INSIDE THE MINDS

Understanding Developments in Cyberspace Law

Leading Lawyers on Analyzing Recent Trends, Case Laws, and Legal Strategies Affecting the Internet Landscape

2012 EDITION

ASPATORE

Piracy, Privacy, and Internet Openness: The Changing Face of Cyberspace Law

Timothy J. Toohey
Partner
Snell & Wilmer L.L.P.

ASPATORE

Introduction

In the past few years, cyberspace law has emerged from the sidelines to much greater prominence. Despite the fact that cyberspace law is now more than fifteen years old, it has rarely attracted public attention in the same way as tort reform, campaign contribution law, or civil rights. Few in the general public are aware of the law relating to "takedown notices," the liability of Internet service providers (ISPs), or trademark infringement claims based on Google "ad words."

Complicating matters is that cyberspace law is not only a relatively technical field, but is also not always easy to locate. It is not embodied in any one legal code, but is instead scattered over many state and federal laws. For example, the provisions of the Digital Millennium Copyright Act (DMCA) are largely found in Title 17 of the US Code pertaining to copyrights, but also in some provisions in the criminal and patent codes. The Anti-cybersquatting Consumer Protection Act (ACPA) falls within Title 15 of the US Code pertaining to commerce and trade, and Section 230 immunity for computer services falls, somewhat quaintly, within Title 47 of the code for "Telegraphs, Telephone and Radiotelegraphs."

Unlike patents and copyrights, cyberspace law is, of course, not mentioned in the US Constitution. Nor is it entitled to its own title of the US Code, as is trademark law, the postal service, or railroads. Perhaps even more to the point, at least for the proponents of an "open" Internet, who decry attempts to control or harness the Internet, cyberspace law continues to have an uneasy, occasionally contentious, relationship with other legal principles, particularly intellectual property law. Moreover, the major players in the Internet, including search engine operators, social media companies, traditional content providers, and users, have divergent and often diametrically opposed views regarding existing and proposed laws in the cyberspace realm.

Piracy and Internet Openness: The Battle over SOPA

Cyberspace law may be said to have emerged from its relative obscurity into the full glare of the public gaze in late 2011 and 2012, when the battle over

the Stop Online Piracy Act (SOPA) [1] proposed in the House of Representatives and its Senate counterpart the PROTECT IP Act (PIPA) [2] erupted into the headlines. The debate revealed the strong differences between those seeking to protect property endangered by Internet piracy and unauthorized downloading of files and proponents of an open Internet existing beyond the control of national laws, including US copyright law.

Much digital ink has been spilled over the debate, but it is nonetheless worthwhile to outline the views of the proponents and opponents of SOPA to highlight countervailing trends that are likely to impact cyberspace law for the foreseeable future.

SOPA and PIPA were legislative responses to the call by media companies, particularly the motion picture and recording industries, for increased legal powers to stop online piracy, particularly that conducted by foreign "rogue" websites and "cyberlockers," i.e., online facilities for the storage of digital files. Through their trade associations, the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA), the industries claimed that legal protections for intellectual property rights, particularly copyrights, needed to be substantially bolstered to cut off infringements through streaming and downloading content from foreign websites.

One of the rallying points for SOPA's proponents was loss of US jobs. For example, the MPAA, in a statement to Congress in support of PIPA, stated:

> [i]t is not an overstatement to say that, the rampant theft of IP [through "rogue" websites facilitating downloading of copyrighted works] strikes at the heart our nation's economy, our core values of reward for innovation and hard work, and our ability to compete globally. In short, Internet theft puts at risk one of America's great export industries. [3]

[1] Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011-12).
[2] PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act), S. 968, 112th Cong. (2011-12).
[3] *Targeting Websites Dedicated to Stealing American Intellectual Property, hearing before the US Senate Committee on the Judiciary,* 112th Cong. (Feb. 16, 2011) (statement of the Motion Picture Association of America Inc.), *http://www.mpaa.org//Resources/94af6e2e-8dfd-48b8-9994-4aa2d11e709e.pdf* (last visited Apr. 2, 2012).

Similarly, the RIAA urged passage of SOPA because of the "toll that music theft takes on the enormous cast of industry players working behind the scenes to bring music to your ears," citing a "credible study" that "pegs the annual harm at $12.5 billion dollars in losses to the U.S. economy as well as more than 70,000 lost jobs and $2 billion in lost wages to American workers." [4]

The proponents of the legislation further claimed that existing provisions, including copyright laws, were inadequate to prevent infringements by foreign websites and that US courts should be allowed not only to bar advertisers and payment facilities from conducting business with infringing websites, but also to order ISPs not to provide links to infringing sites. [5] In a statement to Congress in support of SOPA, MPAA Senior Executive Vice President Michael P. O'Leary claimed that existing measures, such as the DMCA, were inadequate because rogue websites ignored takedown traffic in stolen content" and "when they are based overseas, they can simply thumb their noses at U.S. law." [6]

Mr. Leary further stated:

> [a]s technology has advanced since enactment of these provisions (providing for criminal liability for copyright infringement), however, so too have the means of willful and commercially destructive infringement. Increasingly, copyrighted content is not only made available for unauthorized downloading, but now is frequently streamed illegally, as well. But our laws have not caught up with the thieves, and as a result, uncertainty remains whether unauthorized Internet streaming of copyrighted works can be prosecuted as a felony, as other forms of piracy are.

---

[4] *Who Music Theft Hurts*, http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_online (last visited Apr. 2, 2012).

[5] *See* Cong. Research Serv., Summary of HR 3261 (SOPA), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03261:@@@D&summ2=m&.

[6] *Hearing on H.R. 3261, the "Stop Online Piracy Act" before the US House of Representatives Committee on the Judiciary*, 112th Cong. (Nov. 16, 2011) (statement of Michael P. O'Leary, senior executive vice president, Global Policy and External Affairs, on behalf of the Motion Picture Association of America Inc.), http://www.mpaa.org/resources/3307b183-575b-487b-9427-5630e10b27f0.pdf (last visited Apr. 2, 2012).

> SOPA closes that loophole in our nation's intellectual property laws. In so doing, it eliminates an unjustified, technology-specific disparity between forms of infringement that have increasingly similar commercially destructive impacts. [7]

SOPA's opponents—which included Internet companies, such as Google; websites, such as Wikipedia; commentators and bloggers, such as Techdirt; and organizations, such as the Electronic Frontier Foundation (EFF)—were against passage of the law because they saw it as contrary to principles of Internet openness and freedom of expression. They were generally most critical of the provisions of the bill that would have allowed ISPs to block allegedly infringing websites.

In its first review of the legislation titled *SOPA: Hollywood Finally Gets A Chance to Break the Internet*, the EFF argued that SOPA would promote vigilantism, "chok[e] off" legitimate with illegitimate sites, and strangle at birth the "YouTubes of tomorrow that are generating jobs today." [8] According to the EFF, "Hollywood is tired of those pesky laws that help protect innovation, economic growth, and creativity rather than outmoded business models. So they are trying to rewrite the rules, regulate the Internet, and damn the consequences for the rest of us." [9]

SOPA's opponents attacked not only the provisions of the proposed legislation and the necessity for the law, but also the fundamental premise that Hollywood's intellectual property (IP) should be protected against innovation and change. For example, the blog *Techdirt*, which helped spearhead the early opposition to the measure, disputed the assertion that illegal downloading of copyrighted materials was akin to theft, countering that copyright was a "government granted monopoly privilege over information." [10] *Techdirt* also denied that protection of copyright was

---

[7] *Id.*

[8] Corynne McSherry, *SOPA:Hollywood Finally Gets a Chance to Break the Internet* (Oct. 28, 2011), *https://www.eff.org/deeplinks/2011/10/sopa-hollywood-finally-gets-chance-break-Internet* (last visited Apr. 2, 2012).

[9] *Id.*

[10] Mike Masnick, *RIAA Totally Out Of Touch: Lashes Out At Google, Wikipedia And Everyone Who Protested SOPA/PIPA* (Feb. 8, 2012), *http:// www.techdirt.com/articles/*

important to the Internet, claiming that "[a] strong system of content protection has had nothing to do with the current success of the 'flourishing Internet marketplace.'" [11]

Others commentators, including Professor Laurence Tribe of Harvard University Law School, argued that SOPA violated the First Amendment's prohibition against prior restraints "because it delegates to a private party the power to suppress speech without prior notice and a judicial hearing." [12] SOPA's vague definition of websites "dedicated to the theft of U.S. property" would "effectively require sites actively to police themselves to ensure that infringement does not occur," which was expressly not required by the DMCA, and "would undo the statutory framework that has created the foundation for many web-based businesses." [13] Professor Tribe further argued that because of its "pervasive uncertainties," SOPA would inevitably chill "fully protected and lawful speech" by Internet sites "for fear that they will be accused of a SOPA violation and suffer a cutoff of revenue from online advertising or credit card payments for transactions." [14] Moreover, "[t]he threat of such a cutoff would deter Internet companies from adopting innovative approaches to hosting and linking to third party content and from exploring new kinds of communication." [15]

Although SOPA was opposed from the start by many Internet commentators and scholars, the general public was largely unaware of the proposed measure until the January 18, 2012, Internet "blackout." On that day, Wikipedia and an estimated 115,000 websites [16] replaced their normal

---

20120208/01453517694/riaa-totally-out-touch-lashes-out-google-wikipedia-everyone-who-protested-sopapipa.shtml.

[11] *Id.*, quoting Chris Dodd statement to Atlanta Press Club.

[12] Laurence H. Tribe, *The "Stop Online Piracy Act" (SOPA) Violates the First Amendment*, http://www.net-coalition.com/wp-content/uploads/2011/08/tribe-legis-memo-on-SOPA-12-6-11-1.pdf (last visited Apr. 2, 2012).

[13] *Id*.

[14] *Id*.

[15] *Id.*

[16] Jenna Wortham, *Public Outcry over Privacy Bills Began as Grassroots Grumbling*, NY TIMES (Jan. 19, 2012), *http://www.nytimes.com/2012/01/20/technology/public-outcry-over-antipiracy-bills-began-as-grass-roots-grumbling.html?pagewanted=1&ref=technology* (citing statement by nonprofit Fight by the Future, which helped organize the protests, that 115,000 websites participated in the protests and 3 million individuals e-mailed Congress to protest the bills).

home pages with materials describing their opposition to SOPA. For example, Wikipedia replaced its normal home page with a page headed "Imagine a World Without Free Knowledge" which stated:

> For over a decade, we have spent millions of hours building the largest encyclopedia in human history. Right now, the U.S. Congress is considering legislation that could fatally damage the free and open Internet. For 24 hours, to raise awareness, we are blacking out Wikipedia. *Learn more.* [17]

SOPA's proponents were quick to decry the blackouts as an abuse of power by the Internet. MPAA Chief Executive former Senator Chris Dodd accused the Internet sites participating in the blackout of engaging in a "stunt" and a "gimmick." [18] In an article in the *New York Times*, RIAA head Cary Sherman charged SOPA's opponents of engaging in "misinformation," in making a false attempt "to evoke images of crackdowns on pro-democracy Web sites by China or Iran" and of "present[ing] information that is not only not neutral but affirmatively incomplete and misleading [in attempt to] dup[e] their users into accepting as truth what are merely self-serving political declarations." [19] He also stated that SOPA was justified because there was a "constitutional (and economic) imperative to protect American property from theft." [20]

When the dust settled, an estimated 14 million individuals had written Congress regarding SOPA. [21] Although both SOPA and PIPA were tabled

---

[17] File:History Wikipedia English SOPA 2012 Blackout, http://en.wikipedia.org/wiki/File:History_Wikipedia_English_SOPA_2012_Blackout2.jpg.

[18] Statement by Senator Chris Dodd, chairman and chief executive officer (CEO) of the Motion Picture Association of America Inc. on the so-called Blackout Day protesting anti-piracy legislation (Jan 17, 2012), http://www.mpaa.org/resources/c4c3712a-7b9f-4be8-bd70-25527d5dfad8.pdf.

[19] Cary H. Sherman, *What Wikipedia Will Not Tell You*, NY TIMES (Feb. 8, 2012), http://www.nytimes.com/2012/02/08/opinion/what-wikipedia-wont-tell-you.html.

[20] *Id.*

[21] Jonathan Weisman, *After an On-line Firestorm, Congress Shelves Anti-Piracy Bills*, NY TIMES (Jan. 20, 2012), http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html (noting that shortly after "blackout day," Congress shelved both SOPA and PIPA).

after these protests, the bills' proponents vowed to find a way forward for anti-piracy legislation. [22]

The Implications of the SOPA Battle for Cyberspace Law

The dispute over SOPA reveals two major trends affecting cyberspace law that have important implications for practitioners and clients.

The first trend, espoused by SOPA's supporters, is that the capacity of the Internet for harm, particularly to established IP rights, must be restrained. Although proponents of this view recognize the virtues of the Internet and may indeed profit from it commercially, they believe protecting property and consumers against harm, such as unauthorized file-sharing and streaming of protected content, is a high economic and even moral priority.

The second trend, which is exemplified by SOPA's opponents, is that the open and free elements of the Internet must be preserved from those who would control, censor, or otherwise limit the flow of information inherent in its unique structure and architecture.

Although the concerns of SOPA's proponents are relatively easily understood by many lawyers and clients because they rest on familiar principles protecting intellectual property, the underlying basis of the positions taken by the proponents of openness is sometimes less well appreciated. Despite the fact that some like Chris Dodd of the MPAA may view the opponents of SOPA as pranksters engaging in a "stunt," a closer analysis of the views of the anti-SOPA camp indicates that their opposition to restrictions on Internet "openness" may well be a force that will affect future cyberspace law developments . [23]

Many who opposed SOPA believe that the Internet is not just another new technology, like the telephone or television, but a fundamental departure from the past. In their view, the Internet, unlike past technology, has created through its open and decentralized architecture a means to transform not only communication, but also knowledge itself. For example, Professor Tim Wu of Columbia University Law School has written that the

[22] *Id.*
[23] *Supra* notes 18 and 19.

Internet and its design, "like all design," is "ideology embodied" and that the essence of this design is openness and an antagonism to centralized control. [24] Born in the 1980s as a type of "secret club," the Internet, in Wu's view "clearly bore the stamp of the opposition to bigness characteristic of the era." [25] Because of its origins and architecture, the battle over the Internet reflects the "perennial ideological struggle" between the "concepts of the open system and the closed, between the forces of centralized order and those of dispersed variety." [26]

In Wu's estimation, the future will "be decided by one of two visions." One is the "utopia" of the "openness movement" of the Internet and companies such as Google. This is a "world in which most goods and services are free or practically free, thereby liberating the individual to pursue self-expression and self-actualization as an activity of primary importance." [27] The other vision is the dystopia of the "centralizers—AT&T, Hollywood, and Apple"—which will be "informed by a marriage of twenty-first century technology and twentieth-century integrated corporate structure. The best content from Hollywood and New York and the telephone and networking power of AT&T will converge on Apple's appliances, which respond instantly to ever more various human desires.[28] The centralizers seek to eliminate the "worst of the Internet"—"the spam, the faulty apps, the junky amateur content." *Id.* In contrast, the "champions of openness propose an untidier world of less polish, less perfection, but with more choice." [29]

Wu's analysis of the "open" Internet is not unique. As the critiques of EFF, *Techdirt*, and others indicate, many who opposed SOPA held strong views that the open architecture of the Internet was threatened by the chilling effect of Internet "censorship." Although many will dismiss these views as either exaggerated or self-serving, they will likely influence future Internet battles, particularly because the holders of these views were emboldened by the battle over SOPA.

A SOPA Footnote: The Megaupload Takedown

[24] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* 201 (2011).
[25] *Id.*
[26] *Id* at 289.
[27] *Id.* at 296.
[28] *Id.*
[29] *Id.* at 297.

On January 19, 2012—the day after Internet blackout day—the Department of Justice seized the site of a major cyberlocker, Megaupload.com, and brought a criminal indictment against Megaupload and its principals, including its colorful founder "Kim Dotcom," accusing them of criminal copyright infringement, racketeering, and other crimes. The takedown of this site provided fodder for those on all sides of the debate over SOPA. [30]

Those who believed that existing law is adequate pointed to the fact that the Department of Justice was able to seize the site under existing legal procedures. Those who believed current laws are inadequate pointed out that the Department of Justice had jurisdiction only because Megaupload had servers in Virginia and that other cyberlockers may not be susceptible to similar government takedown efforts. [31] Finally, those who feel that existing law imposes excessive controls on the Internet pointed to the fact that the seizure of Megaupload harmed innocent parties who housed legitimate content on the site. [32] As of this writing, the fate of the users' files on the Megaupload site is uncertain, with the MPAA calling for the data to be retained for potential copyright infringement lawsuits against Megaupload. [33]

The Challenges of Privacy to Cyberspace Law

Although privacy can be seen as reflecting many of the same trends in cyberspace law that were seen in the debate over SOPA, including both Internet control and openness, it presents particular challenges because of

---

[30] Tony Bradley, *MegaUpload Takedown Proves SOPA and PIPA are Unnecessary,* PC WORLD (Jan. 20, 2012), http://www.pcworld.com/businesscenter/article/248469/megaupload_takedown_proves_sopa_and_pipa_are_unnecessary.html.

[31] Andrew Chow, *Megaupload Shutdown May Help SOPA's Supporters and Critics,* Technologist: The Findlaw Technology Blog (Jan. 20, 2012), http://blogs.findlaw.com/technologist/2012/01/megaupload-shutdown-may-help-sopas-supporters-critics-alike.html.

[32] Mike Masnick, *Megaupload Details Raise Significant Concerns About What DOJ Considers Evidence Of Criminal Behavior,* TECHDIRT (Jan. 20, 2012), http://www.techdirt.com/articles/20120119/13052817473/doj-gives-its-opinion-sopa-unilaterally-shutting-down-foreign-rogue-site-megaupload-without-sopapipa.shtml.

[33] David Kravets, *MPAA Wants Megaupload User Data Retained for Lawsuits,* WIRED (Mar. 21, 2012), http://www.wired.com/threatlevel/2012/03/mpaa-megaupload-user-litigatio/.

consumers' views and expectations regarding privacy. In the privacy arena, Internet openness may be viewed quite differently, depending on whether one is looking at the flow of data from the point of view of a search engine, advertiser, or social network, or that of an individual user. Because users have divergent—and sometimes contradictory—views regarding privacy and because those views are receiving increasing government attention, privacy will continue to present challenges in cyberspace law.

There is little dispute that the Internet allows for the wide and sometimes uncontrolled dispersal of what in the past would have been private information regarding individuals. Personal information that normally would have been known only to a few intimate friends can now be easily located on a social networking site accessed by millions. Other information about individuals, including data regarding political contributions, house valuation, education, children, current and former addresses, and telephone numbers that previously would have required considerable effort to obtain, is now only a click away on a data aggregator or broker site.

Although many, if not most, Internet users are willing to provide personal information online for certain purposes, such as sharing with family or friends, research indicates that users have concerns regarding the use of such information for other purposes. For example, a recent Pew Research Center study indicates that 59 percent of the individuals surveyed "see the business practice of targeting ads based on data collected from users of email, search or social networking sites as an unjustified use of private information." [34] More than half (52 percent) of users of social network sites agree with this view, as do 64 percent of people over fifty years of age, 59 percent of those thirty to forty-nine years old, and 47 percent of those aged eighteen to twenty-nine. [35] These statistics are remarkable when one considers that consumers are expressing discomfort with the advertisements that are the economic lifeblood of many Internet sites, including Facebook. Nonetheless, the same survey shows that only 45 percent of those surveyed believed the government should do more to

[34] *Auto Bailout Now Backed, Stimulus Divisive,* Pew Research Center for the People & the Press, 17 (Feb. 23, 2012) (chapter on Privacy and Government Regulation), http://www.people-press.org/2012/02/23/auto-bailout-now-backed-stimulus-divisive/?src=prc-headline.
[35] *Id.*

regulate Internet privacy, and 49 percent did not want the government to get more involved. [36]

The conflicting views of Internet users, who are willing to provide private information, and fearful that it will be misused, may rest on a concern regarding control over personal information. As a researcher regarding the uses of social media in daily life has observed, "[users] feel as though control has been taken away from them or when they lack the control they need to do the right thing, they scream privacy foul." [37] However, even when users believe that a "privacy foul" has occurred on the Internet, they may have little redress, given the lack of a national US privacy law and the difficulty of demonstrating standing or damages under existing laws.

US Privacy Law: Limitations and Potential Changes

Unlike the European Union and other countries, including Canada, the United States has no comprehensive privacy law. Instead of comprehensive laws, the United States has adopted a "sectoral" approach that affords privacy protection for certain types of data, including health care, financial, and credit information, in certain specific contexts, including online transactions directed to children under the age of thirteen. Although the Federal Trade Commission (FTC) has the power to bring enforcement actions against businesses that do not adhere to privacy or data security policies under its authority to stop unfair and deceptive practices (e.g., using data for purposes different from those for which it was collected), these provisions do not provide a baseline privacy standard. [38]

The lack of national legislation regarding online privacy and conflicting consumer views create complexities for both Internet companies and the public. Although the self-regulatory framework that currently exists in many

---

[36] *Id.*

[37] Danah Boyd, *Making Sense of Privacy and Publicity* (Mar. 13, 2010), http://www.danah.org/papers/talks/2010/SXSW2010.html.

[38] *See, e.g.*, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Federal Trade Commission A-3 – A-8 (FTC Privacy Milestones) (March 2012), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 5-9 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

industry sectors frees companies from government regulation, it does not free them from lawsuits when perceived privacy violations occur. On the other hand, even where consumers perceive that their privacy has been violated, they may have considerable difficulty in establishing standing or damages under existing laws.

An example of the challenges of the current legal landscape is the recent decision in the Facebook privacy litigation case. [39] In the Facebook litigation, plaintiffs brought a class action against the social networking site alleging injury from transmittal by Facebook of personal information to third-party advertisers without the individuals' consent. As alleged in the complaint, plaintiffs claimed that when they clicked on an advertisement on the Facebook website, Facebook sent a "referrer header" to the advertiser that revealed the user's web page address used prior to clicking on the advertisement. This in turned caused transmittal to the advertiser of additional user information, including the user's name, gender, and picture, without the user's consent and "in violation of [Facebook's] own policies" to the injury of plaintiffs. [40]

Facebook prevailed on a motion to dismiss the case, largely because the court found that plaintiffs could not fit their allegations into any existing state or federal statutory framework. For example, the court found that plaintiffs did not state a claim under the Electronic Communications Privacy Act (Wiretap Act), 18 U.S.C. §§ 2510 *et seq*., because they had voluntarily communicated personal information to Facebook, which meant that Facebook could not be liable under the Wiretap Act for divulging the information to a third party. [41] Moreover, if the communication were considered as one directly from a Facebook user to an advertiser, the advertiser was the intended recipient, which again meant there was no violation of the Wiretap Act. [42]

Plaintiffs were equally unsuccessful in alleging claims against Facebook under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq*., which requires a plaintiff to have "suffered injury in fact and ... [to have] lost money or property as a result of the unfair

[39] *Facebook Privacy Litigation*, 791 F. Supp. 2d 705 (N.D.Cal. 2012).
[40] *Id.* at 709.
[41] *Id.* at 712-13.
[42] *Id.*

competition." [43] Because Facebook users do not pay fees to use the services, their personal information is not "property" under the UCL, and they were not entitled to redress under that statute. In contrast, the court noted that the users who sued AOL in a recent case for posting a database containing search records for more than 658,000 AOL users, lost "'highly-sensitive financial information' [such] as credit card numbers, social security numbers, financial account numbers, and passwords which was 'not something that members bargained for when they signed up and *paid fees for* [the defendant's] services." [44] The court concluded that the personal information of consumers was not equivalent to money or property, and they could therefore not state a claim under the UCL. [45]

The dismissal of the claims in *Facebook* is noteworthy, not because the plaintiffs' claims have (or did not have) merit, but because the existing legal framework for claims for misuse of private information does not comport with the views of a substantial portion of the public, who feel that such misuse violates their privacy. Many, however, would argue that a Facebook user who voluntarily provides private information to a free website is not entitled to redress when that information is used for a purpose other than the original one for which it was given, even if others indeed see this as a "privacy foul."

United States v. Jones: Changing Expectations of Privacy

Although the law, as yet, does not provide redress for many perceived privacy violations, attitudes may be changing in some prominent quarters. A recent Supreme Court case involving the right to be free of unreasonable government searches and seizures provides insight into how at least two justices of the Court view privacy in an era of changing technology.

In *Jones,* the Supreme Court held that a warrantless use of a GPS device attached to a car violated the Fourth Amendment prohibition against unreasonable searches and seizures. [46] The majority opinion in *Jones,*

[43] *Id.* at 714.
[44] *Id.* at 714-15, quoting *Doe 1 v. AOL LLC,* 719 F. Supp. 2d 1102, 1113 (N.D. Cal. 2010) (emphasis in original).
[45] *Id.* at 715.
[46] 132 S. Ct. at 950-51.

authored by Justice Scalia, affirmed the Court of Appeal's reversal of Jones's conviction on the grounds that the government violated the Fourth Amendment by physically trespassing on Jones's constitutionally protected area (i.e., his car) to obtain information. *Id.* The Court thus found it unnecessary to determine whether the government's placing of a GPS device in Jones's vehicle violated his "reasonable expectation of privacy" under *Katz v. United States*, 389 U.S. 347, 351 (1967). [47]

Justices Sotomayor and Alito wrote separate concurrences addressing the question left open by the majority—i.e., whether Jones's reasonable expectations of privacy were violated by the attachment of the GPS device. In considering this question, both justices noted that expectations of privacy are changing because of the use of technology. For example, Justice Sotomayor stated:

> *it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties*. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; and the books, groceries, and medi-service providers; and the books, groceries, and medications they purchase to online retailers. [48]

In his separate concurrence, Justice Alito acknowledged that public attitudes toward privacy have changed in our digital era, noting that "the*Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of

[47] *Id.*
[48] *Id.* at 957 (emphasis added).

privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[49]

The observations of Justices Sotomayor and Alito, who are not noted for seeing eye-to-eye, have significant implications for privacy law in the cyberspace field. Justice Sotomayor's observation that individuals may both reveal information about themselves and have an expectation of privacy is not only consistent with the views of many Internet users, but may presage a changing approach to privacy concerns. Although the "right to privacy" in the United States had its origins in the concept of the "right to be left alone" posited by Louis Brandeis and Samuel Warren in their famous law review article, that formulation may not be sufficient for the twenty-first century, where privacy is as much a social value as a personal one.[50] Similarly, Justice Alito's recognition that privacy expectations and "popular attitudes" are affected by technological changes taps into a current that may well affect both privacy and cyberspace law in the upcoming years. Although the day has not yet dawned when these theories can be translated into private rights of action, as evidenced by the *Facebook* decision, the fact that two Supreme Court justices from different ideological camps have formulated concurring opinions highlighting this issue is certainly worthy of note.

Toward National Privacy Legislation: The Challenge of Internet "Openness"

An additional reason privacy is a challenging issue for cyberspace law is that it is contrary in some ways to the values of openness and free expression on which the Internet was built—a view that also found its way into the opposition to SOPA. For many, the free flow of data is the essence of the Internet, particularly as it allows individuals to interact in new ways through social networking sites. The belief in openness has led some in the social networking world to make statements regarding privacy that strike some as either tone-deaf or self-serving. For example, Facebook's founder, Mark Zuckerberg, has claimed that privacy is no longer a social norm in the era of

[49] *Id.* at 962.
[50] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)*; see also* Daniel J. Solove, *Understanding Privacy* 91-93 (2010).

social media and instantaneous access through mobile devices. [51] Similarly, Reid Hoffman, the founder of LinkedIn, has stated that "all these concerns about privacy tend to be old people issues." [52]
Even if most proponents of Internet openness would not formulate the issue in these terms, they most likely would agree with George Pappachen, the chief privacy officer of the Kantar Group, who stated in opposition to "Do Not Track" technology that "[o]ur position is data should flow." [53]

The debate over privacy, however, is unlike that over SOPA because Internet users have (or are at least more willing to express) much more of an interest in protecting their personal information than in downloading copyrighted files. Conversely, those in favor of a free and open Internet are willing at least to consider self-regulation in the interest of satisfying consumers.

It is possible that the privacy debate may finally be entering a new stage and that momentum is building to enact some sort of national privacy legislation. For example, the highly publicized FTC settlements with Google and Facebook raised the profile for privacy on the national level by focusing on two of the most prominent Internet giants. [54] Moreover, the European Union's proposal for a comprehensive new data protection regulation in January 2012 highlighted the lack of similar laws in the United States. In the United States, proposals by the Obama administration and the FTC have called on Congress to enact national "baseline" privacy legislation, and some in Congress have welcomed those proposals.

The White House and FTC proposals are noteworthy because they both tread relatively carefully by encouraging both self-regulation and legislation. Additionally, both proposals put the burden on Internet companies to use

---

[51] Bobbie Johnson, *Privacy no longer a social norm, says Facebook founder*, THE GUARDIAN (Jan. 10, 2010), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.
[52] *Privacy is for old people says LinkedIn founder* (Jan. 27, 2010), http://www.youtube.com/watch?v=pexGCUPlUeA&feature=player_embedded.
[53] Tanzina Vega, *Opt-out Provision Would Halt Some, but Not All, Web Tracking*, NY TIMES (Feb. 26, 2012), http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=1&bl.
[54] *Facebook Settles FTC Charges that it Deceived Consumers by Failing to keep its Privacy Promises*, http://www.ftc.gov/opa/2011/11/privacysettlement.shtm; *FTC Gives Final Approval to Settlement with Google over Buzz Rollout*, http://www.ftc.gov/opa/2011/10/buzz.shtm (last visited Apr. 2, 2012).

technological means to affect consumer control over personal information. For example, The February 2012 White House Proposal, which included a consumer Privacy Bill of Rights, called on the use of technology to preserve consumer privacy. [55]

As the White House stated:

> It is increasingly common for Internet companies that have direct relationships with consumers to offer detailed privacy settings that allow individuals to exercise greater control over what personal data the companies collect and when it can be collected. In addition, privacy-enhancing technologies, such as the "Do Not Track" mechanism, allow consumers to exercise some control over how third parties use personal data or whether they receive it at all. All of these mechanisms show promise. However, they require further development to ensure they are easy to use, strike a balance with innovative uses of personal data, take public safety interests into account, and present consumers with a clear picture of the potential costs and benefits of limiting personal data collection. [56]

As commentators were quick to point out, the Do-Not-Track mechanism referenced by the White House may not meet consumers' expectations regarding online privacy because it will not block advertisements from first-party sites. In other words, if a consumer accessed a website, such as Facebook, it could still deliver ads to the consumer based on information provided on a visit to the site. On the other hand, Do-Not-Track would prevent a website from providing information to third parties for advertisements on other websites. The head of one privacy advocacy group, the Center for Digital Democracy (CDD), told the *New York Times* that "[w]e cannot accept any 'deal' that does not really protect consumers, and merely allows the data-profiling status quo to remain. Instead of

[55] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 13 (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[56] *Id.* at 12-13.

negotiations, the CDD would have preferred the White House to introduce new legislation that clearly protected consumers online." [57]

The FTC's privacy report of March 2012—*Protecting Consumer Privacy in an Era of Rapid Change*—called on Congress to enact a baseline for privacy protection. [58] The FTC also called on companies to adopt the principles of privacy by design, simplified choice for businesses and consumers, including a Do-Not-Track mechanism, and greater transparency regarding information collection and uses. [59] The proposed framework, according to the FTC, was "intended to articulate best practices for companies that collect and use consumer data," but would not "serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC." [60] The report acknowledged that there was "broad consensus … that consumers need basic privacy protections for their personal information" and acknowledged that some commenters "stated that the Commission should recognize a broader set of privacy harms than those involving physical and economic injury." [61]

In light of the divergence between consumer expectations regarding privacy, the lack of existing legal protections for such privacy (and for monetary redress of privacy violations), and the support of some in the Internet community for the free and unregulated flow of data, privacy is likely to continue to be contentious issue. Any privacy legislation, including that suggested by the White House and FTC reports, is likely to create controversy among at least some of the stakeholders in the cyberspace law field.

Trademark Law in Cyberspace: The "Growing Sophistication" of Internet Users

---

[57] Tanzina Vega, *Opt-out Provision Would Halt Some, but Not All,* Web Tracking, NY TIMES (Feb. 26, 2012), http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=1&bl.
[58] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, Federal Trade Commission iii (Mar. 2012), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
[59] *Id.*
[60] *Id.* at vii.
[61] *Id.*

Two recent cases from the Ninth Circuit indicate that courts may be modifying their views regarding the degree of sophistication of knowledge of Internet users. In *Toyota Motor Sales v. Tabari* [62] and *Network Automation v. Advanced Systems Concepts*, [63] the Ninth Circuit indicated it was likely to assume, at least in the context of trademarked terms in domain names and in search results, that Internet users had a greater degree of experience than it has assumed in the past.

As early as 1999, the Ninth Circuit acknowledged that courts had to be sensitive to the rapid pace of technological change brought about by the Internet in deciding cases in the cyberspace field. In *Brookfield Communications Inc. v. West Coast Entertainment Corporation*, [64] which involved the use of trademarked terms in domain names and "metatags," the court stated "[w]e must be acutely aware of excessive rigidity when applying the law in the Internet context; emerging technologies require a flexible approach." Despite this pronouncement, the court in *Brookfield* adopted a somewhat protective view regarding the Internet, holding that a user who clicked on a search result for a defendant's site that was produced using plaintiff's trademark could suffer "initial interest confusion" when detouring to the site that could give rise to trademark infringement. [65]

The Ninth Circuit in *Brookfield* posited that an Internet user might be unknowingly led down a false path through search results because the user would not know that the search results were the result of purchased metatags. Ten years later, in the *Toyota Motor Sales* and *Network Automation* cases, the Ninth Circuit modified its views, now giving users credit for knowing that not all domain names and search results that included trademarked terms are those of the trademark owner.

In *Toyota,* the court addressed the issue of whether consumers were likely to be confused into thinking that websites for auto brokers with the names "buy-a-lexus.com" and "buyorleaselexus.com" infringed the Lexus trademark. In finding that the defendants were entitled to use the term

[62] *Toyota Motor Sales v. Tabari,* 610 F.3d 1171 (9th Cir. 2010).
[63] *Network Automation v. Advanced Systems Concepts,* 638 F.3d 1137 (9th Cir. 2011).
[64] *Brookfield Communications Inc. v. West Coast Entertainment Corp.,* 174 F.3d 1036, 1054 (9th Cir. 1999).
[65] *Id.* at 1060-61.

"lexus" in their domain names under trademark nominative fair use principles, Chief Judge Kozinski of the Ninth Circuit opined that consumers would not necessarily believe that a website was connected to the owner of a trademark simply because it included the trademark. In the court's view, "the worst that can happen is that some consumers may arrive at the site uncertain as to what they will find. But in the age of FIOS, cable modems, DSL and T1 lines, reasonable, prudent and experienced Internet consumers are accustomed to such exploration by trial and error." [66]

According to the Ninth Circuit, Internet users exercise a "sensible agnosticism" in their views as to websites' names. [67] Whereas a user in 1999 might be diverted from his or her true goal by search results produced through metatags, the "reasonably prudent" Internet consumer of 2010 would know better:

> Consumers who use the Internet for shopping are generally quite sophisticated about such matters and will not be fooled into thinking that the prestigious German car manufacturer sells boots at mercedesboots.com, or homes at mercedeshomes.com, or that comcastsucks.org is sponsored or endorsed by the TV cable company just because the string of letters making up its trademark appears in the domain. [68]

In *Network Automation*, the Ninth Circuit applied its view of Internet user "agnosticism" to the question of whether a user would be confused in viewing sponsored search results produced through the Google "ad words" program into thinking that such results were sponsored by the trademark owners. The court found that users were unlikely to be confused, at least for the products in question, stating that "[a] sophisticated consumer of business software exercising a high degree of care is more likely to understand the mechanics of Internet search engines and the nature of sponsored links, whereas an un-savvy consumer exercising less care is more likely to be confused." [69] Citing *Toyota*, the court held that "the default

[66] *Toyota*, 610 F.3d at 1179.
[67] *Id.*
[68] *Id.* at 1178.
[69] *Network Automation*, 638 F.3d at 1152.

degree of consumer care is becoming more heightened as the novelty of the Internet evaporates and online commerce becomes commonplace." [70]

The recognition by the Ninth Circuit of the increasing sophistication of Internet consumers raises several questions regarding the effect of changing technology and user experience on cyberspace law. Although the sophistication of consumers was at issue in *Toyota* and *Network Automation*, because the degree of care of consumers is relevant to trademark infringement, would the same presumption of user sophistication or "agnosticism" apply to other contexts, such as SPAM, "phishing" or advertisements on websites?

Although courts have not addressed the issue, it is likely that the Ninth Circuit's view of user sophistication may not be applicable in all Internet contexts. There may indeed be users who understand how Google search results are produced, but undoubtedly, many others have no more understanding of this than they do about TCP/IP network protocols. As in the privacy area, Internet users may also have inconsistent views regarding the Internet, regardless of their level of experience. This is borne out in research conducted by the Pew Research Center, which indicates that Internet users expect liberty and security, transparency and confidentiality, and free expression and tolerance and civility when they go online. [71] The point is not that cyberspace law should be affected by public opinion surveys, but rather that familiarity with the Internet does not equate into sophistication regarding its operations or technology.

The International Cyber Law Quandary

Two cases from the Court of Justice of the European Union (the "Court of Justice")—the highest court in Europe in regard to EU law—illustrate that different legal systems are grappling with many of the same issues as in the United States regarding file sharing and copyright infringement.

[70] *Id.*

[71] Lee Rainie, *I'm OK, They're Not: Trying to unravel what Internet users want when it comes to governing the Internet*, Pew Internet and American Life Project (July 18, 2011), http://pewInternet.org/Presentations/2011/Jul/Internet-Governance-Forum.aspx.

In the *Scarlet Extended* [72] and *Netlog* [73] cases, the Court of Justice addressed the question of whether an ISP (Scarlet Extended) and a networking site (Netlog) had an obligation to filter user files to determine whether they infringed copyrights in certain works.

The plaintiff in both cases was SABAM, a Belgian management company representing authors, composers, and publishers of artistic works, responsible for copyright protection of such works. SABAM applied to a Belgian court for injunctions requiring Scarlet Extended and Netlog to install a monitoring system to prevent illegal downloading and file sharing on their sites. Scarlet Extended and Netlog argued that a requirement to monitor users' files for copyright violations would violate Article 15 of Directive [74] 2000/31 regarding electronic commerce, which states that "Member States shall not impose a general obligation on providers ... to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity." [75] Defendants also claimed that the monitoring requirement would violate Recital 47 of Directive 2000/31, which states:

> Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation. [76]

[72] *Scarlet Extended SA v. Societe belge des auteurs, compositeurs et editeurs (SABAM)*, Case C-70/10, (Court of Justice of the European Union, Third Chamber, November 24, 2011).
[73] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVA (SABAM) v. Netlog NV*, Case C-360/10 (Court of Justice of the European Union, Third Chamber, February 16, 2012) ("*Netlog*").
[74] A Directive is legislation from the EU that directs member states to achieve a certain result without specifying the particular means. Typically, member states adopt national laws implementing the results through their own legislative procedures.
[75] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0001:EN:PDF.
[76] *Id.*

The Court of Justice held in both cases that the injunction requested by SABAM would violate Directive 2000/31 by requiring active monitoring, including identification of files likely to contain copyrighted works, determination of which copyrighted materials were being made available to the public unlawfully, and blocking the files considered unlawful from being made available to the public. In reaching this conclusion, the Court of Justice balanced the rights not only of SABAM in its copyrights and those of Scarlet Extended and Netlog to conduct their businesses, but also of Internet users. Indeed, the court found that the users of social networking and file-sharing services had a fundamental right in this matter, "namely their right to protection of their personal data and their freedom to receive or impart information." [77]

The requested injunction was therefore defective because it could "potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications." The court further noted that " [i]ndeed, it is not contended that the reply to the question of whether a transmission is lawful also depends on the application of statutory exception to copyright, which varies from one member state to another. In addition, in some member states, certain works fall within the public domain or may be posted online free of charge by the authors concerned."[78]

Although the Court of Justice approached the question from the perspective of the EU law, its conclusion regarding the interests of Internet users in free expression echoes the position of those who argued that SOPA violated the First Amendment. As Professor Laurence Tribe stated in one of his objections to the proposed legislation:

> Although the problems of online copyright and trademark infringement are genuine, SOPA is an extreme measure that is not narrowly tailored to governmental interests. It is a blunderbuss rather than a properly limited response, and its stiff penalties would significantly endanger legitimate websites and services. Its constitutional defects are not

[77] *Scarlet Extended*, ¶ 50.
[78] *Id*. ¶ 52.

> marginal ones that could readily be trimmed in the process of applying and enforcing it in particular cases. Rather, its very existence would dramatically chill protected speech by undermining the openness and free exchange of information at the heart of the Internet. It should not be enacted by Congress. [79]

The Court of Justice decisions in *Scarlet Extended* and *Netlog* thus highlight an important trend in cyberspace law: the impact of the interests of Internet users on the law. As in the opposition to SOPA, attitudes toward piracy, or in the posited sophistication of such users regarding trademark infringement matters, Internet users continue to have a significant stake and influence on the development of cyberspace law.

Conclusion

It is likely that the developments in cyberspace law for the next few years will continue to play out the trends seen in the past few years.

The pressure for anti-piracy legislation for "rogue" foreign websites is likely to persist, since downloads from those sites will continue to have an adverse financial impact on the recording and motion picture industries. It is also likely there will be controversies regarding takedowns of cyberlocker sites, as with Megaupload, with commentators arguing that such takedowns demonstrate that existing legal mechanisms are sufficient and others that they are an abuse of government power.

Privacy will also continue to be a major focus in cyberspace law. Although it is unlikely that any national privacy or data breach notification laws will be passed in the United States in the election year 2012, there may be greater likelihood of passage in future years. The proposed new European regulation on data protection will continue to be actively debated, although it is also unlikely that it will receive approval by the EU Parliament and Council this calendar year.

---

[79] Laurence H. Tribe, *The "Stop Online Piracy Act" (SOPA) Violates the First Amendment*, http://www.net-coalition.com/wp-content/uploads/2011/08/tribe-legis-memo-on-SOPA-12-6-11-1.pdf (last visited Apr. 2, 2012).

It is also safe to assume that technology will continue to have an impact on cyberspace law, whether in the form of measures for users to control personal data, such as Do Not Track, or the continued expansion of cloud and mobile computing.

These issues are important because the main actors in the cyberspace law arena—ISPs, search engines, social media platforms, hardware and mobile computing manufacturers, content providers, and users—have vested, but divergent, views regarding any laws that impact their interests. Because there is no unanimity regarding these issues, any changes to the law will be difficult to achieve without substantial compromises by relevant stakeholders. In this regard, the SOPA dispute is a good indicator that future controversies will likely be fiercely fought.

As in past years, courts will continue to have a major impact on cyberspace law. Currently pending before the courts are significant cases that will affect the course of cyberspace law, particularly regarding the safe harbor under the DMCA. For example, the coming year is likely to see a decision between the Second Circuit in the *Viacom v. YouTube* litigation. [80] This decision is likely again to highlight the divergent interests of media companies, service providers, and users, particularly if the Second Circuit takes a different approach than the Ninth Circuit did in *UMG Recordings Inc. v. Veoh Networks Inc.*, in which it upheld Veoh's safe harbor defense under the DMCA. [81]

It is important that lawyers and clients have a broader understanding of the interests of the different stakeholders in this area so that they can plan for future developments and controversies. In the privacy area, both lawyers and clients should understand the importance of incorporating privacy principles

[80] Brief of Plaintiffs-Appellants Viacom International Inc., *Viacom Int'l Inc. v. YouTube Inc.*, No. 10-3270 (2d. Cir. Dec. 3, 2010), *available at* http://news.viacom.com/pdf/Final_Viacom_Brief.pdf; Brief of Defendants-Appellees YouTube Inc., *Viacom Int'l Inc. v. YouTube Inc.*, No. 10-3270 (2d. Cir. Mar. 31, 2011), *available at* https://www.eff.org/sites/default/files/filenode/viacom_v_youtube/2011-03-31_YouTubeBrief_3270.pdf. After this article was written, the Second Circuit issued its decision, which caused the Ninth Circuit to ask for briefing of the impact of the decision on its Veoh Networks *decision. See Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2012); *UMG Recordings, Inc. v. Veoh Network Inc.*, Order, June 7, 2012.

[81] *UMG Recordings Inc. v. Veoh Networks Inc.*, 667 F.3d 1022 (9th Cir. 2011).

into their business efforts from the planning stage, rather than as an afterthought. Although national privacy legislation in the United States may not immediately be on the horizon, it is more likely than ever before that this country will eventually have such laws. Because the EU will also eventually adopt a much stricter data protection regulation binding on all its member states, clients that sell product to consumers in the EU, have employees there, or transfer data from the EU should immediately consider beginning to incorporate stricter privacy protections into their policies and procedures.

Developments in other cyberspace law sectors are more difficult to predict, but it is important for both lawyers and clients to understand the reasons the trends that resulted in the SOPA battle are likely to persist. Indeed, if the opponents and proponents of SOPA had spent their resources on engaging in more dialogue, there may have been a greater chance for compromise regarding what is likely to be an ongoing debate in cyberspace law.

Key Takeaways

- Keep in mind the argument over metatags and services such as Google Ad Words when guiding clients in both copyright and trademark protection actions and promotional activities. Past decisions and guidelines may no longer apply because of the growing sophistication and "sensible agnosticism" of today's consumers, according to the Ninth Circuit.
- Plan for the eventual adoption of national privacy legislation in the United States, including the possibility of the adoption of a Consumer Privacy Bill of rights or other requirements for baseline privacy protection. Considering adopting privacy protections at an early stage (privacy by design), rather than as an afterthought.
- Stay on top of privacy protections and legal developments in the EU, which is in the process of developing and implementing much stricter data protection regulation. If your client does business with EU member states, sells products in the EU, has subsidiaries/employees in the EU, or transfers data to and from the EU, adopt stricter privacy protections into policies and

procedures with an eye toward compliance and avoiding legal difficulties now, rather than later.

Timothy J. Toohey is a partner at Snell & Willmer LLP, where his practice is concentrated on complex litigation, intellectual property, and privacy and data protection matters. He has extensive experience in all elements of intellectual property counseling and litigation, including trademark, copyright, and patent matters. His experience includes the trial and arbitration of trademark, design patent, and copyright infringement matters, as well as licensing and trade secret disputes. He has also been involved in numerous matters involving privacy and data protection, including matters involving federal, state, and international laws involving data breach and disclosure of personally identifiable information.

Mr. Toohey has handled a variety of privacy and data breach matters, including advice regarding the CAN-SPAM Act, Computer Fraud and Abuse Act, Digital Millennium Copyright Act, Electronic Communications Privacy Act, cloud computing, and social media. He has also advised clients regarding California's Song-Beverly Act, the California Security Breach Notice provisions, and international privacy and security issues, including compliance with European Union (EU) data protection and privacy directives. In addition, he regularly represents clients in environmental and other cases.

Mr. Toohey has lectured in the University of California at Los Angeles (UCLA) Department of History, where he teaches courses in US constitutional and legal history.

Acknowledgment: *I would like to thank David Liu and Brant Freer for their assistance and support.*

ASPATORE

Aspatore Books, a Thomson Reuters business, exclusively publishes C-Level executives and partners from the world's most respected companies and law firms. Each publication provides professionals of all levels with proven business and legal intelligence from industry insiders—direct and unfiltered insight from those who know it best. Aspatore Books is committed to publishing an innovative line of business and legal titles that lay forth principles and offer insights that can have a direct financial impact on the reader's business objectives.

Each chapter in the *Inside the Minds* series offers thought leadership and expert analysis on an industry, profession, or topic, providing a future-oriented perspective and proven strategies for success. Each author has been selected based on their experience and C-Level standing within the business and legal communities. *Inside the Minds* was conceived to give a first-hand look into the leading minds of top business executives and lawyers worldwide, presenting an unprecedented collection of views on various industries and professions.

ASPATORE