1

Secret Handshake Deals

January 18, 2012, has become famous in certain circles as the date of the "Internet blackout," the climax of the world's largest, most dramatic, and—arguably—most effective online protest to date. On January 18, web giants including Google, Wikipedia, Reddit, Tumblr, and Mozilla blacked out some or all of their web pages, as did thousands of smaller websites.

Over the course of several months leading up to that date, a transnational coalition of academics, technologists, civil-society activists, Internet users, and Internet companies came together to oppose Internet censorship and Draconian rules that they said would impede the functioning of the Internet. The protest focused on two intellectual property bills in the United States: the Stop Online Piracy Act (SOPA) in the U.S. House of Representatives and its sister bill in the U.S. Senate, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or Protect Intellectual Property Act (PIPA). These bills targeted websites (or "sites") globally accused of violating U.S. intellectual property laws, which govern the production and use of creative works like movies and music, as well as the commercial manufacture of goods. Such sites offer unauthorized downloads of copyrighted content, particularly movies music, games, or software, or sell counterfeit goods, which are unauthorized reproductions of trademarked products like those bearing the famous Nike "swoosh."

Protesters had reason to be concerned. SOPA and PIPA would have fundamentally altered online efforts to enforce intellectual property rights. The bills proposed requiring Internet intermediaries, which provide or facilitate Internet services, to police intellectual property rights. These intermediaries would be required to act as regulators with the goal of preventing the distribution of counterfeit or copyright-infringing goods on their platforms. Under the proposed bills, rights holders of intellectual property, like the sporting goods firm Nike, could seek court orders to require online payment providers, such as PayPal and Visa, and digital advertising firms like Google and Yahoo, to target sites distributing copyright-infringing content or counterfeit goods. These Internet firms would have been required to withdraw their services from targeted sites for the purpose of disrupting the sites' operations.

Critics of the bills argued—and not without reason—that they would extend punitive U.S.-style enforcement strategies globally. Under the bills, U.S.-based rights holders could have singled out sites worldwide that they claimed violated their intellectual property rights. Censorship was also a central concern. The bills could have endangered free expression on the Internet if actors inadvertently—or, more worryingly, deliberately—targeted legally operating sites and stifled legitimate speech. Moreover, critics claimed the bills could potentially damage Internet infrastructure through the types of technical enforcement measures proposed. SOPA and PIPA were explicitly designed to favor rights holders, particularly large institutional copyright owners in the movie and music industries, and multinational companies like Nike and Pfizer, at the expense of Internet firms that provide essential online services. Largely absent from SOPA and PIPA was any consideration of Internet users who rely upon the Internet to participate fully in economic, social, and cultural life. In articulating their concerns, SOPA protesters tapped into wider societal anxiety over state and corporate actors' power to determine what kinds of content we can access, share, and use, what we can buy and where, and how we can use Internet services, technologies, and platforms.

Until the Internet blackout, intellectual property was not thought of as a subject that triggered widespread public protests or generated heated debate in the mainstream media. In fact, it was generally considered to be an arcane, commercial matter of interest only to large corporations and lawyers (Haggart 2014). The groundbreaking protest against SOPA and PIPA changed that and transformed intellectual property into a topic of popular conversation. At the zenith of the protest,

on January 18, over a hundred thousand web pages went dark in protest and 10 million people signed petitions against the bills. So many people attempted to contact their elected representatives in the United States that the surge in traffic temporarily took down some U.S. senators' web pages (McCullagh 2012). Representative Darrell Issa, a Republican from California and a staunch opponent of the bills, described the protest as an "Internet mutiny" (Franzen 2012). Faced with an unprecedented public outcry over intellectual property bills, the U.S. Congress backed down and withdrew the bills on January 20, 2012. The protest was the first major political defeat for U.S. intellectual property proponents in over thirty years, a monumental achievement of Internet activism, particularly given the strong bipartisan support for the issue in the United States (Sell 2013). Opponents celebrated as the anti-Internet policies appeared dead, at least until the next attempt at legislation.

FROM CONTROVERSIAL BILLS TO HANDSHAKE DEALS

The anti-SOPA uprising and surprising defeat of SOPA and PIPA have been widely reported in academic and mainstream sources. Without doubt they will be the subjects of important studies of online activism and transnational social movements for years to come. What is less well known, however, is that the Internet blackout failed to kill the provisions contained with SOPA and PIPA. While protesters were campaigning against these bills, a small group of U.S. policy makers, rights holders supportive of SOPA and PIPA, and their trade associations were active behind the scenes. In closed-door meetings, they quietly drafted a series of informal, non-legally binding handshake agreements with Internet firms and online payment providers that incorporate some of SOPA's toughest and most controversial provisions, which were opposed by tens of millions of people in the United States and around the world.

The United States is not alone in creating non-legally binding agreements to regulate intellectual property on the Internet. The United States and the United Kingdom are the epicenters of these nonbinding agreements, as each has multiple agreements. Officials from the European Commission also crafted their own agreement. As happened in the United States, small groups of multinational corporations and officials from the U.K. government and European Commission conducted negotiations outside democratic, legislative processes, between 2010 and 2013.

Government policy makers describe these nonbinding agreements as "voluntary, industry-led initiatives" (Espinel 2013). Industry participants refer to them as "best practices." As these "best practices" are identified and determined by industry, however, they do not represent objectively evaluated measures. Negotiations occurred in closed-door meetings with little participation from consumer or civil-society groups, despite the fact that the agreements broadly affect how people can use popular—and indeed, essential—Internet services. Signatories are major U.S.-based Internet companies and payment providers with global operations: PayPal, Visa, and MasterCard, along with Google, Yahoo, Microsoft, and eBay.

One of the agreements' key targets is websites and marketplaces aimed at consumers in the United States and Europe but located elsewhere, especially China. For rights holders, China is of particular concern because it is the primary manufacturer of counterfeit goods that are exported to North America and Europe. Rights holders are also concerned with counterfeit goods sold through the China-based Taobao marketplace, which is the equivalent to eBay in China. U.S. and European rights holders not only want to combat the manufacture of counterfeit goods in China, but they also want to expand sales of legitimate versions of their brands in China's burgeoning e-shopping environment, particularly through key venues like Taobao.

At their core, the informal agreements are intended to push large Internet intermediaries to go beyond what they are required to do by law in the protection of intellectual property rights. Advocates of this position, including the European Commission, approvingly refer to it as a "beyond-compliance" regulatory strategy (European Commission 2013, 5–6).

The puzzle at the heart of this book is why powerful, globally dominant Internet firms and payment providers adopted non-legally binding agreements to police the online market in copyright-infringing and counterfeit goods on behalf of rights holders. At first glance, this type of regulation does not appear to be in intermediaries' material interests. Further, why did these intermediaries agree voluntarily to go beyond what they are required to do by law? The answer is governmental pressure. Despite government officials' use of the terms *voluntary* and *industry-led initiatives,* the agreements are neither voluntary nor wholly private. State actors—the U.S. and U.K. governments, along with the European Commission[1]—threatened the intermediaries with legislation and legal action to compel the companies to adopt non-legally binding enforcement measures. These state actors did so in response to lobbying

from prominent rights holders keen to expand the online enforcement of their intellectual property rights.

State pressure was necessary to encourage—and compel—intermediaries to exceed their legal responsibilities. This is because, while the intermediaries did not entirely oppose increased enforcement of intellectual property rights, they did not consider this problem to be primarily their responsibility. In addition, the intermediaries largely resisted rights holders' efforts to revamp their enforcement efforts. Intermediaries' adoption of the nonbinding agreements lessened their risk of being subject to legislation or legal action. However, intermediaries also had another motivation. State actors and intermediaries have some overlapping interests in exerting greater control on the Internet. Intermediaries want not only to expand their markets but also to influence state standard-setting in relation to issues important to them, such as data collection and storage policies and rules regarding privacy of users' personal information.

More broadly, this book explores the growing practice of states designating powerful corporate actors as global regulators to set and enforce rules on the Internet. This regulation increasingly occurs in the absence of any meaningful public or judicial oversight, through nonlegally binding arrangements. Such practices raise critical questions of fairness, due process, legitimacy, and the degree to which relying upon private-sector actors to deliver public-policy objectives is good for democracy. Core questions guiding my argument in this book are: what effects may informal corporate regulation have on how we access and use Internet services, applications, and technologies; and what are the associated problems?

New Global Regulators

A valuable and intriguing lens through which to examine the growing practice of informal regulatory practices carried out by corporate actors on the Internet is the regulation of intellectual property. *Regulation* in this context refers to the practice of nonstate organizations, including private companies and nongovernmental associations, setting and enforcing rules, standards, and policies that guide the provision of important Internet services, such as search or payment processing. The online regulation of intellectual property is an important case study because it is a key area of Internet governance, since it involves setting rules that govern the global flow of information and goods.

In terms of intellectual property, the two main areas I study are copyright law and trademark law. Copyright law lays out rules that determine how knowledge, and creative and artistic works like music, films, and books can be accessed, used, and shared, by whom, and with what technologies. Trademark law determines the entities that can lawfully manufacture, distribute, advertise, and sell trademarked products. Counterfeit goods are a form of trademark infringement. On the Internet, regulating trademarks entails making rules that determine how and on what platforms goods are sold, by whom, and in what ways, and how goods can be advertised. Rules governing intellectual property fundamentally affect what content people can access, and how they can access this content and exchange goods and services online.

Responsibility for policing those rules is increasingly falling upon Internet intermediaries that act, sometimes reluctantly, as gatekeepers on behalf of rights holders. Intermediaries are typically for-profit entities that provide important commercial and technical services that enable the effective functioning of the Internet. Some intermediaries, such as search engines or web hosts, facilitate access to or the hosting of information on the Internet. Others, such as social media platforms like Facebook and Twitter, or payment providers like PayPal, enable transactions or interactions among Internet users. Internet intermediaries vary widely in size, scope, and market share. Some intermediaries provide services across multiple sectors. Google, Yahoo, and Microsoft, for example, all operate search engines and digital advertising platforms. Certain intermediaries, such as Visa, MasterCard, and PayPal, can be used in both real-world and online environments. Other intermediaries, like domain registrars, exist solely online.

Large intermediaries like Google, eBay, and PayPal can be thought of as "macrointermediaries" owing to their global platforms, significant market share, and sophisticated enforcement capacities that protect their systems and users from wrongdoing like fraud or spam.[2] Macrointermediaries can set rules that govern hundreds of millions of people who use their services. They are in a powerful position to shape the provision of essential Internet services, such as search and payment processing, by virtue of their ability to monitor their platforms, remove unwanted content, and block suspicious transactions and behavior. Given their regulatory capacity, cooperative macrointermediaries can allow rights holders to police mass populations globally in ways that were previously unattainable, technologically unfeasible, or prohibitively expensive.

Why do rights holders want to work with macrointermediaries? These Internet firms act as chokepoints with the capacity to exert significant control over the access to and use of essential online sectors, including payment, advertising, search, marketplaces, and domain name services that enable users to access websites. People commonly—but mistakenly—understand the Internet to be a relatively ungoverned space, a "Wild West" of loosely connected networks that extend globally. Contributing to this perception are frequent claims by various governments and law enforcement agencies that they struggle to enforce laws on the Internet and are relatively powerless to reach outside their legal jurisdictions to target bad actors. Despite this Wild West stereotype, in many ways the Internet is a highly controlled environment. By withdrawing their services, macrointermediaries can disable sites' capacity to process payments, thereby "choking" sites' revenue streams. These intermediaries can also impede users' ability to locate and access counterfeit goods by controlling search and domain services and restricting the operation of marketplaces, thus creating access barriers. In essence, intermediaries use revenue and access chokepoints to deter unwanted behavior and target inappropriate content.

Given macrointermediaries' market dominance and global reach, they have a significant capacity to set rules governing hundreds of millions of people and determining how global flows of information are handled. Further, as these macrointermediaries police and sanction their users, remove certain types of content from their platforms, or withdraw their services from particular sites, they are shaping public policies in areas as diverse as privacy, data collection and retention, intermediary liability, intellectual property rights, and freedom of expression. As a result, through their roles as regulators, intermediaries are becoming de facto policy makers on an array of complex social issues, including obscenity, intellectual property rights, promotion of terrorism, and child pornography (DeNardis 2014). Internet firms' work as regulators or policy makers, however, may not be readily apparent to or fully understood by the general public. Internet users may not realize how intermediaries have changed rules relating to their services until users are unable to access certain information or use particular features. Intermediaries' global reach and sophisticated enforcement practices make them a valuable enforcement partner for rights holders and for states, as the Snowden files show in regard to the NSA's surveillance programs that siphon information from Google, Yahoo, and Microsoft.

Uncovering the Informal Agreements

This book is the first to map the creation and operation of nonbinding enforcement agreements as they pertain to the online control of counterfeit goods. Informal agreements provide an ideal regulatory solution for actors who favor increased protection for intellectual property rights online. As is discussed in chapter 2, non-legally binding measures enforced by intermediaries enable rights holders and government officials to sidestep failed bills in the United States, stalled legislation in the United Kingdom, and a series of lawsuits between intermediaries and rights holders in the United States and Europe. Away from the public eye, small groups of government and corporate actors had the freedom to negotiate enforcement measures that significantly expanded intermediaries' responsibilities for policing the online trade in counterfeit and copyright-infringing goods. The goal of the nonbinding agreements is compliance-plus enforcement, in which intermediaries exceed their legal responsibilities and undertake regulatory duties in the absence of legislation or court orders.

In this book I discuss eight informal agreements struck among Internet firms, government officials, and rights holders and their trade associations in the United States and the European Union. The agreements lay out broadly worded general principles to guide Internet firms' regulation of websites that distribute counterfeit goods and copyright-infringing content. Within these agreements, intermediaries participate from five Internet sectors: payment providers (e.g., PayPal); search and advertising intermediaries (e.g., Google); marketplaces (e.g., eBay); and domain name registrars (e.g., GoDaddy), which register domain names, the unique names given to sites, such as www.wikipedia.org. Each of these intermediaries acts as a revenue or access chokepoint, which is why rights holders pushed them to adopt the informal agreements. By partnering with the intermediaries, rights holders are able to strengthen their online enforcement of their intellectual property rights.

REGULATING INTELLECTUAL PROPERTY

My goal in this book is to illuminate often-opaque interdependencies between corporate-state regulatory practices on the Internet and the little-known practice of governing through chokepoints. Consequently, it is vital to appraise how these corporate-state regulatory efforts may affect the way we use Internet services and technologies and, more

broadly, the online environment as a whole. To understand why prominent industry actors and government officials are devoting significant attention to the illicit trade in counterfeit goods and copyright-infringing content, it is important to first appreciate what intellectual property rights are, as well as why certain companies and governments are keen to strengthen the online protection of copyrights and trademarks.

Intellectual property is an issue of significant economic and political importance. In the modern globalized economy, ownership of intellectual property rights is central to economic dominance. Economic benefits from intellectual property primarily flow to those who own these rights. Individuals and corporations in industrialized countries, particularly the United States but also countries in Europe, own the greatest proportion of intellectual property rights.[3] In the case of trademarks, this means that rights holders in the United States and Europe receive considerable revenue from the manufacture of products, even though the production of those goods increasingly takes place in lower-cost countries, particularly China (Dedrick, Kraemer, and Linden 2009). For example, a 2011 study of Apple's production of iPads reveals that manufacturers in China receive approximately ten dollars per iPad in direct labor wages, which amounts to 1.8 percent of the value of the iPad (Kraemer, Linden, and Dedrick 2011, 4).[4] Apple, in contrast, captures 58 percent of the value from the iPad because it owns the trademarks and patents (the latter refers to industrial methods or processes) involved in the manufacture and also keeps product design, software development, and product management in the United States (Kraemer, Linden, and Dedrick 2011, 2). Analyses of the value generated by intellectual property show that revenue disproportionately flows to the rights holders, and, by extension, to the rights holders' home countries. In the case of Apple's iPads, China receives only a sliver of the iPad's value for its manufacturing role, while the United States benefits from Apple's retention of high-value services in the United States.

This is why countries that benefit from strong intellectual property rights regimes, particularly the United States, aggressively seek ever-increasing standards of protection. The U.S. government, globally the strongest proponent of greater protection for intellectual property rights, uses bilateral and multilateral trade agreements to pursue its preferred policies on intellectual property worldwide (Drahos and Braithwaite 2002). Intellectual property is a core feature of international agreements like the Trans-Pacific Partnership Agreement (TPP). Negotiations for the TPP began in 2005 among multiple countries, including the United

States, Australia, Canada, Japan, and Malaysia, and concluded in 2015. The TPP has incited protests and heated debate in many countries because, among its provisions, it would institute strengthened enforcement provisions to protect intellectual property in ways that critics charge would grant too much power to corporations (Flynn et al. 2012).

As the next chapter discusses, the economic and political importance that the U.S. government and the European Union accord to the protection of intellectual property is the result of policy decisions dating back to the 1970s. At that time, prominent rights holders and their trade associations persuaded the U.S. government and other governments to adopt rules to protect intellectual property that would disproportionately favor both U.S. industries and rights holders in a handful of other industrialized countries (Sell 2003). The influence of prominent U.S. and European rights holders and their trade associations continues today. They lobby countries worldwide to toughen laws protecting intellectual property and increase enforcement against the infringement of intellectual property rights. They also pressure companies that they contend are involved in or facilitate infringement to adopt suitably tough (i.e., U.S.-style) enforcement policies and processes. Private enforcement agreements that target the online trade in counterfeit goods are the latest incarnation of efforts to ramp up enforcement activities.

Purpose of Trademarks

We all encounter hundreds of trademarks in the course of daily life, even if we do not consciously recognize them as such. Trademarks are the logos and symbols that adorn our clothing, vehicles, food, and beverages, and the signs on stores and restaurants. Trademarks can consist of words, letters, numerals, drawings, symbols, colors, audible sounds, fragrances, three-dimensional shapes, logos, pictures, or a combination of these or other characteristics (Ricketson 1994). Well-known trademarks are McDonald's golden arches, Nike's swoosh, and Toblerone's distinctive triangle-shaped chocolate bars.

Trademarks serve, or are supposed to serve, a dual purpose. First, they are intended to enable individuals or companies who develop and cultivate trademarks to protect their marks from misappropriation by others. Second, for consumers, trademarks are supposed to serve a public good, designed to assist consumers in identifying the commercial origin of goods (e.g., Apple). They are also intended to prevent the likelihood of confusion

among consumers by enabling individuals to differentiate among similar offerings in the marketplace (Ricketson 1994). Trademarks allow someone to distinguish Apple's iPhones from Samsung's Galaxy phones, or lesser-known brands' phones that may otherwise closely resemble these popular trademarked products. Consumers thus rely upon trademarks for information about products and as indicators of a product's quality or consistency. Trademarks promise, but do not legally guarantee, reliability or adherence to certain standards.

Trademarks owners typically register their trademarks with national intellectual property agencies, such as the U.S. Patent and Trademark Office, although registration of trademarks is not required in all jurisdictions. Internationally, trademark registration occurs through the Madrid System at the World Intellectual Property Organization (WIPO) in Geneva, Switzerland. WIPO, as an organization of the United Nations, is responsible for the administration of various international treaties pertaining to intellectual property.

The 1994 Agreement on Trade-Related Aspects of Intellectual Property (TRIPS), discussed in chapter 2, sets worldwide standards for the protection of trademarks. According to TRIPS, the owner of a registered trademark has the exclusive right to use that mark and prevent all others from using "identical or similar signs for goods or services which are identical or similar to those in respect of which the trademark is registered where such use would result in a likelihood of confusion" (art. 16.1). Limited exceptions to this exclusive right are permitted, such as the use of a competitor's trademark for comparison in advertising. Counterfeit goods are unauthorized reproductions of products or packaging that infringe a rights holder's registered trademark. TRIPS, which provides the main global framework for domestic trademark legislation, defines counterfeit goods as "any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation" (art. 51[a]).

Billion-Dollar Trademarks

Developing and protecting trademarks is a serious, multibillion-dollar business. This is because trademarks have no expiry date and can be renewed indefinitely, as long as they are in use. Therefore, unlike

copyrights and patents, which have limited terms of protection, trademarks can provide a potentially unending source of revenue. That trademarks can hold significant value explains rights holders' efforts to protect them from unauthorized use.

Trademarks are often considered synonymous with brands. Brands, however, are better understood as "the soul of a product" (Rothacher 2004, 2), embodied within a specific trademark. Marketers strategically shape trademarks into brands to cultivate value in the trademarks. Consumers may imbue brands with certain personality characteristics, whether real or perceived (de Chernatony, MacDonald, and Wallace 2011). When people see the distinctive Apple logo (Apple's trademark), for example, they may think of cutting-edge design with reliable operating systems (its brand). Consumers use brands to convey aspects of their personal identities to others, such as creativity or rebellion, or to signal their status through the consumption of luxury products. Purchasing a premium watch from the high-end Swiss company Blancpain, for instance, may imbue the wearer with a sense of urbane distinction because each watch is individually handcrafted.

Based upon the characteristics and sentiments attached to brands, certain brands can accumulate significant value. The brand-valuation firm Interbrand, for example, estimates Nike's brand at $23 billion, whereas the brand of France-based Louis Vuitton is valued at $22 billion and that of Germany-based Adidas is worth an estimated $7 billion (Interbrand 2015). Large Internet firms also possess lucrative brands. Google's brand is worth an estimated $120 billion, which is in second place among the top one hundred brands, just behind Apple at $170 billion (Interbrand 2015). Brands are intangible assets, so these figures are only estimates. The value ascribed to brands shifts over the years and also rises and falls with firms' fortunes and scandals. There are also variances among brand-valuation companies in their appraisals of brands. Nonetheless, these large figures indicate the importance of corporate brands and show that firms have considerable economic interest in protecting their trademarks.

The challenge for rights holders is that brand attachment is an intensely subjective process. Consumers develop strong preferences for one brand over another, even when there are few differences between products, and shift their loyalty among brands. For those who produce and sell counterfeit goods, their value is the trademark. Consumer surveys show that people may purchase some counterfeit goods as trial versions or as substitutes for genuine branded goods (Rutter and Bryce

2008). Individuals desire products with certain trademarks because of what that mark represents (Gentry 2001). People who desire a particular product may knowingly purchase a counterfeit version and find satisfaction because of the characteristics they associate with the brand. As a result, people may choose to consume a brand (e.g., Gucci) but not a specific product (e.g., authentic Gucci purse). Simply put, consumers may desire counterfeit goods because they are "counterfeits of some brand" that they desire (Gentry 2001, 264). Although this is not a problem for these consumers, companies that invest considerable resources to create and market brands they hope will inspire and maintain consumers' loyalty see it as a serious problem.

The actual harm caused by counterfeiting of such goods is not cut-and-dried. Counterfeited products indicate that the goods—and the associated brands—are popular. "The unfortunate part is: if your brand isn't being counterfeited, you're in more trouble," explains David Lipkus, an associate with the Toronto-based law firm Kestenberg, Siegal, and Lipkus (interview, Lipkus 2012). Given varying degrees of consumer support for counterfeit goods, rights holders acknowledge that they cannot entirely eliminate the problem. "The goal of a good enforcement program is not to let it [counterfeiting] overwhelm the brand," comments Roxanne Elings, former cochair of global trademarks/brand management practice, with the law firm Greenberg Traurig in New York City (interview, Elings 2012).

Why Care about Anticounterfeiting Efforts?

Why should we be interested in studying online regulation that occurs through non-legally binding agreements? It is important to understand the specific nature of online anticounterfeiting enforcement efforts. Studies of copyright infringement are contributing to a rapidly growing literature of interest to scholars, activists, and industry (see Haggart 2014). Trademark infringement, in contrast, is woefully underexamined (a notable exception is Raustiala and Sprigman 2012). This book's focus on counterfeit goods represents an effort to address the paucity of studies that examine how states or corporate actors regulate this issue.

A key reason to study anticounterfeiting efforts is that, as noted above, the harms typically associated with counterfeiting are not as clear-cut or substantial as industry officials typically portray. In fact, as discussed in the next section, it is difficult to calculate with any certainty the economic losses to rights holders from this problem, given the scarcity of

reliable data. Purchases of counterfeit products by willing consumers do not represent lost sales to rights holders, since those consumers may have never intended to buy authentic products. However, rights holders may argue that their brands are still damaged because the counterfeits may be of poor quality or harm the consumer in some way.

Anticounterfeiting rhetoric often equates "authenticity" (i.e., authorized branded goods) with quality and safety. Counterfeit goods may be shoddily constructed and pose safety risks, but so can genuine, legitimately trademarked goods. For example, the widely publicized scandal of food products containing traces of horsemeat in Great Britain in 2013 and the scare over melamine-contaminated food in China in 2008 respectively appear to be problems of supply-chain management and deliberate adulteration, not counterfeiting (Castle and Dalby 2013; Gillan 2008).

Not all counterfeits are poor imitations. Some counterfeits are perfect replicas that are virtually indistinguishable from genuine goods. This is why a test purchase—purchasing and testing a suspicious product—is generally the most accurate way to determine whether a product is counterfeit or not. There are "many criteria that help you assess whether it's likely to be a counterfeit," explains Jeremy Newman, a partner with Rouse Legal in London. "You'll never be sure until you see that physical sample" (interview, Newman 2012). Test purchases can be time-consuming and costly, because the products must be shipped from the seller to the examiner. Intermediaries generally only require rights holders to make a good-faith statement in relation to their complaint regarding counterfeit goods, not conduct test purchases. Test purchases are not a requirement within the nonbinding agreements. Without test purchases, however, which provide clear evidence of trademark violation, rights holders' may inaccurately identify genuine or secondhand goods as counterfeit.

Examining corporate regulation through non-legally binding agreements uncovers systemic problems with due process measures. The case studies in chapters 3 through 5 reveal serious problems with rights holders or intermediaries mistakenly targeting lawful behavior. Even if we spare little thought for the due process of merchants selling counterfeit goods, we should be concerned about law-abiding individuals and businesses who may be swept up in enforcement dragnets with little opportunity to appeal their cases. Regulatory efforts that emphasize speed and mass policing, especially through automated tools, are typically vulnerable to problems of false positives, as is the case with the nonbinding agreements.

Equally, this type of enforcement—using macrointermediaries to institute chokepoints in the absence of legislative or judicial requirements—raises serious questions about regulation on the Internet in general. Macrointermediary-facilitated regulation illustrates the capacity of private actors to set and enforce rules globally in ways that tend to benefit narrow corporate interests at the expense of the general public. As the practice of governing through chokepoints expands, there are no reasons why it cannot be adapted to other problems. This is an emerging governance practice that echoes the private, unaccountable nature of the national-security surveillance state. As such, it provides a preview of one possible future for governance, one that is unaccountable, open to abuse, and highly reliant on constant surveillance. It prompts us to ask: is this the type of future we want?

PROBLEM OF COUNTERFEIT GOODS

Most people have likely encountered or even purchased counterfeit goods at some point in their local flea markets, dodgy strip malls, or along Canal Street in New York City. Counterfeiting affects a broad range of goods from luxury clothing and accessories, especially sunglasses and purses, to cosmetics and perfume, food and alcohol, and personal care items like toothpaste and condoms. Companies interviewed for this book investigated cases of counterfeit clothing, hats, and sunglasses sold in open-air flea markets and outside concert venues. They discovered counterfeit beer and wine poured into bottles recycled from high-end manufacturers, and luxury perfume adulterated with animal urine to achieve a particular hue. Industrial products, such as commercial circuit breakers, vehicle brake pads, and pumps for mining operations may also be counterfeited. Counterfeit goods are manufactured in many countries. China, however, is the largest global producer of counterfeit goods. This should be unsurprising given that China also legitimately produces many of the world's best-known brands. Apple's iPhones and iPads, for instance, are manufactured at the Taiwanese-owned Foxconn Technology Group's factories in Shenzhen, China.

It is important to recognize that consumers may knowingly purchase counterfeit goods, as discussed earlier, a practice termed "nondeceptive counterfeiting," in order to benefit from lower prices. People may also unknowingly purchase counterfeit goods, a phenomenon termed "deceptive counterfeiting." Companies that are most publicly prominent in their anticounterfeiting efforts are typically those with sought-after brands in

the apparel and accessories sector, such as Louis Vuitton, Chanel, Gucci, Coach, Nike, and Adidas. These companies are motivated, at least in part, by consumer surveys that demonstrate that people who knowingly purchase counterfeit goods do not perceive counterfeit apparel and accessories as harmful. For example, a 2009 study that examined nearly four hundred reports of consumers' perceptions of counterfeit goods, and surveyed consumers in five countries, including the United Kingdom, found that consumers believe counterfeit apparel to be less harmful than counterfeit pharmaceuticals (Business Action to Stop Counterfeiting and Piracy 2009).

Framing Counterfeiting as a Serious Offense

Industry actors have been very successful in framing counterfeit goods as a serious economic issue and a criminal offense. Framing is a concept that explains how actors employ certain ideas to construct issues as "problems." Actors can use ideas and metaphors as discursive frames to present events or behavior in certain ways and suggest alternatives (see Odell and Sell 2006). Effective framing is vitally important. "One must convince people that one's arguments are good, one's institutional innovations necessary, and one's horror stories disturbing," says James Boyle (Boyle 2007, 18, quoted in Sell 2003, 3). As discussed earlier in this chapter, rights holders made intellectual property enforcement a priority for the U.S. government in the 1970s by strategically constructing an association between intellectual property and international trade. Proponents of tougher enforcement against online intellectual property infringement draw upon arguments they have successfully employed since the late 1970s: counterfeit goods cost jobs, threaten innovation, and endanger public health (Halbert 1997).

Counterfeiting undoubtedly causes economic losses to rights holders. As in the case of other illicit markets like drugs, however, there is a lack of reliable, detailed data on the size of the market for counterfeit goods, and few estimates of economic losses to rights holders. Industry and government officials often cite studies from the Organization for Economic Cooperation and Development that calculate economic losses related to counterfeit goods. In its most recent report, in 2016, the OECD estimated that the value of counterfeited and copyright-infringing goods moving through international trade was as much as $461 billion annually (Organization for Economic Cooperation and Development 2016). According to Business Action to Stop Counterfeiting

and Piracy, an organization created by the Paris-based International Chamber of Commerce, counterfeit and copyright-infringing goods internationally is estimated between $770 billion and $960 billion (Business Action to Stop Counterfeiting and Piracy 2009).

Industry actors use estimates of losses from counterfeit goods to advocate particular policies and enforcement responses and to legitimize such demands to governments. Critics, however, argue that these estimates are weakened by poor methodologies, a reliance on anecdotal information, and political self-interest from rights holders and industry associations (see, e.g., Staake, Thiesse, and Fleisch 2009). As with other illicit markets, efforts to generate reliable, comprehensive data on counterfeiting and any related negative effects are open to charges of bias, distortion, politicization, and fabrication (Andreas 2010).

Rights holders' emphasis on counterfeiting as a criminal act downplays any responsibility companies may bear for weaknesses or problems in their corporate processes. There is a common misconception among big companies with problems of counterfeited products "that there's some kind of boogeyman counterfeiter or evil empire. Nine times out of ten it's their own suppliers" (interview, lawyer, Hong Kong law firm, 2012). Vincent Volpi, CEO of the U.S. security firm PICA Corporation, explains that factories contracted to manufacture products for a rights holder may exceed their orders. "They're flooding your primary marketplace with the same products that you've designed and authorized," Volpi says, "That's a supply chain issue, because it's technically a counterfeit; but at the end of the day, what you have is unauthorized production" (interview, Volpi 2012).

The complexity of global supply chains and outsourcing production from the United States and Europe to China also creates vulnerabilities (Mackenzie 2010). At an Alibaba Group investor meeting in Hangzhou, China, in June 2016, the founder and executive chair, Jack Ma, pinpointed outsourcing as a contributing factor in counterfeiting. Ma stated that "fake products today are of better quality and better price than the real names" because they are manufactured in "exactly the same factories, [with] exactly the same raw materials but they do not use the names" (Dou 2016). Companies that use production brokers, especially in China, also face the risk of having unauthorized versions of their goods manufactured for sale in China or shipped to overseas markets. Production brokers help rights holders choose manufacturers, particularly in China, to produce their goods, and this involves distributing product designs and specifications to multiple factories to determine

which factory has the skills, equipment, and competitive bid. Volpi highlights the problems inherent in this outsourcing process:

> I'm using a production broker, and I'm giving my designs to a production broker with the idea that they are going to go out and shop my designs all over Asia-Pacific to try to get me the best quality for the least amount of price—then that sounds like a good deal, right? At the end of the day, what I've just done is I've just distributed all of my designs all over Asia-Pacific to companies that are capable of producing them—I'm only going to choose one . . . to actually produce. That means that if I've shopped 300 companies, 299 [others also] got my specs. I don't even know who those people are, because the broker's job is to shop those guys. (interview, Volpi 2012)

Counterfeiting is therefore a much more complex problem than the unauthorized production of trademarked goods. Rights holders should bear some responsibility for logistical and financial decisions that introduce vulnerabilities into their manufacturing and distribution processes and weaken their supply chains. The question, however, is how much responsibility rights holders should assume and how much other actors—Internet intermediaries and the state—should bear. In some cases, problems framed as "counterfeit goods" may be more accurately described as problems of parallel trade or contractual disputes between rights holders and manufacturers that could be addressed by changing how manufacturers conduct their business.[5] By framing these problems as a criminal offense (counterfeiting), not a contractual dispute, rights holders have a stronger case to petition for state assistance.

Rights holders tend to condemn all instances of counterfeit goods, but counterfeiting can serve a useful economic purpose since it points to consumer needs or desires in the marketplace. In fact, some companies use counterfeit versions of their products as a form of market research. Peter Vesterbacka, CEO of the Finnish firm Rovio, which owns the popular Angry Birds game, argued that counterfeit Angry Birds merchandise in China helped the company. At a conference in Beijing in 2011, Vesterbacka states, "Angry Birds is now the most copied brand in China, and we get a lot of inspiration from local producers. The way we look at it is: of course we want to sell the officially licensed, good quality products, but at the same time we have to be happy about the fact that the brand is so loved that it is the most copied brand in China" (Kidman 2011).

Alongside claims of economic losses, rights holders emphasize serious public health and safety risks posed by counterfeit goods. "I don't envy my colleagues in the copyright field because I think they have a bigger task of proving harm," remarks Ruth Orchard, head of the Anti-Counterfeiting

Group in England, a prominent trade association. "We can demonstrate harm—all sorts of harm—much more easily with concrete goods" (interview, Orchard 2012). Some counterfeit goods, such as medication, food, drink, and electrical goods, can cause harm if the goods malfunction, are substandard, or lack safety features. A U.S.-based manufacturer of commercial electrical components, including circuit breakers for apartment buildings, found counterfeit versions of its products for sale in China that violated safety standards (interview, Garner 2012).

Despite media coverage and anecdotal reports, there is little comprehensive data on the health and safety harms caused by counterfeit products. One reason is rights holders' reluctance to reveal their problems to their competitors and customers, fearing a loss of competitive advantage or decline in their brand's reputation. Another reason is that rights holders may consider data of counterfeit-related harms to be proprietary. For example, the U.S.-based Pharmaceutical Security Institute, a trade association representing the largest pharmaceutical companies, holds the most comprehensive data on counterfeit pharmaceuticals but does not release that information publicly (interview, Kubic 2012).

Rights holders may be motivated to associate all counterfeit goods with safety risks if they are trying to solicit assistance from government officials. Many counterfeit products, such as clothing and accessories, generally do not pose health and safety problems to consumers. The head of the nonprofit Electrical Safety Foundation International, in the state of Virginia, alluded to this slippage between harmful and nonharmful goods when he spoke about the risks from counterfeit electrical products: "You plug it in and it sets on fire. There's no gray area in that. That's the difference between what we're talking about and the Louis Vuitton handbag" (interview, Brenner 2012).

The idea that intellectual property infringement should be treated as a harmful crime can oversimplify certain inherently complex cases. What is often defined as a problem of "counterfeit pharmaceuticals," for example, can be much more complicated. Intellectual-property actors sometimes conflate issues of generic medication, counterfeit pharmaceuticals, parallel trade medication, and substandard medication.[6] For some of these issues, such as the sale of counterfeit and substandard medication, the public interest is obvious. People need to be protected from medication that may be contaminated or adulterated with dangerous substances. Similarly, medication that contains too little or too much of the active medical ingredients could lead to serious side effects, overdoses, or untreated health conditions. The presence of generic medication in a

marketplace may have a beneficial effect, by lowering drug costs on legitimate, licensed medication via increased competition. Such slippage among different issues can enable actors to portray a counterfeiting problem as larger or more serious than it is in reality. More broadly, the conflation of generic medication with counterfeit can decrease public—and government—trust in generic medication, which materially benefits the manufacturers of nongeneric pharmaceuticals.

Regulating Counterfeit Goods

Counterfeit goods must be physically manufactured and shipped from production sites to consumers. This is in contrast to copyright-infringing copies of movies or music, which can be digitally copied and illicitly downloaded from sources like the Pirate Bay or Kickass Torrents. Consequently, rights holders concerned about counterfeit versions of their products often have both real-world enforcement programs that address the manufacture of counterfeit goods in particular physical locations, and online programs targeting the advertisement and distribution of counterfeit goods using the Internet.

Real-world anticounterfeiting efforts can be legally complex, time-consuming, costly, and challenging. Government and local officials may be unwilling or incapable of providing assistance. In some areas corruption of local and state officials is a significant problem, and counterfeiting may provide benefits to the local economy through employment (Mertha 2007). Foreign production facilities, many based in China, can be difficult to locate and surprisingly resilient to raids, because there "are lots of small on-the-ground facilities" (interview, lawyer, Hong Kong law firm, 2012). When one factory is closed, workers may simply shift production to another site. In developing countries, the protection of foreign companies' trademark rights is often not a priority for law enforcement agencies, which understandably must focus on more serious offenses, like social unrest or terrorism. Even within industrialized countries, anticounterfeiting efforts can pose challenges. Enforcement efforts aimed at flea markets or discount outlets, for example, can be resource-intensive and ineffective, since sellers shift locations or rapidly replenish their stocks if counterfeits are seized.

Online anticounterfeiting efforts have two goals: to deter consumers from purchasing counterfeits on stand-alone websites and online marketplaces, and to interrupt the distribution and advertisement of counterfeit goods. Most Internet users have probably come across advertisements

for counterfeits or sites selling suspiciously cheap brand-name goods. Some products may be euphemistically described on sites or in marketplaces' sales listings as "replicas" or "lookalike" products. Many of these sites are obviously fraudulent, with spelling and grammatical errors or poor-quality web design. Other sites are carefully designed to replicate exactly the official sites of popular brands. These mirror sites are intended to deceive consumers who wish to purchase authentic products and believe the sites they visit to be genuine.

How significant is the online trade in counterfeit goods? As with efforts to quantify economic losses to rights holders from counterfeit goods, there is little reliable data. Enforcement actions by rights holders give some indication of the scale of the problem. Deckers Outdoor Corporation, owners of the famous Ugg brand of footwear, identified eleven thousand sites between 2007 and 2011 that sold counterfeit versions of its products (Outdoor Industry Association 2011). Similarly, in a series of U.S. court cases between 2008 and 2012, Coach, True Religion, and Tory Burch (based in the United States); Hermès and Chanel (France); and Gucci (Italy), companies selling high-end clothing and accessories, each identified hundreds of sites selling counterfeit versions of their products.

Alongside stand-alone sites, rights holders are also concerned about the sale of counterfeit goods through online marketplaces like eBay and the massive China-based Taobao. These marketplaces are important because they have hundreds of millions of users and are responsible for a significant volume of trade. It is difficult, however, to estimate the proportion of counterfeit goods flowing through legitimate marketplaces. Private security companies that monitor marketplaces on behalf of rights holders can identify thousands, or even tens of thousands of sales listings for counterfeit versions of popular brands, as I discuss in chapter 5.

Those in the business of policing copyright and trademark infringement refer to websites selling counterfeit goods as "infringing sites" or, more colorfully, "rogue sites." There is no commonly accepted definition for infringing sites. Many in the intellectual-property-protection industry define the term in a manner similar to the definition proposed in the Stop Online Piracy Act. SOPA's section 102 defines "foreign infringing sites" as sites or a "portion thereof" that are directed toward and used by individuals in the United States in which the site operator "is committing or facilitating the commission of criminal violations," including trafficking in counterfeit goods or services. SOPA's definition would have applied to sites selling counterfeit goods and those offering copyright-infringing content. The breadth of SOPA's definition alarmed critics, who argued

that a "portion thereof" could be interpreted to include sites that had only a small problem with infringement. This could include a site that offered for sale one counterfeit good among all its other, legitimate products. It could also include legitimate sites that had hyperlinks to sites that sell counterfeit or copyright-infringing goods. Fan sites for popular books, movies, or video games may sell branded clothing or memorabilia that violate rights holders' trademarks.

If SOPA had passed into law, its legal definition of infringing sites would have been subject to judicial interpretation and scrutiny. This process would have given critics and defendants a chance to raise objections. Legal rulings on SOPA would have shaped how the definition could have been used and to what types of situations the legislation should apply. In contrast, non-legally binding agreements provide no similar opportunity for scrutiny. For advocates of nonbinding enforcement agreements, the expansive nature of the term *infringing sites* is highly useful. It means that there is no defined threshold of criminality. As a result, regulators have the flexibility to target any sites that they believe are selling, distributing, or advertising counterfeit goods, even if only one item. For critics, however, this looseness is extremely problematic. Sites that, deliberately or unintentionally, sell a mixture of legitimate and infringing goods—or that are even accused of doing so—could be crippled commercially instead of given an opportunity to challenge the allegations or address any problems.

Despite these challenges, in this book I employ the term *infringing site* because it is commonly used. However, I do so with the proviso that such sites are designated as infringing based on allegations, not proof, of infringement by rights holders. In the informal agreements, macrointermediaries typically require only a statement of good faith from the rights holders, not any definitive proof of infringement. Enforcement is undertaken rapidly, often using automated tools, which can make it difficult for the accused to appeal the allegations, as is discussed in chapter 2.

Rise of the Macrointermediaries

Proponents of more policing by intermediaries contend that the online distribution of counterfeit goods is too large, complex, and difficult for rights holders to address alone. It is relatively simple for vendors of counterfeit goods to set up a website, name it something catchy like "www.Nikeoutletsale.com," and spam consumers with advertisements. Vendors may also open multiple seller accounts in online marketplaces

TABLE 1 MACROINTERMEDIARIES' ENFORCEMENT CAPABILITIES

Macrointermediary	Enforcement Action
PayPal, Visa, MasterCard, American Express	Withdraw payment processing
Google, Yahoo, Bing (Microsoft)	Withdraw advertising services
Google, Yahoo, Bing	Remove search results
GoDaddy	Withdraw and/or disrupt domain name services
eBay, Taobao	Remove sales listings

and sell their wares to unsuspecting customers or those looking for too-good-to-be-true deals. Laws prohibiting these activities are in place, but enforcement in the online environment is often complex, time-consuming, and difficult. Offenders can operate anonymously and shift among different legal jurisdictions. They can locate in countries infamous for their governments' reluctance or inability to address online offenses. Those wishing to evade the law can strategically choose web hosts or payment providers who may be unaware of or turn a blind eye to illicit activities. Site operators may also strategically move from one jurisdiction or service provider to another in response to enforcement pressure. Those involved in policing intellectual property online, commonly termed the "brand-protection industry," refer to this challenge as "whack a mole," in a reference to the popular arcade and carnival game. Bob Barchiesi, president of the International Anti-Counterfeiting Coalition, an influential trade association based in Washington, D.C., explains that rights holders would "take websites down and they'd pop right back up. Within twenty seconds, they'd knock a site down and it would pop back up with a number one or a dot, just something a little bit different [in the domain name]. It just wasn't doing anything. It didn't have any effect at all" (interview, Barchiesi 2012).

Rights holders argue that intermediaries are better placed and equipped to counter these problems. In this book, I focus on the following macrointermediaries, which are signatories to the informal enforcement agreements: PayPal, Visa, MasterCard, American Express, Google, Yahoo, Bing (Microsoft's search engine), eBay, and the domain registrar GoDaddy (see table 1). I also examine the Taobao marketplace, which primarily caters to consumers in China.

Macrointermediaries' regulatory capacity stems, in part, from "their positions at the nexus points between communications networks" (Murray 2011, 27). PayPal, Visa, MasterCard, and American Express

collectively dominate the online payment sector. If you want to buy something online, chances are you'll do so using their services. Google operates the world's largest search engine and largest digital advertising marketplace, distantly trailed by Yahoo and Microsoft. Many of the advertisements users see online are part of Google's advertising services. eBay runs one of the world's biggest online marketplaces, with country-specific platforms around the world, such as eBay.fr (France) and eBay.de (Germany). GoDaddy, as the world's largest domain name registrar, provides and registers domain names.

These Internet giants collectively comprise a "Big Tech" industry sector that ranks alongside the traditional corporate powerhouses of Big Oil, Big Banks, Big Pharma, and Big Tobacco. The companies are all headquartered in the United States, which indicates the considerable commercial influence of U.S. companies on the Internet. Given their operational scope and ability to facilitate access to important services and online spaces, these macrointermediaries have regulatory capacity similar to or even exceeding that of state-based regulators (Murray 2011).

Terms-of-Service Agreements

Informal enforcement agreements with macrointermediaries offer rights holders a useful opportunity to shift some of their enforcement burden to Internet firms and payment providers. More importantly, these agreements allow rights holders to undertake global enforcement campaigns in a manner that previously would have been unfeasible or prohibitively expensive. With their vast, global platforms and technologically sophisticated surveillance and enforcement capabilities, macrointermediaries can conduct mass policing of Internet networks, platforms, and services. By working with PayPal, for instance, rights holders can target sites offering counterfeit goods worldwide that use PayPal to process customers' payments.

Intermediaries set and enforce rules that govern their platforms through their terms-of-use contracts with their users. Terms-of-service or terms-of-use contracts are ubiquitous online. We click to agree to these legal contracts, often without reading or understanding the contracts, whenever we sign up to Twitter or LinkedIn, update iTunes agreements, or open a PayPal or eBay account. These agreements enable companies to determine how their users can access and share certain content, what items users can purchase, methods of payment, and the personal information users must divulge. Through these agreements,

intermediaries may collect personal information, including users' names, mail and email addresses, phone numbers, and payment details. Intermediaries may also collect information relating to the individuals' use of the service, such as web browsing histories, email history, and payment transactions.

These contractual agreements also outline users' obligations and their responsibility to adhere to specific terms in exchange for intermediaries' services. The agreements incorporate laws from countries in which the Internet firms operate, such as laws that prohibit fraud, the distribution of child pornography, and the sale of counterfeit goods. They also incorporate policies that relate to the protection of the intermediaries' intellectual property rights and that of third parties. Intermediaries have significant latitude in deeming certain types of content and activities as appropriate or inappropriate for their services through their terms-of-use contracts. They can also penalize users who violate their policies. Facebook, for instance, formerly had a real-name policy that required people to use names that corresponded to government-issued identification. Although Facebook has recently relaxed this policy somewhat to allow non-government-issued identification, such as library cards, the social network has frozen the accounts of people found in violation of this policy. Facebook's real-name policy has angered those, including transgender people, drag performers, and victims of domestic violence, who often do not use names that match official government identification (Holpuch 2015).

Intermediaries can respond to problematic content or behavior on their platforms in several ways. Depending on the type of services they offer, intermediaries can remove or block problematic information, or they can sanction their users who violate their policies. Web hosts and social networks can remove videos, images, advertisements, and text that the intermediaries decide is inappropriate for their platforms. Search intermediaries can remove search engine results that hyperlink to specific web pages, a process referred to as de-indexing. Intermediaries that provide payment, advertising, social media, web hosting, or domain name services can restrict or limit services to individuals who violate their policies.

PRIVATE TRANSNATIONAL REGIMES

To explain the emergence and operation of the nonbinding agreements, it is necessary to account for all the players involved and trace their

varying interests in addressing the online trade in counterfeit goods. The coalition of elite corporate actors—multinational rights holders, influential trade associations, and commercially prominent U.S.-based Internet firms—and government officials constitutes a loosely structured transnational private regulatory regime. Regimes can be understood as encompassing "the full set of actors, institutions, norms and rules" involved in a particular regulatory arrangement (Eberlein and Grande 2005, 91).

The concept of a private regime, borrowed from nonstate governance theory within the international relations discipline, provides a useful framework to explain particular state-corporate regulatory dynamics that produced the non-legally binding agreements. Stephen Krasner, along with other international relations scholars, developed the concept of regimes to account for the influence of nonstate actors in global governance. Krasner's classic definition of regimes refers to "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge" (Krasner 1982, 185). Scholars of nonstate governance, particularly Claire Cutler, Deborah Avant, Virginia Haufler, Thomas Biersteker, and Rodney Bruce Hall, have further expanded the definition of regimes to explain nonstate actors' capacity to set and enforce rules transnationally (see particularly Avant, Finnemore, and Sell 2010; Cutler, Haufler, and Porter 1999).

Roles of State and Corporate Actors

Regimes recognize state and nonstate actors, especially corporations, who may play varied roles in designing, implementing, and enforcing particular rules and standards. The concept also explicitly recognizes the capacity of nonstate actors to make and enforce rules, particularly through soft law measures, such as nonbinding codes of conduct or industry-derived best practices. Regimes are thus useful to trace the specific historical and sociocultural context from which actors emerged to form particular regulatory arrangements. They can help uncover and explain, for example, the long history of U.S. rights holders and trade associations in shaping intellectual property policy making in the United States and internationally (Drahos and Braithwaite 2002; Sell 2003). By employing the concept of regimes, one can also account for similarities and differences among actors' material and ideational interests in relation to the governance of a particular issue. Actors may have conflicting, sometimes irreconcilable differences that shape the composition

and function of governance arrangements. Regulatory efforts that materially benefit one party may impose costs on the other.

Because government officials are central actors in this private regime, it is important to understand the role of the state. To do so, I have adopted in this book the concept of a "regulatory state" (Braithwaite 2005). Central to this idea is the fact that the state deploys power "through a regulatory framework rather than through the monopolisation of violence or the provision of welfare" (Walby 1999, 123, quoted in Braithwaite 2005, 11). States have shifted, since the 1980s, from providing regulation through the production and enforcement of rules to shaping the provision of regulation by nonstate actors (Jordana and Levi-Faur 2004). This means that states may govern through regulation by shaping discourse and distributing resources to nonstate actors in order to direct regulatory efforts (Rhodes 2012). States may strategically confer authority on civil-society or corporate actors, thus empowering those actors to create or enforce regulatory frameworks (Levi-Faur 2013). Governments, for example, may delegate authority to civil-society organizations to enforce animal welfare legislation, or permit corporations to use self-regulatory programs to monitor their adherence to environmental laws. Although states vary in their capacity and interest in governing, the concept of a regulatory state does not indicate a hollowing out of state authority. States retain the capacity to endorse, influence, or reject regulatory frameworks put forth by nonstate actors (Büthe 2010).

States determine which actors are more authoritative, lend legitimacy to some interests over others, and privilege certain policies (Hall 1993, 288). Not all interest groups, of course, have equal resources with which to persuade states to support their regulatory preferences or command the same degree of influence in shaping policy making processes. In the private anticounterfeiting regime, public advocacy groups are sidelined. Rights holders and their industry associations have an institutional advantage over intermediaries through decades of lobbying for strengthened protection of intellectual property (Sell 2010). Despite rights holders' history of successful lobbying, it is important to emphasize that states retain distinct interests and goals.

Private Enforcement Agreements

Regimes may be defined as transnational according to the scope of the rule-setting actors, the level of the rule-setting institutions, the scope of

the rules themselves, or a combination of these factors (Mügge 2006, 179). The private anticounterfeiting regime is transnational because of the global scope of the intermediaries involved and their capacity to impose rules on their users through their terms-of-use policies. Regardless of its scope, a regime may also have roots within a specific territorial base or embody distinctly local features (Graz and Nölke 2008, 10). These local roots may infuse a regime with characteristics that shape its character or operation. Prominent rule-making actors, for example, may all be based within the Global North, creating rules that govern activities in the Global South.

The nonbinding agreements have a distinctive Global North-South arrangement. Actors set rules and standards in the United States and Europe and then export them to shape standard-setting practices in other countries worldwide through intermediaries' global operations, especially in China. Three of the agreements were created in the United States, two in the United Kingdom, one in China, and one covers Europe. Intermediaries participating in the agreements include Google, Microsoft (Bing), Visa, PayPal, MasterCard, GoDaddy, Yahoo, eBay, American Express, and Taobao.

Government officials from the United States, the United Kingdom, and the European Commission employed various methods to compel macrointermediaries to adopt the agreements, including threats of legal action and legislation. These government officials did so in response to lobbying from prominent U.S. and European rights holders and their powerful trade associations like the Motion Picture Association of America and the International Anti-Counterfeiting Coalition. These trade bodies have a well-documented history of influencing public-policy making in the United States and internationally, as is discussed in chapter 2. Rights holders involved in the private agreements are large, well-known companies with multiple, valuable trademarks, including Adidas, Nike, Burberry, Louis Vuitton, Nokia, and the consumer care companies Proctor & Gamble and Unilever. The public, in contrast, was largely sidelined.

Enforcement of intellectual property rights online is not solely the job of intermediaries. A whole industry has arisen to support it. The brand-protection industry provides enforcement services to rights holders and intermediaries and can be understood as a service provider to members of the transnational anticounterfeiting regime. This industry, which is part of the global private security industry, emerged in the 1980s with the outsourcing of manufacturing from industrialized countries to those in Asia, particularly China. Brand-protection services

rapidly expanded with the growth of the Internet and rights holders' fears of online infringement in the beginning of the twenty-first century. These firms are part of the "high policing" component of the private security industry that specializes in corporate security and investigative work (see Brodeur 2007). They operate globally on behalf of corporate clients and mostly serve clients from the Global North (see O'Reilly 2011). This is in contrast to "low-policing" actors who perform front-line private security duties, which includes guarding specific spaces like malls or airports, or certain populations, such as prisoners. Brand-protection companies offer a variety of surveillance and enforcement services to rights holders, including automated monitoring and enforcement tools to police the online sale of counterfeit goods, which is explored in chapter 5.

There are important commonalities among these agreements. Each contains broadly worded general principles that lay out minimum requirements to guide intermediaries' practices in the enforcement of intellectual property rights. There are common enforcement strategies. Intermediaries are responsible for removing advertisements or search results for counterfeit goods to make it more difficult for consumers to find and access vendors selling counterfeit goods. Intermediaries also agree to withdraw important commercial and business services from sites involved in selling or advertising counterfeit goods. Payment providers, for instance, terminate their services to targeted sites, thus commercially disabling sites.

The regime functions because of common interests among corporate and state actors. Rights holders and intermediaries have financial and reputational interests in protecting their intellectual property from infringement and in maintaining the confidence of their users by cracking down on any association with criminality. Collaboration with rights holders and trade associations on non-legally binding enforcement measures may offer intermediaries greater flexibility and less onerous conditions than legislation or court-imposed requirements. More broadly, actors in the regime have shared interests, although sometimes differing goals, in expanding their control over the Internet, particularly by governing online flows of information and behavior.

CHOKEPOINTS: TECHNICAL POINTS OF CONTROL

Technology is a key component of the transnational anticounterfeiting regime. Rights holders, their trade associations, and private security

companies use technology to monitor sites and marketplaces for the sale of counterfeit goods and to send complaints to intermediaries, These intermediaries, in turn, use technologically sophisticated enforcement programs to remove problematic content or withdraw their services from targeted sites. By withdrawing their services, intermediaries create technological chokepoints that deter consumers from accessing targeted sites and hamper the sites' functioning. The use of the terms *throttle* and *chokepoint* by actors who are intent on strengthening enforcement practices explicitly underlines the punitive nature of withdrawing critical services. This strategy assumes that intermediaries, who often rely upon allegations from rights holders, can surgically disable specific sites without negatively affecting other related sites and services. A common problem, however, is the wrongful removal of lawful content by rights holders or intermediaries.

To understand how intermediaries use technology to target suspicious behavior or content, techno-regulation provides a useful framework. *Techno-regulation* refers to the use of technology as a regulatory instrument to shape human behavior (Brownsword 2004). The concept has roots in science and technology studies, a field of research prominently associated with Bruno Latour (2005). Science, technology, and society are understood as mutually dependent upon and shaping one another. Technology is both real and constructed: its design and use are imbued with norms, concepts, and cultural values that in turn influence people's behavior, beliefs, and practices (Franklin 1995).

The use of new technologies is shaped by existing laws and regulations, as well as by state and nonstate actors promoting certain policy goals (Mueller, Kuehn, and Santoso 2012, 350). In addition, there are actors—individuals, states, companies, and other organizations—with material stakes in the development and use of technologies in certain directions (DeNardis 2014). In other words, with techno-regulation, "one can see technology structuring the politics, and politics constraining and channeling the technology" (Bendrath and Mueller 2011, 1156). Macrointermediaries appear to be ideally suited to regulate a wide variety of activities, since they have specialized technical skills and a global enforcement reach. Intermediaries, however, are not "natural" gatekeepers. People created these companies to provide Internet services, not to control the flow of information or transactions across their platforms on behalf of state or corporate actors. Intermediaries became regulators for intellectual property in response to considerable pressure from states and industry groups. Further, as the rest of the book shows,

government officials and rights holders have repeatedly demanded that intermediaries make specific technological changes to their enforcement programs to target and address online infringement.

The recognition that the built environment—and technology generally—is designed in ways to shape and constrain how individuals use these spaces is not new. There is a long history, for example, of improving street lighting or altering traffic flows to reduce crime (e.g., Clarke 1997). Digital architecture, too, can shape and manipulate how people access and use technologies. In the context of the Internet, legal scholars Lawrence Lessig and Joel Reidenberg famously refer to rules designed into digital architecture as "code" (Lessig 1999; Reidenberg 1998).[7] *Code* here refers to rules designed in software that control the various systems, tools, and protocols that compose the architecture of the Internet (Lessig 1999). In other words, code may function as law, since these rules can—in some circumstances—have the force of law. Whoever "controls the underlying 'pipeworks' and the protocols controls the Internet" (Guadamuz 2011, 87).

Automated Regulation

One way of thinking about code-based regulation is to consider how algorithms have changed regulation. *Automated regulation,* sometimes called *algorithmic regulation,* refers to the use of software algorithms to shape or affect human behavior (see O'Reilly 2013). Algorithms are sets of rules that influence our lives in many ways. Financial agencies and insurance companies use algorithms to rate and rank our credit worthiness and health risks, while Amazon suggests books we may like, and Google decides the search results we see. The development of computational systems enables regulators—both state and corporate—to regulate via the use of "big data," which can be understood as "the capacity to search, aggregate and cross-reference large data sets" (boyd and Crawford 2012, 663). Algorithms enable data to be "systematically extracted or disclosed, analyzed," and, ultimately, translated into "actionable data" (Lyon 2014, 3) for use by state or corporate regulators.

Thus, state or nonstate actors could introduce rules or standards into the code of software applications that would shape—or even prevent—certain types of online activities or behavior. For example, following a consumer backlash against Microsoft, in June 2013 the company removed restrictions that required gamers, even when playing offline games, to connect to the Internet daily for Microsoft to authenticate

their gaming systems (Stuart 2013). As a result of the outcry, Microsoft now allows players to play games offline, as well as to share games with friends.

Automated regulation is increasingly commonplace in the regulation of intellectual property on the Internet. Major Internet intermediaries, some rights holders, and a growing number of private security firms in the brand-protection industry use automated tools to detect and address online infringement. These actors may employ fully automated programs or use a combination of automated measures and human analysts. For example, intermediaries may employ automated monitoring programs to detect suspicious transactions or behavior on their platforms and may then require human analysts to review those instances and impose penalties if necessary. In fully automated systems, rights holders can use automated tools to detect infringement and then send a notification of complaint to the relevant intermediary. In turn, those intermediaries may employ automated programs to remove problematic content or withdraw services from targeted websites. Criminologist Pat O'Malley, in his analysis of automated traffic enforcement, such as cameras linked to traffic stoplights, describes this process as one in which individuals can be "policed, judged and sanctioned" through their "electronic trace" without any human interaction (O'Malley 2010, 795).

Because they effectively regulate what we can and cannot do, rules embedded in technology can raise serious questions relating to their legitimacy and accountability, and to whether they supersede or conflict with actual laws and regulations. Code-based regulation can operate opaquely, in ways unobservable to those who may be regulated. Those who design and implement certain rules may refuse to allow them to be openly inspected and challenged, and people may be unaware of the rules regulating their behavior. Equally troubling, in some contexts rules drafted by corporate actors may displace—or supersede—public laws (Lessig 1999). In terms of opaque state control, governments may require that firms incorporate particular rules within technology, allowing them to govern indirectly, bypassing constitutional or legal controls on state power (see Lessig 1999).

Automated regulation enables states and corporations to take action in response to wrongdoing. It also enables regulators to identify wrongdoing before it occurs, in what is often called "pre-crime." This means that regulators employ algorithms to "predict and intervene *before* behaviors, events, and processes are set in train" (Lyon 2014, 4). Intermediaries have sophisticated enforcement programs in place to detect

possible violations of their policies, such as fraudulent transactions intended to cheat an intermediary or its users of funds. Rights holders want intermediaries to target people who are perceived as being at high risk of copyright or trademark infringement because of patterns of previously suspicious behavior. An important element of techno-regulation, therefore, is examining how technology may constrain or prohibit certain types of behavior, thereby forcing people to comply with the rules and removing individual choice (see Brownsword 2011).

Those who design and deploy automated regulatory processes often portray them as operating objectively, accurately, and in a highly targeted manner. But because humans design this software, "their biases and values are embedded into the software's instructions" (Citron 2008, 1249). Simply put, algorithms are pieces of code, and code reflects the biases, prejudices, and assumptions held by the person who wrote the code. Advertising algorithms, for example, have shown advertisements for high-income jobs to men more often than to women (Datta, Tschantz, and Datta 2015). These rules are also often opaque to those they regulate. Companies designing or using regulatory algorithms often hide them in "black boxes" composed of "laws of secrecy and technologies of obfuscation" (Pasquale 2015, 9) by claiming that they are protected trade secrets. Secretly drafted, opaquely implemented rules pose clear challenges in terms of the legitimacy and accountability of regulation. As a result, we must ask: who do algorithms serve, and to what end?

METHODOLOGY

The regulation of intellectual property rights is a rapidly evolving topic, particularly in regard to the Internet. This book focuses on the period from roughly 2009 until late 2013, when small groups of government and industry actors created a series of nonbinding enforcement agreements aimed at sites that distribute copyright-infringing or counterfeit goods. The book focuses on eight agreements that cover multiple Internet sectors: payment, advertising, search, the marketplace, and the domain name system.

Much of the book focuses on the epicenter of the transnational anticounterfeiting regime: multiple agreements negotiated by U.S. and U.K. government officials. The book also examines U.S. rights holders' successful effort to institute an informal agreement with the Taobao marketplace, a platform of particular concern to U.S. and European rights

holders. In addition, the book discusses an informal agreement negotiated by the European Commission relating to marketplaces, including eBay, which is the first of its kind in the world. Each of these nonbinding agreements represents an important element of the transnational private regime.

The book draws upon ninety semistructured interviews with rights holders, trade associations, Internet firms, policy makers, attorneys, investigative firms, and civil-society groups in the United States, the United Kingdom, Canada, and Australia. Most interviews were undertaken in Washington, D.C., New York City, and London. Initial interviews to gain a detailed understanding of anticounterfeiting enforcement and to identify the main players, trends, and issues in the field were undertaken in my former home base of Australia. Interview subjects were selected for their direct experience in creating or implementing the private agreements and involvement in carrying out online anticounterfeiting enforcement programs. Questions were adjusted in line with the subject's expertise and nature of involvement in anticounterfeiting efforts. Rights holders were selected from a wide range of industries—namely, pharmaceuticals, apparel and accessories, sporting goods, commercial electrical components, and consumer electronics. This diversity facilitated an examination of online regulatory measures targeting counterfeit goods across industry sectors. The interviews were a mixture of in-person, telephone, email, and Skype interviews depending on the participant's availability and preferences. Most agreed to participate in for-attribution interviews, although some interviewees asked that their comments not to be attributed to them.

In addition to conducting these interviews, I attended a three-day industry conference hosted by the International Anti-Counterfeiting Coalition in Washington, D.C., in 2012, which focused on anticounterfeiting enforcement strategies, and which proved invaluable as a window into the state's role in private agreements. The book also draws upon primary government and legal documents relating to the negotiation and creation of the nonbinding enforcement agreements. This includes testimony before government committees, strategic plans to regulate intellectual property, and debates over intellectual property bills. The book also employs information from corporate annual reports, new releases, and blogs, as well as material from trade associations and civil-society groups. This information was supplemented with media sources, particularly from blogs focusing on technology and intellectual property.

BOOK OVERVIEW

The rest of the book is divided into six chapters. Chapter 2 provides the historical and political contexts in which the private agreements emerged. It briefly traces the growing influence of multinational rights holders on the U.S. government's intellectual property policy making processes from the late 1970s to 2012. The chapter then examines in detail four U.S. intellectual property bills, including the unpopular Stop Online Piracy Act, which proposed to reshape fundamentally the online regulation of intellectual property rights infringement. When these bills failed, rights holders redoubled their efforts to establish non-legally binding agreements with Internet firms that incorporated many of the bills' toughest provisions.

Chapters 3 through 5 present the book's case studies and examine how the informal agreements aim to regulate through three types of chokepoint: revenue, access, and marketplace chokepoints. These agreements have received little attention in academic studies or popular media. Chapter 3 focuses on payment (PayPal, Visa, and MasterCard) and advertising intermediaries (Google, Yahoo, and Bing), while chapter 4 examines search intermediaries (especially Google) and domain name registrars (specifically GoDaddy). Chapter 5 then examines enforcement efforts by marketplaces (eBay and Taobao). Drawing upon these case studies, chapter 6 considers the interactions, interdependencies, and overlapping interests among corporate and state actors in the regulation of online infringement.

The book concludes in chapter 7 by exploring ways in which states and corporations can use technology to regulate users online in ways that are fair, proportionate, and accountable, and which adhere to broadly accepted good governance practices. In that chapter, I recommend that Internet firms use industry transparency reports to be more open about their regulatory actions. The chapter ends with a call to strengthen digital rights.