Relatively little is known about the activity of U.S. intelligence agencies pursuant to Executive Order 12,333, which has allegedly been used as the basis for NSA efforts to intercept communications data traveling between corporate data centers. In December 2013, the American Civil Liberties Union filed a lawsuit seeking more information on the rules and procedures that govern the activities of U.S. intelligence agencies pursuant to authority provided under this Executive Order. Notably, surveillance conducted pursuant to the authority granted by this Executive Order is not subject to review by the FISA Court.

Managing Government Requests in Practice

In thinking about how best to manage your company's responses to law enforcement requests, you should consider the following questions:

- Do you have a process in place to respond to law enforcement requests? What internal or external resources do you need to properly respond to these requests?
- Do you have a process dictating how you might respond to requests that may be abusive or invalid?
- Does your company inform users when a government or law enforcement agency makes a request for their account information or communications?
- How transparent are you regarding the types of requests that you receive and how you respond to those requests?

Recognizing that many companies rely on third-party service providers to handle data, you should also consider the following issues:

- Do you use third parties to host or distribute any of your user data? Do you have business partners that have operational control over your user data? If so, do you know how they respond to law enforcement requests? And have you communicated your policies on responding to law enforcement requests to them?
- Do you know whether you can require these third parties to abide by your company's process requirements?

At minimum, your company should ensure that all requests received from the government:

- Comply with all legal requirements; and
- Are appropriately tailored to address the legitimate needs of the agency requesting the information.

Companies should assess whether requests seem overbroad and, if so, should consider how best to respond without providing more information than necessary. This could include pushing back on overbroad requests or tailoring responses narrowly.

Ultimately, if the government fails to meet its legal obligations, you should consider challenging the request. You should also ensure that you have an escalation process in place to ensure that difficult requests receive appropriate attention from senior members of your company.

The information below is intended to provide guidance on considerations that should inform your review of specific types of law enforcement requests. This information is necessarily general: if you have questions about a specific law enforcement request, you should consult counsel.

Standard Legal Process Requests

Search Warrants

A search warrant is an order issued by a judge that permits law enforcement to search designated premises for designated evidence. As discussed above, a search warrant is required to obtain the content of user communications, especially if those communications are less than 180 days old.

Generally, a judge or a magistrate issues a search warrant, although other judicial officials, such as clerks of court, may issue search warrants in certain circumstances.

What does law enforcement need to show to obtain a search warrant?

To obtain a warrant, law enforcement must convince a judge or magistrate that *probable cause* exists to believe that the requested information is either evidence of a crime or contraband (such as child pornography). Law enforcement must also provide a judge or magistrate with specific details regarding the device(s) or account(s) to be searched and the evidence that is being sought.

What should you look for when reviewing a search warrant?

A valid warrant should include:

- A recent date;
- Specific information regarding the device(s) or account(s) to be searched;
- Specific details regarding the type of information that is being sought; and
- The signature of a judge or magistrate.

Can you challenge a search warrant?

If you receive a valid warrant that meets these requirements, you must comply with the search (even if you do not agree with the warrant).

Your customer can subsequently challenge the validity of the search in court, but law enforcement does not have to obtain your consent to obtain the information covered by the warrant.

Can you notify impacted users?

Search warrants are often accompanied by orders directing companies not to notify "any other person" of the existence of the warrant. Companies can seek to challenge such gag orders.

If you do not receive an order telling you not to disclose the search warrant, you are free to notify impacted users.

Section 2703(d) Orders

Section 2703(d) of ECPA provides law enforcement with authority to seek court orders requiring the disclosure of specified information.

What does law enforcement need to show in order to obtain a court order?

Under the SCA, law enforcement can obtain a court order by offering "specific and articulable facts" showing that there are "reasonable grounds" to believe that the contents or records being sought "are relevant and material to an ongoing criminal investigation." This is an easier standard for law enforcement to satisfy than the "probable cause" standard that governs the issuance of search warrants.

What should you look for when reviewing a court order?

A valid court order should include:

- The signature of a judge; and
- Specific description(s) of the data that is being requested, including specific dates.

To be valid, a court order should be issued by a court has jurisdiction over the matter. This could be a federal district court that has jurisdiction over the place where your company is based, or where the data being requested is stored. You should consult with counsel to understand what courts have "competent jurisdiction" to issue a court order to your company.

Can you challenge court orders?

You may challenge the validity of a court order before complying.

Section 2703(d) specifically notes that a court may quash or modify an order, upon receiving a motion from a service provider "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."

Can you notify impacted users?

Court orders requesting the disclosure of information may be accompanied by orders directing companies not to disclose that such a request has been received. If you do not receive such a non-disclosure order, you are free to notify impacted users.

Notably, the SCA requires the government to provide prior notice to the individual whose information is being requested through a court order, unless the government has sought specific authorization to delay notice.

Subpoenas

An *administrative subpoena* is a form of request issued by law enforcement seeking evidence relevant to the investigation of a specific crime. Judges play no role in the issuance of administrative subpoenas.

A *judicial subpoena* is a form of subpoena that has been issued by a judge, clerk, or officer of a court.

What does law enforcement need to show in order to obtain a subpoena?

Instead of *probable cause,* law enforcement only needs to establish a *reasonable belief* that the information requested will produce information *relevant* to a specific investigation. This is a weaker standard even than what is required to obtain a Section 2703(d) order.

What should you look for when reviewing a subpoena?

A valid subpoena should include:

- The name of the court or administrative body that issued it;
- The title of the relevant proceeding and a case number; and
- Specific information identifying the information that is being sought, which may include a requested appearance to testify and/or produce documents.

A valid subpoena must also be properly served by a qualified process server. The requirements for proper service of process are generally governed by state law. Questions as to whether your company has been properly served should be referred to counsel.

Can you challenge a subpoena?

Unlike a warrant, you can ask a judge to quash a subpoena before complying with it.

If you do not challenge a judicial subpoena and you fail to comply, you can be held in contempt of court. You cannot be held in contempt of court for failing to comply with an administrative subpoena unless the issuing agency has asked a court to compel your compliance.

Before complying with any subpoena, it is a good practice to ensure that it is not overbroad and that the information requested relates to the relevant investigation.

- *Example of Overbroad Request:* Every file stored by John Smith.
- *Example of Narrow Request:* Every file uploaded or downloaded by John Smith and Jane Doe between February 20-29, 2016.

Can you notify impacted users?

You can notify your users of subpoenas, unless law enforcement has obtained a court order prohibiting such disclosure.

When the government requests information through a subpoena, the SCA requires it to provide notice to the affected individual, unless the government seeks and obtains the authorization of a court to delay notice.

Wiretap Orders

A wiretap order is a special kind of warrant permitting the real-time interception and capture of the content of communications.

What does law enforcement need to show in order to obtain a wiretap order?

Law enforcement must first affirm that "normal investigative techniques" have been tried and failed, won't work, or are too dangerous to try given the circumstances. They must then satisfy a judge that *probable cause* exists to believe all of the following:

(1) one or more specified offenses (including murder, robbery, drug trafficking, and most other felonies) has been or is about to be committed;
(2) the wiretap will intercept "particular communications" concerning that offense; and
(3) the communications facility to be wiretapped is either commonly used by the suspect (*e.g.*, their personal cell phone), or being used or about to be used in connection with the offense.

What should you look for when reviewing a wiretap order?

A valid wiretap order should include:

- the nature and location of the communication facilities that will be wiretapped;
- a statement of the particular offence to which the wiretap relates;
- the identity of the agency authorized to intercept the communications;
- the signature of a judge or magistrate; and
- a date less than 30 days ago.

Can you challenge a wiretap order?

No. Only individuals with a privacy interest in the communications that are being intercepted may challenge a wiretap order.

Can you notify impacted users?

If you receive a valid court order or request under the Wiretap Act, you are obligated to maintain the confidentiality of the order and can be sanctioned under the statute if you disclose the fact that a wiretap is taking place.

National Security and Foreign Intelligence Requests

Requests for "Tangible Things"

The Foreign Intelligence Surveillance Court may issue orders requiring a company to produce records and documents for investigations involving foreign intelligence or to protect against international terrorism.

What does law enforcement need to show in order to obtain a FISA court order for business records?

In seeking an order for business records from the FISA Court, the FBI need only show that the requested records either pertain to a foreign power or to an authorized investigation of an agent of a foreign power or someone in contact with them. The FBI must also provide details of the specific procedures it will employ to "minimize" the amount of information it incidentally collects concerning non-consenting U.S. citizens and permanent residents.

What should you look for when reviewing a FISA court order?

A valid FISA court order should include:

- The signature of a judge;
- A specific description of the information that is being requested, including relevant dates;
- The dates by which such information must be produced; and
- "Clear and conspicuous" notice of the relevant non-disclosure requirements and principles, including notification that you may contact an attorney to provide advice regarding your response.

Can you challenge a FISA court order?

Orders received from the FISA Court may be challenged through a specialized petition process. Yahoo! was recognized by many civil liberties groups, including the Electronic Frontier Foundation, for mounting an ultimately unsuccessful challenge to a FISA court order in 2008.

Can you notify impacted users?

No. As with national security letters, if you receive a FISA court order, you are generally prohibited from disclosing to anyone that the FBI has sought or obtained access to information. You may only inform those people at your company whose assistance is required in order to respond to the request. You may also inform outside attorneys whom you consult regarding the request.

Section 702 Orders

The Attorney General and the Director of National Intelligence, if authorized by a FISA Court order, may issue a specialized directive to a company directing it to provide all "information, facilities, and assistance" necessary to conduct an investigation targeting persons reasonably believed to be outside the United States for the purposes of acquiring foreign intelligence information.

What does law enforcement need to show in order to obtain authorization to issue a directive?

The Attorney General and the Director of National Intelligence must certify to the FISA Court that procedures are in place to ensure that the requested acquisition is targeting persons "reasonably believed to be outside the United States."

The required certification must also attest that procedures are in place to "prevent the acquisition of any communication" to or from any individuals that are known to be located in the United States. The government must also attest that procedures are in place to minimize the acquisition and retention of information concerning non-consenting U.S. citizens and permanent residents.

What should you look for when reviewing a directive?

Once they have made the required certifications to the FISA Court, the Attorney General and the Director of National Intelligence have the authority to issue a written directive to a company directing it to immediately provide the requested assistance or information.

You may seek compensation from the government for the costs associated with any assistance you provide the government when responding to the written directive.

Can you challenge a directive?

Directives received from the Attorney General and the Director of National Intelligence in connection with the investigation of foreign nationals may be challenged through a specialized petition process.

If you wish to challenge a directive, you should consult with counsel regarding the filing of a petition.

Can you notify impacted users?

No. You must provide this requested information in a manner that will prevent the intended target(s) from finding out the information was requested or delivered, and in a manner that will minimally impact the target's use of your services. The goal of these requirements is to ensure that the secrecy of the government request for information is maintained.

Emergency Requests

ECPA and its component statutes contain emergency provisions allowing companies to voluntarily disclose content and non-content information to U.S. and foreign law enforcement when "an emergency involving danger of death or serious physical injury to any person" exists. In evaluating emergency requests, you need to balance the need for quick information disclosures to respond to bona fide emergencies against the risk that law enforcement may misuse this exception for any number of reasons.

Best practices require law enforcement to submit emergency requests in writing, with a description of:

- the nature of the emergency;
- what information is being requested; and
- why such information is necessary to prevent an identified harm.

The nature of emergencies requires that such requests be evaluated on a case-by-case basis. Your company will need to make quick determinations as to whether an emergency truly exists, and what data you should disclose in response. By requiring that law enforcement submit emergency requests in writing, a written record is generated that you can use in evaluating current and future requests. Some companies have developed standard forms for law enforcement to use in making emergency requests.

Best Practices in Managing Law Enforcement Requests

Transparency Reports

Being transparent on how your company responds to law enforcement requests helps your customers understand what protections apply to their information and what you are doing to protect their rights. You should therefore consider publishing a "transparency report" with statistics indicating how many law enforcement requests your company has received and how often you have provided data in response to such requests. Publishing transparency reports has become a best practice for technology companies.

Even if you are not ready to publish a transparency report, you should start compiling and organizing information regarding these requests starting right now. This aids your company in auditing your process for responding to law enforcement requests, and it ensures that you have the information you need to publish a transparency report when you are ready. Specifically, you should start tracking and storing the following information for all requests you get from law enforcement:

- The date you received the request;
- The date you responded;
- Who responded;
- What the response was;
- The agency/government making the request;
- The legal authority under which they made the request;
- The number of accounts impacted by the request;
- Whether the government requested content or not;
- Whether you provided content or not;
- Whether you complied in part or in whole;
- Whether you pushed back or not;
- Your basis for pushing back; and
- Whether you provided notice to the users.

Tracking this information is not only useful for internal purposes, but ensures that you can provide accurate information to your users if and when you choose to create and publish a transparency report.

National Security/Foreign Intelligence Requests

While companies are generally prohibited from providing any information regarding requests received pursuant to U.S. national security laws, companies may disclose the following information in bands of 1000 at six-month intervals:

- the number of national security letter requests that they received;
- the number of customer accounts affected by national security letters;
- the number of FISA orders for content that they received;
- the number of customer selectors targeted under FISA content orders;
- the number of FISA orders for non-content that they received; and
- the number of customer selectors targeted under FISA non-content orders.

For example, if your company received 53 NSL requests during the previous six months, you could disclose that you received between 0-999 requests.

Alternatively, companies can disclose, in bands of 250:

- the total number of all national security letter and FISA requests received; and
- the total number of customer selectors targeted by national security letter and FISA requests.

For example, if in a six-month period your company receives 26 NSLs pertaining to 82 accounts, and 53 FISA court orders targeting 320 people, you may publicly report that you received 0-249 requests implicating 250-499 selectors.

Early-stage companies should be aware that the Department of Justice has imposed a two-year delay on the publication of information regarding certain orders received with regard to new platforms, products, or services. Specifically, if you receive an order designated by the government as a "New Capability" order, you are prohibited from making any disclosures regarding that request for two years. The "New Capability" order is intended to address new platforms, products or services for which a company has not previously received a national security request. The restriction does not apply if your company has already made disclosures of national security requests received in relation to the platform, product, or service in question.

TRANSPARENCY REPORTS

In its 2015 Who Has Your Back? report, the Electronic Frontier Foundation recognized Adobe, Amazon, Apple, AT&T, Comcast, Credo Mobile, Dropbox, Facebook, Google, LinkedIn, Microsoft, Pinterest, Reddit, Slack, Snapchat, Sonic.net, Tumblr, Twitter, Verizon, Wickr, Wikimedia, Wordpress, and Yahoo! for publishing transparency reports. The report observed that "transparency reports are now industry standard practices."

Law Enforcement Guidelines

As you develop your policies and procedures for responding to law enforcement requests, you may also wish to consider making public your guidelines for law enforcement. An increasing number of companies are publishing such guidelines, which provide clear guidance to law enforcement officials – and your users—regarding the company's policies and procedures.

Topics that are frequently covered in law enforcement guidelines include:

- the information that should be included as part of any request (i.e., contact information for the requesting officer, response deadlines, etc.);
- whether the company requires a warrant for content data;
- what the company's requirements are for the submission of emergency requests;
- what the company's requirements are for the submission of requests by non-U.S. law enforcement officials; and
- what the company's policies are with regard to the notification of users about specific requests.

These guidelines can help ensure that the requests you receive are legitimate and appropriately tailored. In addition, such guidelines provide your users with valuable insight into the policies and practices in place to protect their rights.

LAW ENFORCEMENT GUIDELINES

In its 2015 Who Has Your Back? report, the Electronic Frontier Foundation recognized the following companies for publishing law enforcement guidelines: Adobe, Amazon, Apple, AT&T, Comcast, Credo Mobile, Dropbox, Facebook, Google, LinkedIn, Microsoft, Pinterest, Reddit, Slack, Snapchat, Sonic.net, Tumblr, Twitter, Verizon, Wickr, Wikimedia, Wordpress, and Yahoo!.

Action Items

Legal Review and Policy Development

- ❑ Review your company's operations and identify all jurisdictions in which law enforcement may request access to data held by the company and enforce such requests against company personnel.
- ❑ Create an internal policy defining how the company plans to address law enforcement requests, including an escalation plan that defines when a request must be sent to external counsel or to senior executives for review.
- ❑ Draft a customer-facing policy that clearly communicates how requests from law enforcement are handled, and when you will or will not be able to inform customers of these requests.

Human Rights Review

- ❑ Conduct human rights due diligence to identify, prevent, and mitigate adverse human rights impacts associated with offering new services or expanding to a new country.

Managing Relationships with Third Parties

- ❑ Conduct due diligence on your third party service providers to understand how they store and manage your users' information, including: where their servers are located; where they store, process, or manage any data on your behalf; and in which jurisdictions they may be subject to enforceable requests.
- ❑ Create template requirements to include in any RFPs for third party vendors, including restrictions as to where and how the vendors may store, use or process data.

Training and Capacity Development

- ❑ Train all relevant personnel on how to respond to law enforcement requests, including who to consult within the company regarding questions or concerns about the validity of, or potential concerns regarding, specific requests.
- ❑ Train all relevant personnel on the potential human rights impacts of law enforcement requests with a focus on the concerns most relevant to the jurisdictions in which your company is subject to enforceable requests.
- ❑ Identify and engage with relevant external stakeholders that can help the company build capacity to respond in a responsible and transparent manner to law enforcement requests. This may include outside counsel, human rights consultants or even advocacy organizations. You should create a plan on how and when to engage external stakeholders to help you address these types of issues.

Transparency

- ❑ Consider publishing a transparency report on the types of law enforcement requests received by the company, and the quantity for each type. Bear in mind that you may not legally be able to report actual numbers depending on the type of request.

Resources

Statutes

- Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq.*
- Stored Communications Act, 18 U.S.C. §§ 2701-2711
- Wiretap Act, 18 U.S.C. §§ 2510-2522
- Pen/Trap Statute, 18 U.S.C. §§ 3121-3127
- Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010
- Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq*.
- USA FREEDOM Act

Other References

- Global Network Initiative, Implementation Guidelines, *available at* https://globalnetworkinitiative.org/implementationguidelines/index.php
- Electronic Frontier Foundation, Who Has Your Back? (2015) *available at* https://www.eff.org/who-has-your-back-2015
- Congressional Research Service, Privacy: An Overview of the Electronic Communications Privacy Act (October 9, 2012), *available at* http://www.fas.org/sgp/crs/misc/R41733.pdf

CHAPTER 4:
Privacy & Security by Design

This chapter explores the various consumer privacy and data security issues online service providers may encounter, especially as companies continue to collect more and more data and information from and about their customers. Specifically, the chapter aims to provide some best practices for the implementation of privacy-protecting data and information practices that, in turn, will help companies gain the trust of their users.

Before getting into the law, it is important to understand the difference between privacy and data security. While the two concepts are linked, they are not the same; and understanding the differences can help a company establish sound privacy and data security practices.

Privacy

Privacy deals with how companies collect, use, and share information from and about their customers that is *personally identifiable*. Different statutes define personally identifiable differently, but in general, such information includes a customer's name, date of birth, address, social security number, financial information, IP address, and anything else that could be used to determine an individual's identity. Companies should keep in mind that data which, on its own, may not be personally identifiable could become so if an individual could be identified by matching that piece of information with other information.

As a general principle, companies should strive to limit their collection of personally identifiable information. This does not mean that all data collection should be avoided, nor does it mean that companies should not collect personally identifiable information; rather, companies should collect only whatever information is necessary to provide their products and services and not a byte more.

Collecting additional information that is not really needed carries the risk of upsetting customers and attracting unwelcome attention from regulators. For example, when Google's Street View vehicles were caught capturing data from unprotected Wi-Fi networks all over the world, consumers, lawmakers, and privacy advocates responded with outrage.[1] While Google's unlawful practices resulted only in nominal fines of $25,000 in the United States[1] and €145,000 in Germany,[1] the incident tarnished the tech giant's reputation and has contributed to public skepticism about its data collection practices.

Data Security

Data security deals with how safely personally identifiable information is stored once it is collected. As people everywhere produce, store, and transmit ever-increasing quantities of personal, sensitive, and confidential information online, securing such data against cyber-attackers and accidental disclosures has never been more challenging – or important.

LinkedIn made headlines for its data security practices in the summer of 2012, when hackers made off with 6.5 million passwords from the popular social networking site. Since the passwords had been secured using only the SHA-1 hashing algorithm and nothing more, hackers were able to decrypt two-thirds of them in a matter of days. A lawsuit filed against LinkedIn in the aftermath of the breach was ultimately dismissed on a technicality, but the company's reputation for protecting user information suffered as a result.

It may not be possible to guarantee the security of all data at all times, but your company can discharge its duty to protect the privacy of its customers' information by employing security protocols that meet or exceed industry standards. Failing to employ the latest security measures, on the other hand, will almost certainly lead to a security breach and to the wrong kind of media exposure.

Privacy Law in the United States

Privacy law in the United States is a patchwork of federal and state statutes that have developed over time in response to changing needs and technologies. At the federal level, privacy law in the online space has largely been developed through the enforcement powers of the Federal Trade Commission (FTC), though there are some statutes in place targeting specific industries such as healthcare, education and financial services. Generally, with some exceptions, American privacy law is an "opt-out" system, allowing online service providers to define their own privacy practices provided they:

- Do what they say, and
- Honor customers' requests to opt-out of certain practices.

With the exception of the industries and situations detailed below, companies have a lot of flexibility as to what they can do with the information they collect from and about their customers, so long as they comply with their own privacy policies and do not deceive customers. By contrast, the privacy regimes in most other countries impose much tighter restrictions on what companies can do with data, and often require companies to obtain consent before collecting and using personally identifiable information. While foreign laws are beyond the scope of this guide, companies should be aware of the different privacy regimes abroad, especially if they plan to target or collect information from consumers outside the United States. At the very least, online service providers whose operations are entirely in the U.S. should notify users that their service is operated in accordance with U.S. privacy law, and all information collected from their customers around the world will be treated following U.S. privacy law.

THE FEDERAL TRADE COMMISSION

The Federal Trade Commission is a federal agency with broad powers to prohibit and prosecute "unfair or deceptive acts or practices in or affecting commerce." In a series of investigations targeting companies from HTC to Twitter, the FTC has taken the position that weak privacy and data security policies constitute unfair trade practices falling within its investigative and prosecutorial mandate. FTC prosecutions can lead to the imposition of significant financial penalties, but most are resolved by settlement agreements that combine a fine with a detailed set of steps a company must take to mend its ways. Facebook avoided an FTC fine in 2011 when it settled charges that its privacy policies were deceptive by agreeing to submit to biennial privacy audits for the next 20 years. Google, by contrast, had to agree to a $22.5 million penalty to settle FTC charges that it unfairly tracked the online activities of users of Apple's Safari web browser by circumventing the browser's privacy settings.

Exceptions to the General Rule

Healthcare Applications: Applications and online services that provide services to healthcare providers such as doctors, hospitals and healthcare insurance companies must comply with the Health Insurance Portability Act (HIPAA), which establishes privacy protection for medical records and other health data. Online service providers that aim to provide any type of services involving health information should confirm whether or not they are subject to HIPAA.

Applications for Education: Any online service providers serving schools, teachers, or other types of educational institutions should be aware of the Family Educational Rights and Privacy Act (FERPA), which is enforced by the Department of Education. FERPA applies directly to educational institutions receiving funding from the Department of Education, rather than to commercial service providers, but consequently, most educational institutions require online service providers that provide services to them or their students to be FERPA compliant. Furthermore, many states are imposing additional obligations directly onto online service providers that provide tools for education. To that end, online service providers working in the educational space should be aware of FERPA, regardless of what service they provide (e.g. infrastructure, learning games, teaching tools, etc.), as well as any state laws that may apply to them.

Applications for Children: Any online services or applications that collect information from children under the age of 13 are required to comply with the Children's Online Privacy Protection Act (COPPA). In particular, COPPA requires online service providers to obtain consent form a child's parent before collecting personally identifiable information from a child. Online services targeting children should be aware of COPPA and its requirements.

Credit Reporting and Background Check Services: Any organizations or services that create or provide consumer reports or otherwise furnish consumer information, such as credit reporting agencies, background check service providers, as well as organizations that use this information are subject to the Fair Credit Reporting Act (FCRA). Companies that provide consumers with credit reports or provide businesses with information about consumers, employees or other individuals should confirm whether or not they are subject to the FCRA. Likewise, organizations that automate certain types of checks through their online portals, such as employers or credit card companies may also be subject to FCRA requirements.

Financial Services: The Gramm-Leach-Bliley Act (GLBA) imposes heightened privacy obligations on financial institutions, which the statute defines as "companies that offer financial products or services to individuals, like loans, financial or investment advice or insurance." Online Service Providers intending to provide any type of financial service, or intending to collect financial information from individuals, should confirm whether or not they are subject to the GLBA.

State Laws

As noted above, many states have started to regulate privacy to fill gaps in the federal system. To that end, you should know which jurisdictions' laws apply to your company, and what the privacy laws are in those jurisdictions.

Establishing a Privacy Strategy

Given that privacy law in the United States is an uneven patchwork, it is important not only to understand how your company collects, stores and uses information, but also to come up with a data privacy philosophy that reflect and aligns with your business model. Beyond complying with the law, implementing a thoughtful, transparent, and integrated privacy regime can help your company instill trust in your customer base and avoid public relations fiascos. The following are some short-term and long-term strategies aimed to help companies protect the privacy of the information they collect through technological mechanisms and other means.

Short Term Steps and Strategies

Ensure Data Security Through Authentication and Accountability Systems

Companies should ensure that all sensitive data is shielded by at least one layer of authentication so that only authorized personnel, rather than everyone in the organization, can access such information. An authentication system should ideally log both successful and unsuccessful attempts to access user data in order to enhance accountability in the event of a breach.

Requiring employees to authenticate before accessing sensitive data may seem like obvious advice, but a surprising number of companies fail to take even this basic step. For example, an FTC complaint against Twitter alleges that between 2006 and 2009, the micro-blogging service "granted almost all of its employees the ability to exercise administrative control of the Twitter system, including the ability to: reset a user's account password, view a user's nonpublic tweets and other nonpublic user information, and send tweets on behalf of a user."

Companies must also carefully consider just how much data any given employee is allowed to access. As storage capacities grow by the day, a single misplaced laptop or flash drive could expose the sensitive personal information of tens of millions of customers. Providing employees with unlimited access to your company's data stores could also invite the kinds of massive leaks that have plagued the U.S. government in recent years—such as the Snowden revelations and the WikiLeaks incident. Limiting access to data by an employee's function is therefore not just common sense, but sound business sense, too.

Protect Privacy Through Encryption

To the extent that the law doesn't already require it, your company should protect any confidential or personally identifying data that has been entrusted to your care using the strongest available encryption methods.

As LinkedIn's experience shows, gone are the days when simply encrypting your data virtually guaranteed its security. Despite being encrypted using the SHA-1 hashing algorithm, it was a trivial task for hackers employing modern computers and sophisticated tools such as John the Ripper to decrypt more than two-thirds of the passwords stolen from LinkedIn in a matter of days. Your company can greatly reduce the risk that sensitive information will be exposed in a data breach by employing stronger encryption algorithms and other techniques such as "salting" passwords and multi-iteration encryption.

Many of the industry-specific privacy laws described above have long required the use of encryption to protect sensitive personal information. A growing number of states, led by Massachusetts, now also require companies to encrypt any personally identifiable data that comes into their possession. Since the legal standards governing when an online service providers is subject to a state's laws are notoriously complex, it's worth consulting a lawyer to ensure your compliance with all applicable state laws.

Conduct Audits to Certify your Data Security Practices

Consider hiring one of the growing number of information security auditing firms to review both your technological security safeguards and your internal procedures to prevent employees from leaking out sensitive information. Such firms can certify your compliance with various recognized security and privacy standards, thereby allowing your company to publicize your compliance on your website as a selling point for conscientious consumers. If you are concerned about the possibility of litigation, you might consider hiring a law firm to evaluate your security and privacy protections so that the findings of the review are protected by attorney-client privilege. If hiring an external auditor is cost prohibitive, it may be worth conducting periodic internal audits to ensure you are complying with your established privacy policies.

Long Term Steps and Strategies

Minimize the Scope of Personal Data Collection

As the big data revolution makes it cheaper and easier than ever to store, analyze, and leverage vast quantities of data, the temptation to collect and store as much data as possible can be overwhelming — particularly since customer data can be shared and sold for profit to advertisers, data brokers, and others who want to be in the know.

Storing vast quantities of data is not a cost-free proposition, however. Despite the proliferation of nominally free cloud storage solutions, one recent study finds that the average mid-sized American business spends $300,000 per year on data storage and security. More significant still are the costs your business will incur if any of that data ends up in the wrong hands. Between litigation expenses and compensation payments, the costs of dealing with a data breach averaged $194 per compromised record in 2011.

The potential benefits of keeping vast quantities of sensitive customer data on hand need to be balanced, therefore, against the risk that the information will be compromised and your company will be on the hook for damages and legal fees. One way companies can strike a better balance between the risks and rewards of storing customer data is to store only what they truly need, while discarding the rest to minimize the impact of a potential data breach. Before you store that data, here are some questions that responsible companies should ask themselves:

- Is this particular type of data a valuable business asset?
- How essential is the given data type is to the operation of our business?
- What are alternatives to collecting this specific type of data?
- What can I expect to pay to store and safeguard this data?
- How would users react to the accidental disclosure of this data?

Minimize the Length of Data Retention

Once you've decided that you really need to collect and store a particular kind of data, the next question is how long you should retain it. The answer to this question should always be *the shortest period permitted by law and consistent with your company's business needs.* Although the United States does not currently have any laws requiring Internet companies to store logs and other data for a minimum period, countries in other parts of the world—including in Europe—have such requirements.

Responsible companies generally develop formal data retention policies that specify how long they will hold onto the various kinds of data they collect beyond any applicable legal minimum. The process of developing a data retention policy itself can be very valuable, as it forces various internal stakeholders (from technical to legal to marketing) into a conversation about data retention that might not otherwise take place. Having a data retention policy in place also sends a signal to your customers that you take the security of their data very seriously.

If your company decides to retain data beyond any minimum period required by law, consider whether you can anonymize or delete certain fields or records to reduce the harm that would result from a data breach. You may not need to retain a customer's credit card information if you're storing old transaction data for analytical purposes, just as you may be able to delete customer name and street address information if you're retaining data to improve your product recommendation algorithm.

Consider Succession of Ownership

Just as every one of us should ideally have a will, companies need to think about what happens to the data stored on their servers beyond the company's lifespan as an independent entity. What happens to user data if your company is bought? How will users be able to get their data off your servers if your company goes quietly into the night? Who will take care of deleting user data from servers and other machines that might be auctioned

off in a bankruptcy proceeding? And most importantly of all, will the big players in your sector be interested in acquiring your company if you've paid no attention at all to user privacy and data security from the start? Having been chastened themselves following major privacy lapses and data breaches, some of the tech sector's larger companies may not be so willing to invest in or acquire your company if they're buying themselves a host of problems along with your technology.

Consider Privacy's Effect on Your Company's Image

As the public debate over online privacy continues to intensify, consumers are becoming more demanding and discerning when it comes to companies' privacy policies and security practices. The rise of online communities such as *Terms of Service; Didn't Read*, which aggregates user reviews of the privacy policies of popular websites, is one testament to this trend. So too is the fact that some companies are now mounting national media campaigns trumpeting how their privacy protections are better than their major competitors. Smart companies can therefore find a competitive advantage in adopting best-in-class privacy and security measures and in differentiating themselves from their competitors on this basis.

Action Items

- ❑ Draft and publish a privacy policy describing how you collect, store, use, and share information. Take into account your infrastructure, data flows and business needs when creating your policy to ensure you can comply with what you disclose to your customers.
- ❑ Draft a data retention policy that outlines what information you store and for how long. This policy should also include appropriate mechanisms for data deletion and destruction, as well as backup solutions and procedures.
- ❑ Create internal guidelines and an escalation processes to report and handle data and privacy breaches. Included in this process should be someone from the executive team, the chief technologist and internal or external legal counsel.
- ❑ Appoint a privacy officer who will be responsible for developing training materials on the company's privacy practices, will review products for compliance with privacy practices and ensuring compliance across the organization with the privacy policy and data retention policy.
- ❑ Periodically audit data flows, internal processes and technological infrastructure to ensure compliance with the privacy policy and data retention policy.

Resources

Statutes

- Health Insurance Portability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936
- Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§6501 - 6505
- Fair Credit Reporting Act, 15 U.S.C. § 1681
- Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338

Other References

- FTC, Cases and Proceedings, Twitter, Inc., *available at* http://www.ftc.gov/os/caselist/0923093/110311twittercmpt.pdf
- Nate Anderson, "How I became a password cracker," Ars Technica (March 24, 2013) *available at* http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/

- Symantec, State of Information Survey: SMB Results (2012), *available at* http://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-smb.en-us.pdf
- Ponemon Institute and IBM, 2015 Cost of Data Breach Study: Global Analysis, available at http://www-03.ibm.com/security/data-breach/
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006*, available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF