Temple American Inn of Court – December 2014 Program
How the Grinch stole my personal data, and almost Christmas

Selected Materials on Cyber Security
Collected and Summarized by Shannon Cunningham, Esq.

Here are a few different sources of information on cyberprivacy. I know other members of the research team will be sending additional sources of information. You had asked us to find different resources touching on the range of issues presented by cyberprivacy. Let the research team if you need more research on a particular issue.

CYBERPRIVACY AND DIGITAL PRIVACY RISKS: Businesses are trying to manage large volumes of potentially sensitive data and are looking at new technologies, such as cloud computing, to save money and increase efficiency. Attorneys who advise companies that deal with sensitive data should prepare their clients to be held accountable for any data breaches and to understand how new technology may implicate consumer privacy. This article discusses data security breaches, cloud computing, behavioral advertising, mobile privacy, social networking and data mining, mobile marketing and affiliate marketing.

INTELLECTUAL PROPERTY'S LESSONS FOR INFORMATION PRIVACY: This article discusses the tension between the desire to keep information private and the desire to share that information with others. Online technology amplifies the clash between the two desires by allowing for more data to be compiled on individual consumers and by making it easier for that data to be repackaged and communicated to others. Intellectual property law has developed a variety of approaches to address free speech concerns while upholding necessary data privacy measures.

THE GLOBALIZATION OF PRIVACY AND SECURITY IN CYBERSPACE: GOVERNMENT, LAW, AND SOCIETY IN THE TWENTY-FIRST CENTURY ONLINE WORLD: Two of the more interesting topics covered in this article are – how attorneys should advise clients in navigating information privacy and security regulations and the jurisdictional issues with cyberprivacy. This article concludes that there are many companies who are not aware that their data has been compromised by industrial or governmental espionage or criminal activity.

This is a link to a website that discusses several internet law developments from last year. Numbers 9, 2, and 1 are all regarding privacy concerns. If you are interested in basing the script on any of these news items, we can do additional research in these areas.
http://www.forbes.com/sites/ericgoldman/2014/01/09/top-ten-internet-law-developments-of-2013/

Here is a link to a website that lists some state laws related to internet privacy. There are a few interesting ones such as the privacy of e-readers and employee emails:
http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

29-NOV Comm. Law. 10

Communications Lawyer
November, 2012

Cover Story

CYBERPRIVACY AND DIGITAL PRIVACY RISKS

Blaine Kimrey, Bryan Clark[a1]

It is no secret that digital media and mobile marketing are continuing to grow at an astounding rate. Companies worldwide are faced with increasing pressure to provide valuable Web and mobile content. At the same time, businesses are trying to manage large volumes of potentially sensitive data and are looking at new technologies such as cloud computing to save money and increase efficiency.

To facilitate these needs, technology companies continue to develop more advanced systems for managing and protecting data, tracking online and mobile behavior, aggregating information, targeting Web and mobile advertisements, and monetizing mobile content. And despite the privacy concerns, venture capitalists are not hesitant to invest in the future of these operations. The *Wall Street Journal* reported last year that venture firms have invested more than $4.6 billion in online ad firms since 2007, and the industry continues to grow.[1] Meanwhile, companies such as Google have continued to innovate in the arena of cloud computing.[2]

As these industries have grown, scrutiny of their practices has increased as well--particularly in the context of privacy. Attorneys who advise companies that deal with sensitive data should prepare their clients to be held accountable for any data breaches or cyberattacks in which valuable information is compromised. Online and mobile ad firms and technology providers and their more traditional clients also have been named in lawsuits nationwide that raise a variety of privacy and consumer protection issues. This article will address seven primary areas of concern in the realm of **cyberprivacy** and digital privacy risks: (1) data security and data breach, (2) cloud computing, (3) behavioral advertising, (4) mobile privacy, (5) social networking and data mining, (6) mobile marketing, and (7) affiliate marketing.

Data Security and Data Breach

Attorneys operating in this space should advise their clients that they can face significant exposure for privacy issues arising out of inadequate data security and data breach even if litigation is never filed. In 2010, a large national health care company reported that it incurred costs in excess of $7 million for investigating the circumstances surrounding a missing portable disk drive, notifying its members, and offering credit monitoring and identity theft insurance.[3] In our digital world, it is not uncommon for individual employees to have access to the personal identifiable information (PII)[4] or protected health information (PHI)[5] of thousands, if not tens of thousands, of people through e-mail, spreadsheets, or other documents stored on platforms like laptop computers, smartphones, or USB drives that could easily be compromised. In the event of such a breach, a company (and its counsel) will be required to navigate the complicated--and often contradictory--framework of state and federal data breach notification statutes. Led by California, 46 states have enacted statutes that define PII and establish notification requirements.[6] Attorneys dealing with a data breach must carefully assess whether these statutes apply, as well as analyze any requirements under the Health Insurance Portability and Accountability Act (HIPAA)[7] and the Gramm-Leach-Bliley Act (GLBA).[8] According to the 2011 annual study conducted by the Ponemon Institute and released in March 2012, the average cost for a breach is $194 per data subject.[9] Based on this figure, the cost for responding to a data breach involving PII for 10,000 people would be in excess of $1.94 million.

Additionally, companies that fail to protect sensitive information should be warned about potential liability in actions filed by state attorneys general and in putative class action lawsuits. For example, in 2010, the Connecticut attorney general became the

first state attorney general to exercise the authority granted under HIPAA to enforce its privacy provisions. The defendant ended up settling for $250,000 and agreeing to a corrective action plan.[10] Also, although they have had limited success in establishing damages absent evidence of actual identity theft, plaintiffs' attorneys regularly bring class actions on the heels of large data breaches.

Perhaps the best way for your clients to mitigate the risk associated with data breach notification is to ensure that the computers on which sensitive information is stored are encrypted. In most states, data on encrypted computers falls outside the definition of breached PII, meaning that no notification would be required. Additionally, attorneys should advise clients to carefully consider what sort of information they are collecting and how that information will be used. To the extent possible, collection of sensitive information should be avoided unless it is necessary to the company's business objectives. If sensitive information is essential, the company should limit which employees and third parties have access to that information. And if it is necessary for third parties to access sensitive information, companies should ensure that they have agreements in place indemnifying them for any data breach caused by actions of that third party.

Cloud Computing

In recent years, cloud computing[11] has grown in popularity among businesses because it offers significant cost ***11** savings, the ability to scale the system to increased or decreased demand, and increased mobility. But those benefits must be weighed against privacy concerns. State data breach notification statutes, HIPAA, GLBA, fiduciary obligations, and common law privacy torts all create significant risks for entities that allow third parties to control their information on external servers. For example, Google provides a tool that allows users to transfer Microsoft Office files to the Web so that multiple people can edit and collaborate on them. Google's Cloud Connect service allows documents to be uploaded to Google's servers and accessed through a unique Web address. Although using this system likely would result in significant cost savings for businesses, attorneys should advise clients handling sensitive or confidential information to be wary of uploading it to Google's servers (over which the companies have no control) and making the documents available via the Web (where they could conceivably be accessed by third parties). Thus, despite the benefits, it is important for attorneys to advise clients considering cloud computing to carefully weigh the privacy ramifications of that decision and ensure that the cloud computing provider offers sufficient protections against data breach and inadvertent disclosure.

Behavioral Advertising

As online advertisers create new technologies that will help tailor advertisements to consumer behavior, plaintiffs' attorneys have crafted new arguments that these mechanisms violate consumer privacy. Currently, two primary areas of concern are "browser history sniffing" and "Flash cookies."[12] "[H]istory sniffing ... compares ... URL links in a computer's history folder to a master list of links[] to [determine] whether the consumer has visited a particular ... page in the past."[13] Flash cookie technology works in connection with typical browser cookies,[14] allowing the cookie to respawn without notice to the user if deleted. Both technologies have resulted in class action litigation against the creators of the new technologies and against traditional media and major corporations that utilize the technology.

History Sniffing Claims

History sniffing operates through JavaScript-enabled websites. Companies can embed JavaScript code in their websites that (behind the scenes) presents users' Web browsers with a list of uniform resource locators (URLs), or Web addresses. This list essentially creates "invisible" links on the webpage that can be viewed by the script running in the background. Because browsers display links differently when they have been previously visited (typically in a different color), the program can identify which of the websites from the list the user has visited previously and use this information to deliver targeted advertisements. In putative class action lawsuits, plaintiffs have alleged that the collection of this information is an invasion of privacy and asserted claims for: (1) violation of the Computer Fraud and Abuse Act (CFAA),[15] (2) violation of state computer crime laws, (3) violation of state consumer protection statutes, and (4) unjust enrichment.[16]

Flash Cookie Claims

A Flash cookie is a line of tracking code that is planted on a user's computer as an Adobe Flash Media Player local shared object. Consumers typically use Flash Media to view video content on their computers, but various companies have leveraged this technology to create Flash cookies that respawn the typical browser cookie whenever it is deleted. In putative class actions, plaintiffs have alleged that this practice of planting files on their computers and tracking their activities is an actionable invasion of privacy. Plaintiffs have asserted causes of action for: (1) violation of the CFAA, (2) violation of state computer crime laws, (3) violation of state invasion of privacy statutes, (4) violation of state consumer fraud statutes, and (5) trespass to chattels.[17]

Risks and Risk Avoidance

As with many digital privacy issues, the case law on these history sniffing and Flash cookie claims is limited. One likely defense is that plaintiffs were not harmed by these practices and therefore lack standing to assert a claim. However, given the costs and uncertainty of litigation, some defendants have already opted to settle these cases. Last year, a settlement was reached in several Flash cookie lawsuits that had been consolidated in the U.S. District Court for the Central District of California. The settlement calls for a fund of $2.4 million, with no reverter to the settling defendants.[18]

Attorneys should warn clients venturing into behavioral advertising to be sure that they fully understand the technology being used to generate advertisements on their websites and, if possible, seek indemnity and additional insured status from the technology providers in any contracts with those providers. It is also important for companies to provide a clear description of any tracking technologies in their online privacy policies.

Mobile Privacy

In a series of articles beginning in December 2010, the *Wall Street Journal* has shone a bright light on previously overlooked privacy issues arising from advertisers' tracking of mobile activities through iPhone applications and other mobile soft-ware.[19] These articles have revealed that advertisers often collect a significant amount of information from users in an effort to support targeted advertising, often without clear disclosures to consumers as to what information is being collected. Some consumer advocates have argued that this data collection is an invasion of privacy, an argument that has not been lost on plaintiffs' attorneys practicing in the digital space. Since October 2010, numerous putative class action lawsuits have been filed related to tracking of mobile phone browsing. Three of the cases focused on software created by Ringleader Digital, Inc. (Ringleader) to take advantage of HTML5 database technology,[20] and others have focused on the collection of unique device identifiers (UDIDs) from iPhones by Apple, Inc. and other mobile application providers.[21]

HTML5 Class Actions

Ringleader's Media Stamp program (and the advertisers that use it) was the focus of federal lawsuits in California, Texas, and New York. ***12** According to plaintiffs' complaints, Media Stamp takes advantage of HTML5 software, which a growing number of mobile phones use to operate their Internet browsers. HTML5 software contains local storage databases that allow websites to store information on mobile devices to enhance Internet browsing on mobile devices. Media Stamp facilitates the creation of unique identifying information numbers that are assigned to mobile devices, allowing Ringleader, ad agencies, and website publishers to track a user's Web browsing. Plaintiffs alleged that unlike an online cookie, however, these unique ID numbers were stored both in the HTML5 database and in Ringleader's own database and that a cleaning of a user's cookie folder and browsing history did not prevent Ringleader from continuing to track a user's Internet activity.

Arguing that Ringleader's collection of this information is a violation of privacy and that the creation of a nonremovable database has damaged their mobile devices, the plaintiffs asserted causes of action for: (1) violation of the CFAA, (2) violation of state computer fraud laws (including California Penal Code section 502), (3) violation of state consumer protection laws, (4) statutory and common law invasion of privacy, (5) trespass to chattels, (6) unjust enrichment, and (7) violation of the Electronic Communications Privacy Act (ECPA).[22]

Two of the cases against Ringleader were consolidated in the U.S. District Court for the Southern District of New York, and the parties sought approval of a class action settlement that would have provided no monetary relief for the class members. After

Judge Cote declined to grant preliminary approval for the settlement and requested that the parties submit a revised proposal, the case was voluntarily dismissed by the plaintiffs and has not been refiled.

UDID Class Actions

A close analog to the HTML5 database tracking technology is technology that allows advertisers to track Internet activity through electronically readable UDIDs that are encoded in every Apple iPhone. These UDIDs cannot be blocked, altered, or deleted; can be used to track devices; and are often collected by iPhone applications. A study by Bucknell University found that 68 percent of the most popular iPhone applications transmitted the devices' UDIDs to outside servers owned by either the developer or the advertiser.[23]

Plaintiffs in putative class actions against Apple, application developers, and advertisers have alleged that this information collection was not properly disclosed and that plaintiffs would not have downloaded applications if they had realized that developers would then be able to track their devices. The lawsuits have asserted causes of action for: (1) violation of the CFAA, (2) violation of state computer fraud laws (including California Penal Code section 502), (3) violation of state consumer protection laws, (4) statutory and common law invasion of privacy, (5) trespass to chattels, (6) unjust enrichment, (7) violation of the ECPA, (8) breach of contract, (9) conversion, (10) violation of the Stored Communications Act,[24] (11) breach of implied covenant of good faith and fair dealing, and (12) violation of state constitutional provisions.

The UDID cases nationwide--including cases filed in the U.S. District Court for the Northern District of California, the U.S. District Court for the Central District of California, the U.S. District Court for the District of Puerto Rico, the U.S. District Court for the Northern District of Alabama, the U.S. District Court for the Middle District of Florida, and the U.S. District Court for the Southern District of Florida--were consolidated before Judge Koh in the Northern District of California.[25] In September 2011, Judge Koh dismissed the cases without prejudice for lack of Article III standing.[26] Judge Koh held that the plaintiffs had failed to allege sufficient facts to establish actual injury or harm for the purposes of Article III. The plaintiffs have pursued an amended complaint, but the case against many of the defendants was voluntarily dismissed in May 2012. In June 2012, Judge Koh dismissed with prejudice the plaintiffs' claims against the remaining mobile industry defendants (Admob, Inc.; Flurry, Inc.; AdMarvel, Inc.; Google, Inc.; and Medialets, Inc.) and dismissed with prejudice the claims against Apple for violations of the Stored Communications Act, violations of the Wiretap Act, violations of the California constitutional right to privacy, negligence, violations of the CFAA, trespass, conversion, and unjust enrichment. However, the suit continues against Apple on the plaintiffs' claims for violation of the California Consumer Legal Remedies Act and the California Unfair Competition Law.

Because the HTML5 and UDID cases present issues of first impression, there is limited case law that directly addresses these issues. It is possible that courts will follow Judge Koh's lead and hold, as they did with earlier challenges to traditional cookies, that plaintiffs were not harmed. It is also possible that courts could dismiss the UDID lawsuits on the basis that UDIDs are not personal information. In a similar context, a federal district court judge in Washington has held that Internet protocol (IP) addresses are not personally identifiable information; however, a New Jersey state court judge held that service providers cannot disclose users' IP addresses without a subpoena because people expect IP addresses to be kept private.[27]

As with online behavioral advertising, it is important for clients to fully understand and adequately disclose the nature of their mobile tracking technology. To the extent that clients are using technology that may create privacy issues, their contracts with the technology providers should be specifically tailored to address those issues, and they should modify their existing privacy policies to reflect the nature of the technology.

***13 Social Networking and Data Mining**

The immense popularity of social networking websites such as Face-book, MySpace, LinkedIn, and Twitter has, in some ways, changed our understanding of what information should be considered private. But even though many social networking users voluntarily disclose information that might otherwise be considered private, social networking sites have been a lightning rod for criticism related to breaches of privacy. An October 2010 article in the *Wall Street Journal* revealed that many of the most popular Facebook applications transmit identifying information about users (and, in some cases, their friends) to dozens of Internet and tracking companies.[28] This is precisely the type of conduct that typically draws the attention of the class action

plaintiffs' bar, not only resulting in lawsuits against Facebook but also opening the possibility of lawsuits against the parties responsible for creating the applications and the companies that received the information. Facebook, which has been a regular target of such lawsuits, settled a privacy lawsuit related to its Beacon program in December 2009 by setting up a $9.5 million fund for a nonprofit foundation to support online privacy.[29]

In another matter, Spokeo, a self-described "social network aggregator," was sued in two putative class actions in federal court in California for allegedly violating the Fair Credit Reporting Act by offering allegedly false data about individuals without giving them the chance to correct or remove inaccurate reports.[30] Spokeo aggregates data from many online and offline sources, such as phone listings, social networks, photo albums, and business websites. Plaintiffs claimed that the Spokeo entries for them are comprised of misinformation that could, inter alia, undermine their employment possibilities. Plaintiffs asserted causes of action for: (1) violation of the Fair Credit Reporting Act,[31] (2) unjust enrichment, and (3) violation of state consumer protection laws. Defendants filed a motion to dismiss that was granted in part and denied in part, and the matter is currently on appeal to the U.S. Court of Appeals for the Ninth Circuit.

These issues are just the tip of the iceberg when it comes to potential privacy concerns in the social networking realm. Thus, it is critical for attorneys who advise social networking sites, advertisers, or application developers to help their clients draft clear and complete privacy policies setting forth what information is being collected, how it will be shared, and with whom it will be shared. Data aggregators such as Spokeo are in a slightly different position because they do not have direct customer relationships with the consumers whose information they are publishing. For these sites, the focus should be on whether their practices violate any state or federal laws related to credit reporting and unfair or deceptive business practices.

Mobile Marketing

The term *mobile marketing* refers to an array of content directed to mobile telephones, ranging from text messages advertising certain products to premium mobile content such as ringtones, wallpaper, and games. In a general sense, two primary types of claims are associated with mobile marketing: text message spam cases and unauthorized charge cases. In a typical text message spam case, the plaintiffs allege that they received one or more unauthorized text messages. Based on these text messages, the plaintiffs bring a lawsuit on behalf of themselves and putative class members who have received similar text messages. These complaints often assert a count for violation of the Telephone Consumer Protection Act (TCPA),[32] arguing that a text message is a "call" under the automatic dialer provision of the TCPA. In a typical unauthorized charge case, the plaintiffs allege that their mobile phone bills were charged for text messages or other premium mobile content (such as ringtones, games, wallpapers, daily stock tips, and sports scores) that they did not authorize. The complaints typically assert claims for, inter alia, unjust enrichment, tortious interference, trespass to chattels, and violation of state consumer fraud statutes.

Text Message Spam TCPA Claims

Since the Ninth Circuit's June 2009 decision in *Satterfield v. Simon & Schuster*,[33] holding that the TCPA applies to text messages, plaintiffs have filed an increasing number of putative class action lawsuits against businesses and agencies that use mobile marketing as part of their advertising and sales campaigns. Several of these cases have been resolved in expensive class action settlements.

For example, the Northern District of California approved a settlement in *Satterfield* that created a settlement fund of $10 million and awarded attorney fees of $2.5 million.[34] To successfully assert a TCPA claim related to text messaging, plaintiffs must prove that: (1) a "call" was made using an "automatic telephone dialing system" or an artificial or prerecorded voice, (2) the number called was assigned to a cellular telephone service, and (3) the "call" was not made with the "prior express consent" of the receiving party.[35] An *automatic telephone dialing system* is defined as equipment with the capacity to store or produce numbers to be called, using a random number generator, and to dial such numbers.[36] Although the term *call* is not defined and the statute makes no specific reference to text messaging, class action plaintiffs have identified mobile marketing content as "unsolicited commercial text calls to potential customers using an automatic telephone dialing system and/or using an artificial and prerecorded message."[37] Beyond the Ninth Circuit, this interpretation also has been accepted in at least two other jurisdictions: the U.S. District Court for the Northern District of Illinois in *Abbas v. Selling Source*[38] and *Lozano v. Twentieth Century Fox Film Corp.*,[39] and an Arizona state court in *Joffe v. Acacia Mortgage Corp.*[40]

Text messaging TCPA claims have been used to target not only mobile marketing companies but also larger corporations that use their services.

***14** A prime example is *Weinstein v. AIR-IT2ME*, a text messaging TCPA class action brought against outdoor apparel retailer Timberland and its mobile marketing partners.[41] Plaintiffs alleged that Timberland sent unsolicited text message advertisements to plaintiffs' cell phones, subjecting them to "the aggravation that necessarily accompanies unsolicited wireless spam" as well as the cost of text messaging.[42] The only cause of action raised by the plaintiffs was a violation of the TCPA. Plaintiffs alleged that these "text calls" had been made with an automatic telephone dialing system, thereby bringing them within the scope of the TCPA, and that Timberland had not obtained the consent of the recipients.[43]

Because the statutory language of the TCPA does not clearly apply to text messages, several issues are unique to text message cases: (1) whether the plaintiff must allege that he was charged for the text message he received, (2) whether a system's mere capacity to autodial numbers is sufficient to allege an automated telephone dialing system, (3) whether a text message is a call within the meaning of the TCPA, (4) whether the application of the TCPA to text messages would violate the First Amendment, and (5) whether the application of the TCPA to text messages would render the statute void for vagueness under the due process clause. At least six cases nationwide have addressed one or more of these issues: *Satterfield, Abbas, Lozano, Joffe, Satterfield v. Simon & Schuster, Inc. (Satterfield I)*,[44] and *Pollock v. Island Arbitration & Mediation, Inc.*,[45] with the majority of these cases resulting in decisions beneficial to TCPA plaintiffs. *Abbas* was the first case to address all five issues.

Although text message TCPA cases are still a relatively new phenomenon and often present the possibility for defenses that would raise issues of first impression, the momentum is currently with the plaintiffs bringing these cases. This means that attorneys should warn clients about these issues before they initiate text message campaigns, and advise them to insist on indemnities for advertising agencies or networks if at all possible.

Unauthorized Charge Claims

In unauthorized charge cases, plaintiffs typically assert causes of action under one or more of the following theories: (1) unjust enrichment, (2) tortious interference, (3) trespass to chattels, (4) violation of consumer fraud statutes, (5) violation of the CFAA, and (6) breach of contract. Such claims have been brought against mobile content providers, wireless carriers, aggregators (which manage billing between cell phone carriers and content providers), affiliate marketers (entities that engage in Web advertising related to mobile content), copyright licensers, and social networking websites that offer mobile services.

The large class action settlements that have arisen from unauthorized charge cases should pose concerns for businesses involved in mobile marketing and for their insurance carriers. In 2010 alone, courts approved class action settlements with funds of $36 million and $12.25 million.[46] However, none of these cases has ever been tried. In fact, these cases are rarely litigated to conclusion, and it appears that only one court nationwide has certified a text message class in the face of opposition.[47] Although there have been some preliminary rulings, plaintiffs in these cases often withdraw in the face of case-dispositive motions. Many of the possible defenses therefore remain untested in the context of unauthorized charges. Possible defenses include: (1) inadequate pleading under *Bell Atlantic Corp. v. Twombly* and *Ashcroft v. Iqbal*,[48] (2) the voluntary payment doctrine, (3) CAN-SPAM Act preemption,[49] (4) immunity under § 230 of the Communications Decency Act,[50] and (5) passive conduit / common carrier defenses. Regardless of these defenses, mobile marketing clients could face significant risk if they are involved in the distribution of premium mobile content without sufficient opt-in/opt-out procedures.

Affiliate Marketing

The same plaintiffs' lawyers who have pursued the mobile marketing litigation have also focused their attention on affiliate marketers over the last few years. Affiliate marketers are advertising networks that connect advertisers with Internet publishers that create and distribute online advertisements in the form of e-mail offers, sponsored links, and banner ads. The goal is to drive traffic to the advertisers' websites, which sell goods or services. These goods and services are often subscription (or "continuity") plans, meaning that consumers purchasing the product pay a small initial fee and are then charged a larger fee on a monthly basis for as long as they desire to use the product. The affiliate marketer and the publisher are paid based on the number of sales that are made. Some affiliate marketers also have arrangements with advertisers whereby the affiliate marketers will use the information collected at the point of sale to contact the consumer and attempt to sell additional products,

i.e. ""upsell."

Class action plaintiffs have alleged that the advertisements created by the affiliate networks are misleading, false, and/or fail to disclose material terms about the product. Plaintiffs contend that they would not have purchased the product at issue if they had fully understood the terms. These putative class action complaints, which typically name both the advertisers and the affiliate marketers, have asserted causes of action for: (1) violation of state consumer protection laws, (2) fraud in the inducement, (3) conspiracy, (4) breach of contract, and (5) unjust enrichment.[51]

These cases are similar in many ways to the unauthorized charge cases and may be subject to some of the same defenses, including: (1) inadequate pleading under *Twombly/Iqbal*,[52] (2) the voluntary payment doctrine, and (3) immunity under § 230 of the Communications Decency Act.[53] Because these cases are often ***15** filed with boilerplate complaints and minimal investigation, it is often difficult for the plaintiffs to plead the allegations of fraud with the requisite specificity.[54] The individualized nature of the online transactions also could create significant problems for class certification, although one district court judge has certified a class in the affiliate marketing context.[55]

From a compliance standpoint, the key for affiliate marketing clients is to ensure the truth of any ad copy that they create and provide clear and conspicuous terms and conditions on the Web pages where consumers will be signing up for the product. Moreover, to the extent possible, it is important for affiliate marketers to protect themselves through indemnity agreements with both advertisers and publishers.

Conclusion

With mobile and digital media evolving so rapidly, it is crucial that attorneys for all players in the industry--from technology developers and ad networks to companies that utilize their services--understand how new technology might implicate consumer privacy.

Attorneys should advise clients to have robust, accurate privacy policies and, if possible, strong contractual indemnity protections. Before advising clients on contracts, it is important to understand not only the direct relationships but also the third-party relationships. For example, an attorney for a company contemplating a relationship with an ad network should do everything possible to understand the relationships that the ad network might have with publishers, other ad networks, technology companies, list providers, and/or cloud computing providers. Only by understanding all third-party indemnities and representations and warranties can an attorney fully understand the potential risk associated with a new mobile or digital opportunity and advise the client accordingly. Moreover, attorneys should ensure that clients dealing with sensitive personal information have sufficient protection from cyberattacks.

There is significant money to be made through successful digital media and mobile marketing campaigns, but there also is significant risk associated with all of the technologies above. It is therefore imperative that attorneys in this space advise clients to weigh privacy concerns in connection with any new digital or mobile venture.

Footnotes

a1 *Blaine Kimrey is the partner-in-charge of the Chicago office of Lathrop & Gage LLP, and Bryan Clark is an associate in the firm's Digital Privacy & Data Protection Group.*

1 Scott Thurm, *Online Trackers Rake in Funding*, WALL STREET J. (Feb. 24, 2011, 7:51 PM), http://online.wsj.com/article/SB10001424052748704657704576150191661959.

2 Amir Efrati, *Google Tool to Move Microsoft Files to Web*, WALL STREET J. (Feb. 24, 2011), http://online.wsj.com/article/SB10001424052748703775704576162491222895.

3 Gregg Blesch, *Health Net to Pay $250,000 after Conn. Data Breach*, MODERNHEALTHCARE. COM (July 6, 2010), http://

www.modernhealthcare.com/article/20100706/NEWS/307069974#.

4 *PII* refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. *PII* is defined differently in various state statutes, but it includes information such as names, Social Security numbers, financial account numbers, driver's license numbers, and health information.

5 *PHI* is defined by federal law and comprises any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

6 *See, e.g.*, CAL. CIVIL CODE 1798.29 (Deering 2005).

7 42 U.S.C. §§ 17932, *et seq.*

8 *See also* 45 C.F.R. § 164.404.

9 PONEMON INSTIT. LLC, 2011 COST OF DATA BREACH STUDY 5 (Mar. 2012).

10 *See* Press Release, Conn. Attorney Gen.'s Office, *Attorney General Announces Health Net Settlement Involving Massive Security Breach Compromising Private Medical and Financial Info* (July 6, 2010), http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754.

11 For a technical explanation of cloud computing, *see* Miranda Alfonso-Williams, *Demystifying Cloud Computing*, PRIVACY ADVISOR (Nov. 1, 2010).

12 Barry M. Benjamin & Michael J. Breslin, *The Latest Litigation Front: Behavioral Advertising*, LAW360 (Feb. 10, 2011).

13 *Id.*

14 A browser cookie is a text file, stored on Web users' computers by their browsers, that facilitates authentication, storing of site preferences and shopping cart contents, etc.

15 18 U.S.C. § 1030.

16 *See, e.g.*, Pitner v. Midstream Media Int'l, N.V., No. 10-cv-1850 (C.D. Cal. Dec. 6, 2010).

17 *See, e.g., In re* Quantcast Adver. Cookie Litig., No. 10-cv-5484 (C.D. Cal. June 13, 2011).

18 *See id.* at docket entry 5-2 (settlement agreement).

19 Scott Thurm & Yukari Iwatani Kane, *What They Know: Your Apps Are Watching You*, WALL STREET J. (Dec. 17, 2010). The entire digital privacy series, including interactive graphics, is available at http://online.wsj.com/public/page/whattheyknow-digital-privacy.html.

[20] *See* Aughenbaugh v. Ringleader, No. 10-cv-01407 (C.D. Cal. filed Sept. 16, 2010); Hillman v. Ringleader, No. 10-cv-08315 (S.D.N.Y. Mar. 28, 2011); Cooks v. Ringleader, No. 10-cv-00464 (E.D. Tex. filed Nov. 5, 2010).

[21] *See, e.g.*, Lalo v. Apple, Inc., No. 10-cv-05878 (N.D. Cal. filed Dec. 23, 2010) (lead consolidated case); Freeman v. Apple, No. 10-cv-05881 (N.D. Cal. filed Dec. 23, 2010); Rodimer v. Apple, Inc., No. 11-cv-0700 (N.D. Cal. 2011); Chiu v. Apple, Inc., No. 11-cv-0407 (N.D. Cal.).

[22] 18 U.S.C. § 1030.

[23] Wendy Davis, *Apple Sued for Violating iPhone, IPad Privacy*, MEDIAPOSTNEWS (Feb. 16, 2011), http://www.mediapost.com/publications/article/145185/apple-sued-for-violatingiphoneipad-privacy.html.

[24] 18 U.S.C. § 2701.

[25] *In re* iPhone/iPad Application Consumer Privacy Litig., No. 11-md-02250 (N.D. Cal. Sept. 20, 2011).

[26] *In re* iPhone Application Litig., 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).

[27] Wendy Davis, *Court: IP Addresses Are Not "Personally Identifiable" Information*, MEDIAPOSTNEWS (July 6, 2009), http://www.mediapost.com/publications/article/109242/.

[28] Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL STREET J. (Oct. 17, 2010, 8:33 PM), http://online.wsj.com/article/SB10001424052702304772804575558484075236.

[29] *See* Lane v. Facebook, No. 08-cv-03845 (N.D. Cal. filed Aug. 12, 2008).

[30] *See* Robins v. Spokeo, Inc., No. 10-cv-05306 (C.D. Cal. Jan. 27, 2011); Purcell v. Spokeo, Inc., No. 10-cv-03978 (N.D. Cal. filed May 27, 2011).

[31] 15 U.S.C. §§ 1681 *et seq.*

[32] 47 U.S.C. § 227.

[33] 569 F.3d 946 (9th Cir. 2009).

[34] *See* Satterfield v. Simon & Schuster, No. 06-cv-2893, at docket entry 132 (N.D. Cal.) (final judgment and order).

[35] 47 U.S.C. § 227(b); 47 C.F.R. § 64.1200(a)(1).

[36] 47 U.S.C. § 227(a).

[37] Complaint ¶ 25, Weinstein v. AIR-IT2ME, No. 06-cv-0484 (N.D. Ill. 2006).

38 2009 WL 4884471 (N.D. Ill. 2009).

39 702 F. Supp. 2d 999 (N.D. Ill. 2010).

40 121 P.3d 831, 835-36 (Ariz. Ct. App. 2005).

41 No. 06-cv-0484.

42 *Id.*

43 *Id.*

44 2007 WL 1839807 (N.D. Cal. June 26, 2007) (*Satterfield I*), *rev'd, Satterfield II*, 569 F.3d 946 (9th Cir. 2009).

45 869 N.Y.S.2d 740 (Long Beach, N.Y., City Ct. 2008).

46 Paluzzi v. mBlox, No. 07-CH-37213 (Cook County, Ill.); Parone v. m-Qube, No. 08-CH-15834 (Cook County, Ill.); *see also* Gray v. Mobile Messenger Ams., Inc., No. 08-cv-61089 (S.D. Fla.); Valdez v. Sprint Nextel Corp., No. 06-cv-7587 (N.D. Cal. filed Dec. 12, 2006); VanDyke v. Media Breakaway LLC, No. 08-cv-22131 (S.D. Fla.); Sims v. Cellco P'ship, No. 07- cv-1510 (N.D. Cal. filed Mar. 15, 2007); McFerren v. AT&T Mobility, No. 08-cv-151322 (Fulton County, Ga.).

47 The court in *Allen v. New Motion, Inc.*, No. BC386596 (L.A. County, Cal. filed Nov. 6, 2009), certified plaintiff's proposed class of "[a]ll persons throughout the United States who, from March 3, 2004 through the present, (1) subscribed to Bid4Prizes online; (2) were billed for a Bid4Prizes subscription by their cellular telephone carrier and paid for such service; and (3) who have not voluntarily submitted a bid with Bid4Prizes. Persons who received a full refund or who subscribed directly through the Bid4Prizes website are NOT included." *Id.*

48 Ashcroft v. Iqbal, 129 S. Ct. 1937 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544 (2007).

49 *See* 15 U.S.C. § 7707(b)(1).

50 47 U.S.C. § 230.

51 *See, e.g.*, Ford v. Pac. WebWorks, Inc., No. 09-cv-7867 (N.D. Ill. filed Dec. 18, 2009); Rasmussen v. Pac. WebWorks, Inc., No. 09-cv-1815 (W.D. Wash. filed Dec. 23, 2009).

52 *Iqbal*, 129 S. Ct. 1937; *Twombly*, 550 U.S. 544.

53 47 U.S.C. § 230.

54 *See* Ford v. Bloosky, 2011 WL 529265 (N.D. Ill. Feb. 4, 2011) (dismissing complaint for failure to plead with specificity).

[55] *See* Combe v. Intermark Commc'ns, Inc., No. 09-cv-9127, at docket entry 76 (C.D. Cal.) (order granting class certification).

29-NOV COMLAW 10

End of Document

92 Neb. L. Rev. 746

Nebraska Law Review
2014

Article

INTELLECTUAL PROPERTY'S LESSONS FOR INFORMATION PRIVACY

Mark Bartholomew[a1]

TABLE OF CONTENTS

*747 I. INTRODUCTION

Although most may assume the contrary,[1] absent special circumstances, individuals have no right in their personal information.[2] Today's companies routinely collect data on online consumer behavior and use that data for targeted advertising. Web sites send cookies to Web browsers that record not only our trips to the cookie-sending Web site, but also subsequent visits to all other sites in our online travels.[3] Meanwhile, Internet service providers install software directly on customer computers or, in the case of "deep-packet inspection," hardware on our routing devices that tracks the online traffic coming in and out of our homes.[4] These technologies produce rich consumer profiles revealing when, where, and who we travel with in the online world. The technologists then sell these profiles to third parties for the sole purpose of beaming back personally tailored advertisements to our computer screens.[5] Although steps are taken to keep data collected online anonymous, recent exposés reveal how easy it is to extrapolate a particular identity from a few scraps of online data.[6] Information ***748** profilers routinely fail to secure the online data they collect, potentially subjecting consumers to online threats and identity theft as personal information falls into the wrong hands.[7] Online tracking poses real dangers, but the current legal and regulatory framework is largely impotent to deal with them.

Revelation of these practices has galvanized public and political opinion.[8] A substantial majority of American consumers support greater restrictions on and penalties for use of personal information collected online.[9] Recent legislative and regulatory initiatives call for vigorous consumer protections against online data collection and marketing. The Federal Trade Commission recently requested "targeted legislation" to provide greater control over the practices of information brokers.[10] Multiple bills are pending in Congress, including legislation setting mandatory timetables for the safe disposal of collected information,[11] "Do Not Track Acts," which would allow consumers to opt ***749** out of online data collection,[12] and limitations on the solicitation and gathering of online data from children.[13] For citizens and legislators, the question is not whether steps should be taken to enhance consumer privacy, but how consumer privacy should be protected.

Despite the groundswell in favor of greater data privacy, there is a real possibility that none of these legislative initiatives will succeed. In reviewing new information privacy laws, courts will be faced with the separate question of how to balance such protections with the right to free expression. This is because a company's decision to collect our personal data, share it with others, or repackage it into advertisements can be labeled speech. Various authorities, including the United States Supreme Court, maintain that setting privacy limitations on data sharing represents a government effort to censor expression.[14] Although the party facing censorship is typically a corporation using personal information for advertising purposes, commercial speech enjoys constitutional protection[15] regardless of the corporate ***750** status of the speaker.[16] In short, laws protecting data privacy inevitably need to be reconciled with the First Amendment.[17] Under current law, judges on the alert for threats to free expression and bound by higher authority may believe they have little choice but to strangle these fledgling efforts at online privacy in their cradle.

A recent case before the Supreme Court, Sorrell v. IMS Health Inc., illustrates the problem.[18] At issue was a Vermont law restricting pharmaceutical marketers' access to and use of prescription data for advertising purposes.[19] Pharmacies sold prescribing data to the marketers, which resulted in targeted sales pitches to doctors.[20] Vermont banned the practice (with limited exceptions) unless a prescribing doctor's consent was obtained first.[21] Vermont's legislature passed the law, in part, to protect "the privacy of prescribers and prescribing information."[22] Applying "heightened judicial scrutiny" to the law,[23] the Court struck it down as an unconstitutional burden on protected speech under the First Amendment.[24]

Sorrell suggests broad recognition of the use of online information as "speech."[25] The Court condemned the First Circuit, which had upheld a similar state law, for characterizing the prescriber-identifying information at issue "as a mere 'commodity' with no greater entitlement to First Amendment protection than 'beef jerky.'"[26] Instead, the ***751** Court explained, "the creation and dissemination of information are speech within the meaning of the First Amendment."[27] Although Justices Breyer, Ginsburg, and Kagan dissented, a six-judge majority, including Justice Sotomayor, agreed that the government's effort to restrict use of personal prescribing information was an unconstitutional abridgement of speech. This suggests that a stable coalition on the Court deems the use of collected consumer information as speech protected under the First Amendment. Hence, lower courts evaluating new information privacy laws (and the legislators drafting them) will need to construe such laws as speech regulations and square them with constitutional protections for free expression.[28]

Sorrell is just one case, and it may be able to be distinguished by courts reviewing other information privacy laws.[29] Because the Vermont law forbid the use of prescription data for marketing, but not for other purposes such as "educational communications," the majority deemed the speech restriction content-based and, hence, deserving of particularly exacting First

Amendment review.[30] Another statute might be more carefully drafted. Even so, as it stands now, there is no recognizable, effective jurisprudential mechanism for reconciling information privacy with free expression.[31] The Sorrell decision offers no guidance on how to determine when a state's interest in consumer privacy is sufficiently compelling to rebuff a First Amendment challenge.[32] Before Sorrell, various privacy laws from the analog era were subjected to First Amendment review. Rather than representing a balance of two competing interests, however, the Supreme Court treated the First Amendment as an unyielding trump card for defendants. ***752** [33] Repeatedly, the Court invalidated actions for common law privacy violations on free-speech grounds.[34] Statutory privacy protections exist as well but, like their common law cousins, no clear paradigm for assessing their constitutionality has come to the fore.[35] In sum, existing privacy law offers little guidance to a court trying to balance free speech with information privacy.

As a result, judges seeking guidance need to turn to precedents outside of privacy law. As with legal restrictions on the use of online data, intellectual property law necessarily bumps up against constitutional safeguards for free expression. Intellectual property laws, just like proposed data privacy laws, prevent others from engaging in expressive activity and thereby implicate the First Amendment. Laws permitting authors to stop dissemination of infringing works, trademark holders to block unauthorized use of their brands, and celebrities to shut down traffic in their personas all proscribe speech.[36] Unlike proposed data privacy laws, intellectual property law has been on the books for decades. The result has been a raft of judicial decisions considering the proper balance of intellectual property rights and free speech.

Studying the different ways in which intellectual property law addresses expressive concerns offers a variety of models for resolving the ***753** impending conflict between data privacy and the First Amendment. Yet intellectual property's models for calibrating free-speech interests have been ignored by courts and rejected by privacy scholars. This Article remedies that failure. The Article begins in Part II by discussing the largely unexamined parallel between intellectual property law's treatment of expression-based defenses and the similar accommodations that will need to be incorporated into data privacy law. Part II also addresses potential objections to modeling privacy law on intellectual property. Although there are some important conceptual differences between intellectual property and privacy protections, these differences are outweighed by their similarities, at least when it comes to the specific issue of how to harmonize such protections with expressive freedoms.

Parts III through V delineate the doctrinal mechanisms judges have built into copyright, trademark, and publicity rights law for balancing the interests of intellectual property owners with free-speech concerns. Part III describes how intellectual property law deems particular categories of plaintiff communication to be worthy of protection and unworthy of First Amendment privileges for unauthorized users. Part IV notes how intellectual property law uses speaker intent as a proxy for First Amendment interests. Part V details specific doctrinal mechanisms used to evaluate the expressive importance of an intellectual property defendant's speech contribution. Parts III through V also describe how courts could use these mechanisms to evaluate the constitutionality of new data privacy laws. By borrowing from intellectual property, courts can respond to the current public demand for restrictions on data use while still protecting the key expressive interests at the heart of the First Amendment.

II. DEFENDING THE IP LAW/PRIVACY LAW ANALOGY

Both information privacy and intellectual property implicate the First Amendment. Restrictions on the collection and use of personal information limit speech. By declaring certain expressive activities to be infringing, intellectual property law does the same thing. Years of common law development have generated an extensive doctrinal apparatus for addressing free-speech concerns. As a result, intellectual property law offers a potential template for courts struggling to balance new data privacy laws with the Constitution's right to free expression.

Nevertheless, many legal scholars reject comparisons between intellectual property and information privacy law. Instead, they propose mobilizing another legal regime--contract law--to balance privacy and free speech concerns. Given this scholarly backdrop, this Article begins by making the case for analogizing intellectual property to data privacy. (Those already convinced of the salience of intellectual ***754** property law to data privacy issues can move ahead to Part III.) This Part explains why the similarities between intellectual property and information privacy, at least on the narrow issue of accommodating free speech, outweigh the differences. It refutes the arguments of intellectual property skeptics while also demonstrating contract law's inability to resolve the tension between data privacy and free speech.

A. Intellectual Property's Relevance to Information Privacy

Just like privacy regulation, intellectual property law often finds itself in tension with the First Amendment. Copyright, trademark, and publicity rights laws all limit communication by deeming a particular activity as infringing.[37] Hence, just as privacy regulation for online data use can be viewed as a government rule that prohibits some speech, intellectual property law awards certain rights in expression to one group while preventing others from using the same or similar expression.

While sharing data privacy's inherently speech-restrictive nature, intellectual property offers specific doctrinal accommodations for expressive interests. These accommodations possess two critical strengths, which augur in favor of their export to the information privacy context. First, intellectual property has a long history of balancing ownership rights with free speech. New privacy law protections are more likely to take root if they can be modeled on an existing area of law. Legal innovations enjoy greater acceptance if they appear based in a longstanding legal tradition.[38] Judges concerned with reversal from courts above may find more comfort in borrowing from an established area of law than by creating a new body of legal doctrine out of whole cloth.[39] As a result, drawing a parallel to intellectual property law's doctrinal accommodations for free speech may stand a better chance of success than other privacy law innovations. These accommodations boast a long pedigree, one that has typically been validated when considered by the Supreme Court.[40] Legitimacy concerns ***755** may loom especially large in the data privacy context considering that new privacy regulations will compete with the constitutionally protected right to free speech.

Second, intellectual property law is not monolithic: it addresses free speech concerns in a variety of ways. As detailed below, judges and legislators trying to accommodate free expression while addressing privacy concerns have a menu of options to choose from if they decide to borrow from intellectual-property jurisprudence. This is a strength, yet one that most privacy theorists do not acknowledge.[41] Under these options, speakers can receive immunity from infringement suits by demonstrating certain kinds of speaker intent, a particular reshaping of existing expressive content, or that the speech's subject falls into a predetermined, favored category. These defensive options offer a rich template for calibrating expressive interests, a potential improvement from the few simplistic and overly speech-protective precedents that currently set the boundary between information privacy and free expression.

B. Answering the Intellectual Property Skeptics

Despite these strengths, many scholars reject analogies between intellectual property and information privacy. The scholars' objections boil down to three concerns: differences in supply, underlying rationales, and terminology.[42]

First, some skeptics maintain that any analogy between intellectual property and data privacy is inapt because the former deals with a problem of scarcity not found with the latter. At root, intellectual property rights are justified by the natural scarcity in intellectual goods that would result if we allowed unrestrained market forces to work their will.[43] If creators lacked the ability to prevent unauthorized use of their works, they would no longer create with sufficient frequency, and information products would be in too short supply. To ***756** fix this problem, intellectual property law not only awards creators the legal right to stop unauthorized uses, but it also makes these rights freely alienable.[44]

Personal data, by contrast, is not in short supply. Instead, our online activities cause the continual generation of more and more personal information, whether we like it or not.[45] Given the ever-increasing amount of personal data revealed online, skeptics argue there is no need to grant individuals an alienable right resembling an intellectual property right to encourage the creation and dissemination of more of that data.[46]

The disjunction between intellectual property law's efforts to stimulate the creation and dissemination of new works and privacy law's contrasting efforts to restrict the flow of information should give us pause. Consumers do not need legal prompts to create more personal data because life in a wired world does this for us already. As a result, some of intellectual property law's provisions would be an ill fit for information privacy concerns.[47]

***757** Yet just because the commodity at issue in intellectual property (creative output) is naturally scarce and the commodity at issue in informational privacy (personal data) is naturally abundant does not mean that the one legal regime has nothing to tell the other. The markets for the subject of a legal entitlement may differ, but once the legal entitlement has been established, lawmakers need to decide how to construe that entitlement when it clashes with another legal protection. Even after the initial entitlement is constructed, based on its natural abundance or scarcity, defenses to that entitlement still need to be built to take competing interests into account.[48]

Moreover, these defenses must be based on more than the scarcity concerns that triggered the original entitlement. Supreme Court precedent holds that content-based government regulation of speech warrants strict constitutional scrutiny regardless of the amount of speech actually restricted.[49] The interfaces developed to balance intellectual property rights and speech incorporate a host of other normative goals--autonomy interests, fairness concerns, opportunities for democratic participation--separate from the incentive-based rationales animating much of the rest of copyright, trademark, and publicity-rights law.[50] Hence, it is the way that intellectual property law addresses defenses based on free expression, not the way this law promotes the initial creation and licensing of creative goods, that should be of most interest to privacy scholars, particularly in the wake of the Sorrell decision.

Second, some contend that intellectual property and privacy law have little to tell each other because of their different theoretical underpinnings. Intellectual property is most often justified in utilitarian terms.[51] Copyright's constitutional basis is the promotion of "useful arts," not the dignitary values of artists and inventors.[52] Similarly, modern trademark law is described instrumentally--it protects consumers from inefficient searching and encourages business investments in product quality.[53] Even the right of publicity, which blocks unauthorized commercial uses of one's persona, may be promoted as a necessary tool to encourage the creation of captivating celebrity personas.[54] In contrast, privacy regulation is typically justified in terms ***758** of personal dignity and autonomy.[55] Disclosure of personal information against one's will is often objected to because of the emotional harm it inflicts on the data subject, not because of instrumental concerns over the market for personal information.[56] As a result, some scholars suggest that importing the utilitarian intellectual property framework to privacy law is an inappropriate use of economic regulation to resolve questions of civil liberty.[57]

Again, these differences, while perhaps showing that privacy protections should not be exact replicas of intellectual property rights, do not militate against studying the way intellectual property laws negotiate the First Amendment. In actuality, the theoretical bases for intellectual property law are mixed. It is simply not accurate to argue that intellectual property's purposes are antithetical to the goals of privacy regulation.[58] Although intellectual property tends to rely more on utilitarian justifications than privacy law, it also routinely draws on personhood theories. The right of publicity is based, to a large degree, on the argument that individuals naturally have a right to control management of their personae.[59] "Labor-dessert" theory, which holds that individuals have an inherent right to enjoy the fruits of their labors, plays a large role in copyright and trademark jurisprudence.[60] For example, trademark dilution law seems largely justified by a labor-dessert view that those who build up a brand name deserve a legal shield from competing uses threatening to dim that brand's signaling power.[61] Similarly, copyright law decisions frequently invoke ***759** natural rights in assessing the scope of a particular copyright.[62] Given that many of the theoretical bases behind intellectual property mirror those advanced in favor of privacy protections, and intellectual property law has developed several mechanisms for balancing the rights of creators with the speech rights of downstream speakers, it makes sense to look for potential lessons in this area of expression-based defenses.

Finally, some object that because intellectual property law awards "property" rights to individuals, it is not a good fit for the different issues surrounding information privacy.[63] Those holding this position maintain that property rights must have explicit boundaries and that privacy is too broad of a subject to be confined within the property box.[64] Intellectual property can accommodate free speech in its particular fashion, the argument goes, because there are well-defined contours to intellectual property rights that can be pitted against expressive concerns. The same accommodations would not work for privacy regulation, however, as privacy's vague boundaries would chill an excessive amount of speech by commercial actors who cannot determine where privacy begins or ends.[65]

It is true that privacy is notoriously hard to define. Robert Post once lamented, "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all."[66] Yet, as with the other critiques, this objection should not forestall examination of the way intellectual property law balances free speech. Although it is true that the term "privacy" is subject to multiple definitions, privacy's contours become more obvious when we focus on a particular legal entitlement in personal information. This Article leaves aside the two most familiar areas of privacy regulation: the decisional privacy rights used to justify intimate personal choices like the right to elect to have an abortion and residential privacy rights that protect against government intrusions in the home. Instead, the particular question addressed here is how to balance restrictions on the collection and dissemination of online consumer data with rights in free expression. Narrowing the focus to online ***760** uses of personal information brings a potential right in data privacy into a sharper, more definable focus, thereby alleviating some concerns over the fuzzy contours of "privacy," as that term is popularly used.

In addition, we should recognize that intellectual property rights are not always known for their crystal-clear boundaries. For example, legal entitlement to copyright is dependent on a judicial determination that the work at issue is an expression rather than an idea.[67] This is a notoriously hazy distinction that can be impossible for creators to assess ex ante.[68] Similarly, the scope of someone's right in a particular trademarked term depends on judicial evaluation of the likelihood of consumer confusion, an infamously fluid and unpredictable appraisal.[69] Instead of throwing up their hands at intellectual property's vagaries, courts have stepped in to announce principles for reconciling these admittedly indefinite rights with the competing right to free expression. Hence, the argument that intellectual property has clear boundaries and, therefore, can be conceptualized as "property" while online privacy rights are unknowable and unworkable under the property rubric is unconvincing.[70] Once some protection for data privacy has been established (whether it is characterized as a "property" right or not), we are still left with the question of how to balance that protection with free speech concerns.[71]

***761 C. The Insufficiency of Contract**

One final development in the recent information privacy scholarship deserves mention. A number of legal scholars have concluded that the free-speech/privacy conflict can be best managed through private ordering.[72] Consumers that resent the liberties taken by online providers with their personal data simply need to negotiate contractual terms that will provide them greater control. Perhaps the most appealing aspect of a contractual approach is that it promises to protect privacy while avoiding First Amendment challenges. In the Supreme Court's free speech jurisprudence, there is little concern with individuals giving up their speech rights via contract. The Court has been clear: contracts not to speak are constitutional.[73] As First Amendment scholar Eugene Volokh notes, "The great free speech advantage of the contract model is that it does not endorse any right to 'stop people from speaking about me.' Rather, it endorses a right to 'stop people from violating their promises to me.'"[74]

Unfortunately, problems with the contractual approach outweigh its merits. Contract can only play a limited role in reconciling free speech with increased data privacy given the structural power imbalance between individual consumers and data users, cognitive difficulties inherent in making privacy choices, and contract law's particular legal limitations.

A close look at the dynamics of online commerce and communication reveals serious flaws in the market between data subjects and users for better privacy terms. Consumers face collective action problems in attempting to push online providers into offering more protective terms of service.[75] Part of the problem is that individual harm from data misuse is usually minimal, thereby making it unlikely that large groups of online consumers will band together to negotiate better terms of service. Moreover, data misuse often occurs without consumer awareness.[76] As a result, online entities may be concerned with their corporate reputations, but they also appear somewhat immune to public backlash over their use of personal data. For example, ***762** despite being viewed in many circles as a privacy scofflaw,[77] Facebook enjoyed a historic initial public offering, reaching a peak market capitalization of $104 billion, and currently has 1.11 billion subscribers.[78] Most online providers typically confront their data subjects with a one-size-fits-all offer: give up your personal information or forego the proffered online services.[79] Given the importance of online participation, both socially and economically in modern life, it is unrealistic to expect consumers to choose the latter option.[80]

Even without these structural barriers, consumers would still have trouble evaluating proposed privacy terms. A consumer agreeing to disclose personal information has little sense as to the universe of third parties likely to also have access to this information.[81] Consumers understand that their own disclosure might result in a particular item of data being used by the Web site they make the disclosure to. But they have no way of knowing when their personal data, perhaps voluntarily offered to one business, has been passed along to the business's other divisions or subcontractors,[82] or, even more disturbing from a privacy perspective, sold to unknown entities, which may have a very different purpose and corporate philosophy than the business to ***763** which they made the original disclosure.[83] In the ecology of the Web, thousands of unrelated Web sites all participate and share data in a single advertising network.[84] Survey evidence shows that consumers do not know that businesses track a person's entire online history as opposed to just their transactions with one particular Web site.[85] They do not realize that disclosures of data to different Web sites can be combined to develop robust profiles sometimes so precise so as to remove the cloak of consumer anonymity.[86] Most online shoppers would be shocked to discover that retailers like Target and Amazon combine myriad bits of online data from thousands of sources to identify and predict the intimate details of their customers' lives, such as their reading habits or an undisclosed pregnancy, all in an effort to make their sales pitches more effective.[87]

Greater transparency will not resolve these problems. Cognitive biases skew assessments of the costs and benefits of greater

privacy protection. Even with more disclosure of where data goes and how it is used, consumers cannot accurately assess (1) the risk of loss of personal information from participating in behavioral targeting (i.e. data breaches); and (2) the magnitude of potential harms from such a loss.[88] Optimism bias tends to cause consumers to go for the immediate reward of an online transaction rather than looking for alternatives with better privacy terms. We want more privacy but are unwilling to delay gratification in order to get it. At the same time, we minimize the costs of future harms from privacy violations.[89] Thanks to these cognitive handicaps, even highly motivated consumers accidentally trigger undesired privacy settings when they navigate online interfaces.[90] Studies demonstrate that the mere existence of a privacy ***764** policy, regardless of its actual contents, tends to increase consumer disclosure.[91]

Finally, contract law itself imposes several impediments on those seeking greater privacy protection. Contractual protections only apply to the original transacting parties.[92] Because the nature of online data collection and sharing typically involves the collection of data by one party and its use by another party, consumers relying on contract would often be left with no recourse against the actual data user.[93] Another shortcoming relates to the nature of contract damages. The majority of undesired online disclosures yield minimal, intangible harms. In the aggregate, these harms produce significant social costs,[94] but considered individually, they are harms that contract law ***765** currently refuses to recognize.[95] Hence, consumers might find themselves with a contractual right to prevent privacy violations but lacking sufficient proof of damages to actually exercise that right.[96] In addition, contractual privacy solutions still implicate free expression. Contracts designed to ensure privacy can chill speech. Parties might enter into an agreement not to disclose certain sensitive personal details, but outside disclosure of these details could also be in the public interest depending on the nature of the information and how it was to be used.[97] A contractual legal regime allowing too much restriction on the sharing of data could impoverish the discourse.[98]

Given these problems, contract law cannot resolve the tension between enhanced data privacy and free speech.[99] Instead, additional ***766** regulatory responses and doctrinal accommodations will be needed. As discussed below, intellectual property law offers different models for balancing privacy with free speech. One approach focuses on the plaintiff's speech subject. Instead of analyzing what the defendant has done with the plaintiff's materials, the court must categorize the intellectual property holder's expressive project and render a decision as to the defendant's free speech rights on that basis. Another approach focuses on the defendant's intent, using evidence of motive to divide infringing use from permissible expression. A final method assays the expressive potential of the defendant's speech, leaving questions about the defendant's intent or subject of the plaintiff's original expression largely to the side. Parts III-V investigate the soundness of each of these models and discuss how they can be implemented in a combined fashion to bridge the privacy/free speech divide.

III. FREE SPEECH AND SUBJECT MATTER

One potential starting point in weighing expressive rights against other interests is to focus on the expression's subject. The thought behind such an approach is that some subjects of communication are more critical to the goals behind the First Amendment than others. Courts trying to achieve a balance between intellectual property rights and free expression have built doctrines that weigh free speech defenses by categorizing the subject of the original communication. This Part describes these doctrines, as well as their potential application to the privacy/free speech divide.

A. Copyright's Focus on Speech Subject

To some degree, all intellectual property regimes employ free speech safeguards based on the intellectual property holder's speech subject. For example, the type of trademark held by the plaintiff is relevant to building a case for trademark infringement, which requires a showing of "likelihood of confusion."[100] Under established doctrine, those holding a more distinctive or unique mark (e.g., Apple for computers) have an easier time demonstrating infringement than those holding a less distinctive mark (e.g., eMachines for computers).[101] Hence, built in to the fabric of trademark law is a presumption against trademark protection for words considered critical to downstream expression.

***767** In a parallel manner, the type of celebrity at issue can impact the success of a right of publicity claim. The right of publicity gives individuals a right to block unauthorized commercial uses of their personas. Given the importance of celebrities to daily discourse, serious free speech concerns are raised by the right. As a result, both courts and legislatures have created defenses immunizing some journalistic uses of celebrity names or images. Some courts evaluating "newsworthiness" defenses to right of publicity claims ask whether the subject of the defendant's expression was of "public concern."[102] If so, the subject's

publicity interests must be sacrificed to the First Amendment. For example, given his prominence in popular culture, one court deemed stories of Clint Eastwood's romantic dalliances a matter of "public concern."[103] At least one state right-of-publicity law draws a distinction between appropriation of a famous personality and appropriation of a persona without commercial value.[104] Persons falling into the latter category enjoy a much more limited scope of protection and, hence, must submit to more unauthorized uses.[105]

The categorization approach is most evident in copyright law. The primary accommodations copyright law makes for free speech involve categorization of the plaintiff's work. Less attention is paid to what the defendant actually does with that plaintiff's work. When the plaintiff's communication falls into a disfavored category identified with free speech interests (ideas, raw facts, or "scenes-a-faire"), copyright's expressive defenses pack their greatest punch. When the plaintiff's communication falls into a favored subject category viewed as less essential to downstream expression (e.g., fictional works), free speech concerns recede. Copyright law does this through two particular judicial innovations: (1) the idea/expression dichotomy; and (2) the fair-use defense. According to the Supreme Court, their existence exempts ***768** copyright law from the more searching judicial review one might expect for government regulation of expression.[106]

For our purposes, two points regarding these measures bear emphasis. First, courts largely examine the kind of communication created by the plaintiff, not the defendant's use of that communication. Under the idea/expression dichotomy, an author can be awarded a property right in a particular expression (thereby preventing other speech) but not in the idea behind the expression. The thought behind this copyright principle is that ideas are too valuable to be monopolized by one party. Instead, they remain in the public domain as building blocks for other creations.[107] Courts apply the dichotomy by placing the communication that the plaintiff is trying to protect in one of two categories: "idea" or "expression."

Over time, courts have attached additional speech protective mechanisms onto the idea/expression edifice. Again, these mechanisms require categorization of the plaintiff's speech. Copyright law's merger doctrine reasons that when the plaintiff's subject matter is susceptible to only one or a limited number of possible expressions, the subject matter may not be copyrighted.[108] This is another judicial mechanism for accommodating First Amendment principles and, again, the focus is on the plaintiff's work, not the defendant's use of that work.[109]

Similarly, judges have created the scenes-a-faire doctrine, which allows others to borrow stock characters, themes, and scenic elements from a copyrighted work in order to portray a particular time and place.[110] Unlike the merger doctrine, the scenes-a-faire doctrine does not involve an expression that is impossible to separate from its underlying idea. Rather, it takes certain dramatic conventions employed by the plaintiff and removes them from copyright protection to further expressive interests.[111] For example, particular plot details in a romance ***769** novel--a husband and wife endure a miscarriage, separate, reunite, rediscover their love for each other, and, in the end, expect another child--are too "standard" in the romance novel genre to enjoy copyright protection.[112] Although judges first applied the scenes-a-faire doctrine in the context of dramatic works, they have since expanded it to protect all manner of speech, including computer code.[113] As with the idea/expression dichotomy, courts examine the plaintiff's communication to determine whether it falls into the category of an unprotectable scene-a-faire.

Copyright's fair-use defense also trains its attention on the plaintiff's speech subject. As affirmed by the Supreme Court, "the nature of the interest at stake is highly relevant to whether a given use is fair."[114] The defense requires a court to interrogate four factors:

• the purpose and character of the use;

• the nature of the original work;

• the amount and substantiality of the original work taken;

• the market harm to the original.[115]

Three of the four fair-use factors focus on what has been borrowed from the original rather than on the use made by the infringer. Hence, the second factor asks a court to examine "the nature of the original work." According to the Supreme Court, "This factor calls for recognition that some works are closer to the core of intended copyright protection than others."[116]

The third and fourth factors also require an analysis of the original communication. The third factor assesses the amount and substantiality of the original work taken.[117] For this factor, a court must analyze the substantiality of the taking from the perspective of the plaintiff's work, not the defendant's.[118] To wit, in one case applying this factor, it did not matter that the material copied from a book on sales techniques comprised only a small fraction of the ultimate work ***770** created by the defendant.[119] What was important, in evaluating the third factor, was the amount of material taken from the original.[120] As explained by the Supreme Court in an earlier case interpreting the third factor, "[A] taking may not be excused merely because it is insubstantial with respect to the infringing work."[121]

The fourth factor requires the court to determine the amount of market harm to the original. In evaluating this factor, courts inquire as to the worth of the original, as well as potential future derivative works that could be made from the original. Plaintiffs profit when they can show an effect on a market they are exploiting, thinking about exploiting, or could potentially exploit for their work.[122] External benefits to parties other than the plaintiff are not considered in the fourth factor.

This is not to say that the defendant's behavior has no bearing on copyright fair use. Some comparison of the defendant's work to the plaintiff's work is necessary to assess the third and fourth factors. Moreover, as described below, the first fair-use factor engages directly with the defendant's work itself by analyzing its "purpose and character."[123] In general, however, the fair-use analysis represents an effort to categorize the plaintiff's original communication and its importance to downstream expression. In applying factors two through four, courts scrutinize the plaintiff's work to evaluate the strength of the defendant's speech interest.

The second notable characteristic of copyright's two main expressive defenses is that they privilege the use of factual information by others. In describing the idea/expression dichotomy, courts sometimes equate ideas with "facts" or "discoveries."[124] For example, when copyright was asserted in model building codes that had been subsequently adopted by two municipalities, a Web site operator that posted the codes raised the idea/expression dichotomy as a defense to infringement.[125] The Fifth Circuit recognized the defense, holding that the codes were "facts" and, therefore, not copyrightable.[126] The ***771** justification for such a rule is to promote information exchange.[127] As explained by the Fifth Circuit, the dichotomy furthers expression "by permitting the free flow of information in facts and ideas from their emergence."[128] The Supreme Court has ratified this First Amendment privilege for facts (at least in copyright law), holding that the "fact/expression dichotomy" prevents facts alone and compilations of facts lacking originality from being copyrighted.[129]

Judges similarly privilege factual speech when evaluating a copyright defendant's fair-use defense. Free speech rights rise to the foreground when courts identify the plaintiff's work as informational, rather than a work of entertainment.[130] In analyzing the "nature of the original work" under the second fair-use factor, judges shield unauthorized use of factual works while being less willing to recognize a fair-use defense for use of fictional creations.[131] Much turns on whether the original work is considered "factual" or "creative."[132] A copyright infringement suit against the compiler of an unauthorized Harry Potter reference guide illustrates the point. In rejecting the compiler's fair-use defense, the court explained that the "creative nature" of the original Harry Potter books tipped the balance in favor of their author.[133] Once it had identified the nonfactual nature of the original communication, the court could downplay the defendant's free speech interests. On the other hand, an unauthorized biographer of L. Ron Hubbard won his fair-use defense, in part, because the biography's original sources were deemed factual.[134] The biographer quoted extensively, without permission, from Hubbard's writings.[135] Yet because the quoted works dealt "with Hubbard's life, his views on religion, human relations, the Church, etc.," the court concluded that they were "factual or informational," thereby favoring the defendant on the second fair-use factor.[136]

***772 B. Categorization and Information Privacy**

In sum, copyright's idea/expression dichotomy and fair-use defense focus on the original work to determine whether its protection via copyright represents a threat to free expression. Creative activity that is particularly necessary as raw material for other creative output, like "facts," "scenes-a-faire," or highly informational works, is singled out as inappropriate for copyright protection. Applying a similar method to information privacy would focus attention on the particular data meant to be safeguarded, not on how or why that data was used by the defendant. Courts would need to identify ex ante species of data that should and should not be available for use by others.

This categorical approach makes some sense and should be utilized by courts evaluating First Amendment challenges to information privacy laws. In many ways, privacy law already operates under a categorical approach. Just as the objective in

copyright is to identify communicative materials that are necessary for downstream creation, the goal for privacy law is to identify personal data that is particularly sensitive or intimate.[137] Both common law and statutory privacy protections attempt to pinpoint types of personal information that are highly sensitive and attach limits to their collection, use, and dissemination by others. The common law tort for public disclosure of private facts prevents public use of personal information if the information publicized "would be highly offensive to a reasonable person" and is not of public concern.[138] Similarly, existing data privacy statutes target discrete, sensitive information like medical histories and financial records for heightened regulation in the interest of consumer protection.[139]

As currently employed by the courts, the categorical approach to information privacy seems to adequately safeguard restrictions on the use of especially sensitive personal information from First Amendment ***773** challenges. An illustrative example is credit-report regulation. Even after accepting that records of consumer credit performance constitute "speech," courts have applied only intermediate scrutiny to laws restricting the use of such records and held in favor of government regulators.[140] For example, a privacy statute preventing a credit-reporting agency's sale of targeted marketing lists survived a First Amendment challenge.[141] In deciding that the privacy interest in one's credit information outweighs free speech interests, the courts have highlighted two characteristics of the data at issue. First, credit-report information is tailored to individual consumers. As a result, it is not a subject of "public concern" and, therefore, is considered less essential to free expression.[142] Second, credit-report information is personally sensitive.[143] Significant harm to the individual can result from one unwanted disclosure. In the credit-report cases, First Amendment concerns appropriately receded once the data's private, sensitive nature was identified.[144] The decisions in the credit-report cases appear to match public sentiment for keeping certain personal data private and restricting outside speech that uses such data. One can envision similar results when it comes to upholding limits on the use of personal data involving health or sexuality.[145]

Exclusive reliance on the categorical approach would be a mistake, however. A solitary focus on the plaintiff's communication would ***774** come at a cost for consumers. Take, for example, copyright law's general willingness, both through the idea/expression dichotomy and the fair-use defense, to privilege unauthorized uses of factual information. While there may be reasons for such a policy in copyright law, when it comes to privacy law, a similar free ride for use of factual data makes little sense. Use of personal information, even when not of a sexual or financial nature, can cause real harms. Instrumentally, this information can be aggregated to unmask consumers, revealing things they wished to keep secret,[146] as well as to track the online behavior of children.[147] Moreover, the mere perception of being surveilled by others produces psychic harm.[148] These concerns over the collection and use of quotidian, everyday data motivate current legislative proposals like "Do Not Track" acts and restrictions on the use of "like" buttons on Web sites targeting minors.[149] These proposed laws would prevent some types of factual speech. Copyright's categorical willingness to immunize fact-based speech, if exported to the data-privacy context, would stymie these laws and allow these harms to continue.

The copyright approach to free speech and factual data also clashes with an unacknowledged judicial intuition toward speech involving truthful, factual details. When confronted with First Amendment challenges to the regulation of such speech (as opposed to laws affecting more abstract literary, artistic, or ideological speech), courts have bent constitutional doctrine to justify government regulation of such speech. In describing this phenomenon, Ashutosh Bhagwat maintains that these decisions make sense because speech involving factual details can threaten greater social harm than other types of expression while simultaneously being less necessary to listener self-governance.[150] For example, in Planned Parenthood of the Columbia/Willamette, Inc. v. American Coalition of Life Activists,[151] the Ninth Circuit affirmed a lower court's decision to issue an injunction shutting down an abortion protest Web site listing the names and home addresses of current abortion providers, as well as the names of abortion providers that had been killed or wounded.[152] It justified this ***775** decision by characterizing the Web site as a "true threat,"[153] even though the Web site clearly did not meet the "true threat" standard.[154] Yet one can understand why the Ninth Circuit rejected the anti-abortion activists' First Amendment defense. Given the potential harm unleashed from the Web site's specific disclosure of abortion provider addresses, and the arguable irrelevance of those addresses to any rational conception of self-governance, free speech interests seem less important and privacy concerns more relevant. Depending on context, factual data sometimes needs to be deemed less important to expressive needs, not more important.

The ultimate problem with an exclusively categorical approach is that it omits other concerns that are critical to reconciling privacy interests with free speech. Although information relating to sexual habits and financial disclosures appears to be firmly within information privacy expectations, this is not the sort of information that is valued by data aggregators.[155] Instead, today's advertisers prize the information gleaned from everyday online revelations. But there can be strong privacy interests in what

appears, in the abstract, to be relatively innocuous information. For example, addresses are normally considered public information and not subject to privacy restrictions. But addresses can become extremely private depending on the circumstances of their revelation, particularly when revealed to others who could potentially do the subject harm. When the anti-abortion protestors in the Planned Parenthood case revealed the names and addresses of abortion providers, their speech posed dangers deserving of constitutional recognition. Context matters. For this reason, a focus on the data rather than the activities of the data user is a good start but an incomplete solution for the divide between privacy and free speech.

IV. INTENT

Another way to reconcile free speech with privacy is to look to the intent behind the speaker's expression. For all three intellectual property regimes analyzed in this Article, the speaker's mental state plays a role in calibrating First Amendment interests. Inquiries into bad faith and commercial motivation represent explicit and central parts ***776** of the doctrinal balance between intangible property rights and the right to free expression. The experience of intellectual property law suggests that evidence of intent should play an important, yet limited, role in judicial analysis of First Amendment challenges to data privacy laws.

A. Improper Motive and Free Speech

The motivations relevant to calibrating intellectual property rights with free speech can be divided into two broad areas: "bad faith" and "commercial motivation." Considerations of bad faith can be found in expression-based defenses for all three of the intellectual property regimes discussed in this Article. Courts have probed user bad faith when construing copyright's fair-use defense,[156] and defendant "good faith" has been referenced in cases evaluating First Amendment defenses to right-of-publicity claims.[157] Yet bad faith has greatest salience when considering expression-based defenses in trademark law.

To state a claim for trademark infringement, a plaintiff must allege facts demonstrating ownership of a valid trademark and use of that mark by the defendant in a way that is likely to confuse consumers.[158] Even if the plaintiff carries his or her burden of proof as to these two elements, a defendant may escape liability through two judicially created "fair use" defenses: descriptive and nominative fair use. These defenses provide some important breathing room for free expression even when that expression could potentially confuse some consumers.[159] Descriptive fair use exempts unauthorized mark uses that accurately describe a defendant's product. Hence, even though a food products manufacturer held trademark rights in the term "Fish-Fri," a rival manufacturer could also use the term to describe its own batter mix for frying fish.[160] Nominative fair use applies when a defendant uses a mark not to brand its own product but to identify the plaintiff's product. For example, when a newspaper used the trademarked term "Boston Marathon" to report on the famous race, it satisfied the nominative fair-use defense.[161] The newspaper was allowed ***777** to use the trademark because it used the mark to identify the race, not to market a race of its own.[162]

As articulated by the courts (and, in the case of descriptive fair use, also by statute), both of these defenses require an evaluation of the defendant's mindset and are unavailable to those judged to be acting with improper motives. In evaluating the descriptive fair-use defense, courts are statutorily required to look to whether the defendant used the mark "in good faith."[163] Nominative fair use, a strictly common law construction, is similar. The Third Circuit states that the nominative fair-use test requires an examination of "the intent of the defendant in adopting the mark,"[164] adding that "[i] t is the circumstance in which a court does not find bad intent but does find confusion that a nominative fair use defense will be most useful."[165] In a similar vein, the Ninth Circuit requires an analysis of whether the defendant used "only so much of the mark . . . as is reasonably necessary to identify the products or services,"[166] an inquiry that some describe as synonymous with investigating the defendant's intent.[167] As characterized by one federal appellate judge, "the entire 'nominative fair use' defense asks whether the use was made with the intent to confuse."[168]

A different inquiry into speaker mental state asks not whether the defendant acted in bad faith, but rather whether she was commercially motivated. If so, free speech interests are deemed less pressing and the rights of the intellectual property holder tend to take precedence. Again, this type of mental-state inquiry is common to copyright, trademark, and right-of-publicity law.

In copyright, the first factor of the fair-use defense explicitly requires courts to consider "the purpose and character of the use, including whether such use is of a commercial nature."[169] Some courts have described the first factor as an inquiry into

commercial motive.[170] Unauthorized use of copyrighted material in an advertising context is particularly frowned upon since the advertiser's primary intent in using ***778** the work seems to be to sell a product.[171] This holds true even if the plaintiff's original communication was also intended to sell a product.[172] Evidence of commercial motivation may negate a defendant's other, more laudatory reasons for using copyrighted material. For example, despite its journalistic importance, an unauthorized re-broadcast of copyrighted footage of the beating of truck driver Reginald Denny during the 1992 Los Angeles riots on a television newscast was deemed not to be fair use given a finding that the newscaster was motivated by profit.[173]

On the other hand, noncommercial motivations are looked on favorably. In one seminal copyright fair-use analysis, the Supreme Court determined that when individual users of video recording devices made unauthorized copies of copyrighted television programs for the noncommercial purpose of privately watching their favorite shows at a more convenient time, such activity was fair use.[174] Central to the Court's determination was its perception that the users lacked a "commercial motivation" in making their unauthorized copies.[175]

In a similar fashion, some courts place great weight on commercial motivations in deciding what should triumph--a celebrity's right of publicity or an unauthorized user's free speech interests. For example, courts in Missouri employ a "predominant purpose test," which asks whether the motivation behind the use of a person's identity is commercial exploitation or expressive activity.[176] If the predominant purpose is commercial exploitation, then the defendant's First Amendment defense fails. In the main case setting out this test, the court relied on evidence that the defendant, a comic book publisher, used a professional hockey player's persona in its Spawn comic books to induce hockey fans to purchase its comics.[177] This evidence led the court to conclude that the use of the hockey player's persona was predominantly a "ploy" to sell comic books, and the court, therefore, found in favor of the hockey player.[178] In other words, the publisher's commercial motivation negated a potential First Amendment defense. Outside of Missouri, other courts have used commercial intent to ***779** downplay the First Amendment interests of right-of-publicity defendants.[179]

Trademark law also scrutinizes commercial motives. In addition to the descriptive and nominative fair-use tests, trademark law's third major initiative to safeguard expressive activity, the Rogers test, asks whether use of the plaintiff's trademark is (1) "artistic[ally] relevant" to the defendant's work; and (2) whether use of the plaintiff's trademark is "explicitly misleading."[180] If the court answers yes to the first question and no to the second, the defendant escapes liability. Even more so than trademark's two fair-use defenses, the Rogers test has the potential to immunize a great deal of expressive activity from trademark infringement claims. Overall, courts have interpreted its two prongs in a defendant-friendly manner, adopting a broad view of what is artistically relevant[181] and ensuring that the "explicitly misleading" standard puts the plaintiff to a higher burden of proof than the standard likelihood of confusion analysis.[182] Yet courts also posit that only noncommercial expression is eligible for the Rogers safe harbor.[183] Hence, it is of enormous importance for defendants seeking the protection of Rogers to convince the court that their trademark use was not commercial.

Often, the commerciality question is determined by reference to the defendant's intent.[184] For example, the Third Circuit rejected a ***780** Rogers defense advanced by the National Football League (NFL) when it used, without authorization, the voice of legendary sports announcer John Facenda in its twenty-two minute film The Making of Madden NFL 06.[185] Facenda's estate sued for false endorsement, contending that fans hearing his voice on the film would assume that he had lent his approval to the film and the videogame it was describing, John Madden Football.[186] The NFL maintained its periodic use of Facenda's voice represented an artistic choice for a documentary film, not an effort to confuse consumers.[187] The court rejected this argument, explaining that the NFL's "economic motivation" rendered the film commercial speech.[188] Because no one in the film had anything negative to say about the videogame, the court did not believe the film had a "documentary purpose."[189] The court found that the film was only meant to serve as an advertisement for the Madden videogame.[190] As a result, the use was commercially motivated, and the NFL could not take advantage of the Rogers defense.[191]

The Ninth Circuit performed a similar analysis when Vanna White sued for the unauthorized use of her persona in a print advertisement for Samsung VCRs.[192] White sued under the same trademark cause of action used by Facenda's estate.[193] Samsung responded to White's suit with a free speech defense based on parody.[194] The use in question featured only a robot dressed in a gown, pearls, and blonde wig standing next to the Wheel of Fortune letterboard above the caption: "Longest-running game show, 2012 A.D."[195] The court accepted White's claim that consumers viewing the ad would mistakenly think she had endorsed Samsung's product.[196] It then brusquely rejected Samsung's free speech argument, explaining that trademark law's potential ***781** for censoring advertising presented no First Amendment concerns.[197] Even if Samsung meant to spoof the famous letter turner, perhaps making fun of Ms. White's longevity and robotic demeanor, the court

found it potentially dispositive that Samsung also meant to confuse consumers regarding White's endorsement.[198] Ultimately, the court's decision hinged on its belief that Samsung intended the commercial as an advertisement.[199] Once it decided that Samsung primarily intended a "knock-off," not a "parody," it was able to ignore the free speech implications of a judgment in White's favor.[200]

B. Information Privacy and Proscribed Motivations

The discussion above reveals that one method for balancing societal interests with expressive rights is to scrutinize speaker motivations. Intellectual property law, particularly trademark doctrine, hinges the success of its expression-based defenses on showings of speaker "good faith" and noncommercial motive. This method attempts to protect First Amendment values by only restricting speech made with the wrong intentions.

To many First Amendment scholars, however, it is unclear why a speaker's motive should ever matter, particularly when primary consideration is given to the First Amendment interests of listeners.[201] If First Amendment interests are meant to turn on the value or harm of the speech to others, the speaker's state of mind should be disregarded.[202] The motivations of communicators seem largely irrelevant if the First Amendment is meant to facilitate the search for truth or provide information for democratic self-governance.[203]

Nevertheless, as in intellectual property law, intent should have some role in assessing information privacy's First Amendment boundaries. ***782** There are three main reasons for using intent to assess the constitutionality of data privacy laws. First, from a practical perspective, judges can easily incorporate an analysis of intent into their larger consideration of the constitutionality of information privacy laws. Many other areas of the law focus on evidence of mental state, including some pockets of First Amendment jurisprudence.[204] From criminal law to tort law, judges routinely must assess a defendant's inner thoughts in order to determine whether there has been a legal violation. Hence, there is a level of judicial comfort with examinations of intent. As mentioned, a doctrinal innovation is more likely to take root if it resembles other, more firmly established legal standards.[205]

Second, and more importantly, some consideration of intent makes sense when other values behind the First Amendment are considered. When speaker interests are taken into account, intent's relevance becomes clearer. Much of First Amendment law is justified by reference to speaker autonomy.[206] Leslie Kendrick writes persuasively that it is improper to hold speakers strictly liable for speech-related harms precisely because of these autonomy concerns.[207] A legal regime that did nothing to acknowledge speaker mental state would not show a proper regard for speaker interests in being able to freely and openly communicate.[208]

Third, some consideration of intent is necessary when punishing speech to avoid undesirable chilling effects. Strict liability for speech-related acts potentially stifles expression. By requiring some evidence of a culpable mental state before holding a speaker liable, the law provides ***783** notice to those whose speech may cause sanctionable harms and offers breathing space to those who (even if misguidedly) wish to speak out of noble intentions.[209] Thus, when evaluating a data user's First Amendment defense, some consideration should be paid to the motivations guiding their data use.

These arguments have not gone unnoticed by some information privacy scholars. In assessing First Amendment limits on information-privacy protections, they recommend greater attention to speaker interests and speaker mental state (and less of a focus on the category of personal information used by the speaker).[210] For example, Jane Bambauer calls for an invigoration of the common law tort against "intrusion upon seclusion" to address modern privacy concerns.[211] Under Bambauer's conception of the tort, certain observations of human activities would be prohibited if the observation "incorporates a sufficient amount of intent."[212] Part of this approach would require scrutiny of the reasons behind the defendant's use.[213] Similarly, Daniel Solove urges courts to resolve the privacy/free expression boundary by adopting a more contextual approach.[214] He contends that by going beyond study of the data itself and determining which motivations for secondary data use are acceptable and which should prevent application of a First Amendment defense, privacy law could more effectively address consumer injury.[215]

Ultimately, intent's role in representing speaker interests makes it a necessary part of balancing information privacy with free speech. But, for two main reasons, intent should not be a deciding factor in most cases and its consideration should be closely cabined. First, strenuous reliance on defendant intent offers little information for potential litigants. Requiring courts to address the data privacy/free speech balance by focusing exclusively on defendant motivation could yield unintended consequences.[216] Although courts may be comfortable ***784** intuiting a defendant's mental state, motive is hard for parties to assess in advance of

litigation. In the trademark context, courts have given themselves wide latitude in determining bad faith.[217] The Second Circuit explains that "any evidence that is probative of intent to trade on the protected mark would be relevant to the good faith inquiry" necessary to show descriptive fair use.[218] Proof of intent to confuse consumers surely seems relevant to this inquiry, but courts sometimes construe bad faith more broadly and seize on any behavior that seems to transgress standard commercial practice. For example, a defendant's decision not to purchase a readily available license to use the trademarked song title "Sing, Sing, Sing" meant that it could not defend its use of the term "Swing, Swing, Swing" to sell golf clubs as fair use.[219] In another case, the court highlighted the "hidden" nature of metatag use of trademarks in rejecting a nominative fair-use defense for such behavior.[220] Trademark holders suing for infringement and defendants seeking the safe harbors of descriptive or nominative fair use can find themselves on uncertain ground, not knowing how a court will elect to interpret "bad faith."

It is not only that "bad faith" is an amorphous category. Inquiries into motive are inherently messy.[221] Privacy scholars attempt to give content to an information-privacy mental-state requirement by using words like "deliberate," "obnoxious," and "a sufficient amount of intent," and contend that these terms will be concretized over years of common law development.[222] But these words seem plagued with the same inherent opacity as "bad faith."

Second, limiting the regulation of online data usage to acts done in "bad faith" could short circuit regulatory efforts. Such proof could be simply too hard for plaintiffs to come by and result in inevitable First Amendment victories for data collectors and users. History shows that intent requirements can sap the effectiveness of once promising legal innovations, particularly when it comes to calibrating privacy and free speech. One need look no further than the unrealized potential of longstanding common law privacy torts. Although states are divided on this issue, the general trend is for common law private disclosure ***785** claims to require proof of intent; negligent disclosures are insufficient to trigger liability.[223] Intrusion upon seclusion claims also require intent.[224] There is wide agreement that by requiring proof of intentional conduct, courts have eviscerated these causes of action.[225] On the whole, plaintiffs simply cannot come up with, or lack the financial will to try to locate, sufficient evidence of intent to prosecute these actions. A similar emphasis on intent in balancing new data privacy protections with free speech concerns might produce parallel results, in effect immunizing all data uses that are not obviously committed in "bad faith." The result would be a new round of measures designed to safeguard privacy interests that would founder on the rock of too-stringent mental-state requirements.

The better course is to presume that commercially motivated uses of personal data deserve less First Amendment protection than most other types of data usage. Apart from this presumption, speaker intent should be relevant only in exceptional cases. First Amendment claims for commercially motivated use of data should be greeted more skeptically than noncommercial ones. For example, in the Sorrell case,[226] the use of prescribing data to market brand-name drugs to physicians was commercially motivated and, hence, should have triggered a lower tier of First Amendment review. This would have happened if the Sorrell court had assessed First Amendment interests in the same manner as intellectual property law. For example, under trademark doctrine, evidence of the speaker's commercial motive causes courts to downplay First Amendment interests (in the form of the Rogers test).[227] Employing commercial motive in this fashion makes some sense given the Supreme Court's commercial speech doctrine (ignored in Sorrell), which singles out speech made to propose a commercial transaction for a lesser brand of First Amendment review.[228] It also follows intellectual property law's longstanding precedent-- whether through the right of publicity's predominant purpose test, the first factor of copyright fair use, or application of trademark's Rogers test--of downgrading First Amendment arguments made by commercially motivated speakers.[229]

***786** Apart from consideration of commercial intent, courts and legislators should limit the number of proscribed motivations eligible for consideration. A generalized inquiry into "bad faith" should be avoided. Instead, to avoid some of the problems that have plagued both trademark's fair-use defenses and the common law privacy torts, unacceptable motivations for data collection should be specifically described in new information privacy statutes. One could envision proof of intent to defraud consumers automatically invalidating a data user's free speech argument. Perhaps exceptions for collection and use of personal data motivated by scientific research or law enforcement purposes could be written into the new data-privacy laws. Outside of these clearly delineated boundaries, however, speaker motivation should not control when weighing information privacy against free speech.[230] Instead, a third consideration needs to be added to the mix.

V. ASSESSING THE DEFENDANT'S SPEECH CONTRIBUTION

Thus far, we have considered two potential mechanisms for calibrating privacy with free speech. One trains its attention on the subject of the speech, i.e., the plaintiff's original communicative contribution. Another scrutinizes the defendant's motives. A

third approach examines the defendant's activity, not for evidence of bad faith or commercial motivation, but to assess the defendant's contribution to public discourse. This approach is particularly prevalent in cases addressing First Amendment challenges to the right of publicity. Judicially devised doctrinal defenses evaluate the defendant's speech contribution and determine free speech interests on that basis. Similar measures, considered in conjunction with the first two approaches, could offer a more balanced means for calibrating data privacy with free speech, one that would uphold the constitutionality of tailored limitations on the collection and use of online personal data.

A. IP's Formalized Mechanisms for Assessing New Expression

All three intellectual property regimes, at times, scrutinize the defendant's speech contribution to determine whether the property right at issue should yield to First Amendment interests. Trademark courts sometimes engage in an ad hoc balancing test designed to safeguard a defendant's valuable expressive activities. In this test, a court scrutinizes the manner in which the defendant uses the plaintiff's trademark. ***787** [231] If it is recognized from the outset that the defendant is using the plaintiff's mark in a socially valuable, expressive way, the court will apply that understanding to the multifactor likelihood-of-confusion test.[232] One commentator describes this as "putting a discrete judicial finger on the scales in favor of the defendant."[233] This approach has been used to protect the unauthorized use of trademarks for purposes of parody and political speech.[234]

The right of publicity and copyright law adopt similar but much more formalized approaches. By potentially allowing celebrities and authors to block downstream expression, the right of publicity and copyright threaten new speech. In assessing this threat, courts have articulated two defenses meant to balance intellectual property interests with the First Amendment: transformativeness and newsworthiness.

1. Transformativeness

In assessing a First Amendment defense to a celebrity's charge of publicity-rights infringement, courts examine the "transformativeness" of the defendant's expressive activity. This is an independent and absolute defense to a prima facie violation of the right of publicity. First articulated over a decade ago by the California Supreme Court in Comedy III Productions v. Saderup:

[The transformativeness] inquiry is whether the celebrity likeness is one of the raw materials from which an original work is synthesized, or whether the depiction or imitation of the celebrity is the very sum and substance of the work in question.[235]

This is a broad standard for First Amendment immunity from suit. The Saderup court was careful to note that "transformative" contributions could take a wide range of forms and should not be limited to types of speech already well-recognized under the First Amendment, such as parody.[236] Under the transformativeness analysis, unauthorized use of the persona in a new context or to make an unexpected expressive point is protected speech.[237]

***788** The transformativeness standard is best understood in contrast to the previous mechanisms discussed for balancing intellectual property rights with free expression. In assessing transformativeness, a court analyzes the defendant's expressive project, not the type of expression first created by the plaintiff. This approach emphasizes the defendant's contribution to public discourse, not the legal entitlement held by the plaintiff. For example, when right-of-publicity defendants have appropriated celebrity personas and turned them into video game avatars, the courts have looked to the degree of change to the persona. When Sega took singer Kieran Kirby's likeness but also contributed a dissimilar physique, different costumes, and portrayed her as a twenty-fifth-century news reporter, the court concluded that a "transformation" had taken place.[238] On the other hand, when video game manufacturers import college athletes into their games without somehow altering their appearance or expected role, transformation has not been found and the defendant's First Amendment argument fails.[239]

The transformativeness inquiry ignores considerations of intent. For example, when DC Comics published two comic books featuring characters with names and physical features similar to two real-life musicians, rockers Johnny and Edgar Winter, the Winters sued for violation of their right of publicity.[240] DC Comics asserted a First Amendment defense.[241] In response, the Winters maintained that the comic book manufacturer had intentionally borrowed their likenesses to generate interest and stimulate sales.[242] The California Supreme Court explained that, in evaluating whether DC Comics' use was transformative and, consequently, protected under the First Amendment, such evidence of intent was "irrelevant."[243] "The question is whether the work is transformative," the Court noted, "not how it is marketed."[244] Similarly, when a video game manufacturer used the name

and most popular song of the rock band The Romantics without ***789** permission, the determinative issue was the manufacturer's addition of "numerous creative elements," not the manufacturer's intent to trade on The Romantics' popularity.[245]

Transformativeness is also a consideration in copyright fair use and, as with the right of publicity, it requires an assessment of the defendant's speech contribution. Unlike the other three copyright fair-use factors, the first factor engages with the defendant's appropriation by inquiring into its "purpose and character." In considering the first factor, courts will inquire as to whether the defendant's use was "transformative." Copyright's transformation analysis has been used to immunize a broad array of unauthorized uses of copyrighted materials, particularly when those uses serve an entirely new purpose from the original. For example, the Google search engine's unauthorized creation of "thumbnail" copies--reduced, lower-resolution versions of the copyrighted, full-sized images featured on third-party Web sites--to create a searchable index was considered transformative and, therefore, fair use.[246] So was an artist's unauthorized use of a photographer's "serene," black and white, naturalistic photographs of human subjects for a "crude and jarring" collage that incorporated color and distortion.[247] On the other hand, unauthorized uses that do not employ the original work for a new purpose will not be deemed transformative. For example, the unauthorized photocopying of scientific journal articles for use in laboratories was not considered transformative and, therefore, did not constitute fair use.[248] The Second Circuit concluded such copying is disfavored under the first factor, even if undertaken for "archival" purposes, because it "merely supersedes the objects of the original creation."[249]

2. Newsworthiness

In addition to the transformativeness defense, courts have created an alternative standard for reconciling the right of publicity with free speech interests. A newsworthiness defense exempts journalistic uses of celebrity, even when the journalism at issue consists only of mundane ***790** celebrity gossip.[250] (Newsworthiness is not a consideration under copyright fair use.[251]) Courts adjudicating California law have described this inquiry in an open-ended fashion, characterizing the analysis as whether the defendant's work "concerns a matter of public interest."[252] Although one court has attempted to limit the definition of public interest,[253] others hold that even works of entertainment receive constitutional protection under the newsworthiness exception if they fulfill an "informative role."[254]

As with the transformativeness defense, the newsworthiness defense focuses on the nature of the defendant's contribution, not the character of the interest held by the plaintiff. The exemption applies to any use of celebrity personae in a presentation deemed to be "news."[255] In this context, "news" has been defined generously, applying to much more than just conventional news sources and covering much more than political journalism.[256] Courts have also been generous in determining which personas can be newsworthy, even suggesting in a recent case that "liking" something on Facebook is "newsworthy" to the user's circle of Facebook friends.[257] By defining "news" in such a broad manner, courts train their First Amendment analysis on the defendant's use of the celebrity material rather than on the type of subject matter that the celebrity plaintiff is claiming an interest in.

***791** Also like the transformativeness defense, in determining newsworthiness, the motive of the journalist/defendant is not a consideration. As explained by one court:

[T]he fact that a publication may have used a person's name or likeness solely or primarily to increase the circulation of a newsworthy article--and thus to increase profits--does not mean that the name or likeness has been used for trade purposes within the meaning of the statute . . . .Whether an item is newsworthy depends solely on the content of the article--not the publisher's motive to increase circulation.[258]

This can hold true even if the defendant obviously employed the plaintiff's persona for a commercial purpose. For example, when the San Jose Mercury News took quarterback Joe Montana's likeness not only for its front page, but also to sell commemorative posters, the court immunized the use under the newsworthiness exception.[259]

B. Evaluating the Speech Contributions of Data Users

Both the transformativeness and newsworthiness defenses focus on the defendant's expressive project. Adapting these defenses to information privacy law would represent a major legal innovation. As stated above, when the First Amendment and privacy protections conflict, courts currently look to categorize the information at issue instead of examining the context in which that

information is being used.[260] For the most part, this has resulted in First Amendment immunity for those using information others wish to keep private.[261]

The right of publicity's focus on the defendant's speech contribution offers a critical missing ingredient for addressing the constitutionality of new information privacy laws. Perhaps publicity rights law has so much to offer in the data privacy context because of its own origin as a type of quasi-privacy interest.[262] By itself, merely categorizing the plaintiff's communication fails to engage with the real harms of data privacy. Similarly, exclusive or undue emphasis on the defendant's mental state could lead to unpredictable results, potentially immunizing virtually all third-party data usage from regulation. Although analyses of speech categories and speaker intent have their place in reconciling privacy with free expression, the transformation and newsworthiness tests offer a much-needed additional component to any such reconciliation. The tests provide a richer, normative framework for courts that allows for consideration of important, yet ***792** heretofore neglected, interests. In short, they present a better opportunity for balance.

The transformativeness and newsworthiness tests have two particular qualities that recommend their application in the data-privacy context. The first is their track record of actually balancing free speech concerns with other societal interests, instead of simply demanding an overriding deference to the First Amendment. One criticism of existing privacy torts is that they are conceptualized at a level of individual injury.[263] As a result, any court weighing that individual injury against the broader societal interest in free speech will always find the latter more compelling.[264] Commentators argue that this has unfairly doomed the privacy torts to failure.[265] For example, the common law tort for revealing private facts has largely been read out of existence by courts concerned with safeguarding the expressive output of the press. A media defendant invoking the larger social interest in free expression will always trump the single plaintiff complaining about violation of her individual privacy.[266]

This has not been the case, however, with the publicity-rights tort. In determining whether the newsworthiness defense is satisfied, courts have noted potential consequences not only for audiences for celebrity speech but also to the incentives necessary for creative presences like actors and musicians to function. Rather than simply asking if the defendant's expression is "news," the courts undertake a larger inquiry into whether the defendant's use of the celebrity persona represents a real counterpoint to the celebrity voice. Hence, the newsworthiness defense has been upheld when the speech at issue represents some sort of news reporting[267] or "editorial opinion,"[268] but it has been disallowed when the defendant's expression was designed to sell rather than inform.[269]

Second, by focusing on the defendant's speech contribution, the transformativeness and newsworthiness defenses allow for the consideration of multiple normative frames, including the autonomy interests of both listeners and speakers and the fairness concerns of consumers. Some have noted that the Sorrell decision is rooted in a single First Amendment perspective--one that views the market for ***793** online speech as controlled by equally autonomous actors.[270] Under what Shubha Ghosh labels the "classic liberal perspective," the Sorrell Court viewed doctors, pharmaceutical marketers, and consumers as all equally capable of making informed decisions regardless of the marketers' ability to use prescribing information to generate individually tailored commercial appeals. Under the liberal perspective, data-collecting businesses pose no threat to consumers because government actors can alert consumers to undesirable data collection practices, and consumers can simply opt out of such practices. As a result, there is little need for legal safeguards against data collection and use.

In contrast to the Court's approach in Sorrell, in applying the transformativeness test, courts have demonstrated a nuanced recognition of the tradeoffs between free speech and other social interests. The expansive nature of the transformativeness test has encouraged courts to engage with free speech issues on multiple normative fronts. Rather than being limited to the liberal perspective, another First Amendment perspective, personal autonomy, is front and center in these discussions. For example, in evaluating the "transformativeness" of an unauthorized painting of Tiger Woods, the Sixth Circuit noted not only the First Amendment's goal of advancing knowledge through "a free marketplace of ideas," but also its "fulfillment of the human need for self-expression," an autonomy interest.[271] Similarly, when a federal court recently had to determine the duration of publicity rights under New Jersey common law, a decision with direct implications for free speech, it noted that one of the rationales for recognizing a right of publicity remains its protection of "an individual's interest in personal dignity and autonomy."[272] The plaintiff was the purported beneficiary of Albert Einstein's publicity rights under his will.[273] The defendant, an advertiser that used Einstein's image without permission, contended that whatever rights the beneficiary held, they were no longer valid since Einstein had been dead for more than fifty years.[274] Ultimately, the court denied the plaintiff's request for a right of longer duration, explaining that "the personal interest that is at stake becomes attenuated after the personality dies."[275] Hence, the court adopted an autonomy perspective, calibrating the temporal length of the right according to one's personal interest in

self-fulfillment.

***794** Courts have also evaluated the free speech/publicity rights balance from a fairness perspective, assessing the power dynamics of the different speakers and audiences involved. The Sorrell decision suggested that the only remedy for problematic speech (like individualized marketing based on pharmacy prescription data) is more speech, regardless of the costs to patients, prescribing doctors, or the Vermont health care system.[276] The right of publicity's transformativeness test does not assume, however, that more speech is a cure all for any speech with socially deleterious consequences. Instead, it asks whether the speaker is truly making an expressive contribution. If not, the speaker loses First Amendment protection because it is not actually providing a competing voice. For example, when the Tenth Circuit had to decide whether right-of-publicity claims brought by major league baseball players for the unauthorized use of their names and likenesses on parody baseball cards should yield to the First Amendment, it determined whether the cards were transformative.[277] In doing so, it considered the effect of its decision on the allocation of societal resources.[278] Only after assuring itself that the supply of celebrity images for public discourse would remain robust, even after the defendant's unauthorized uses were allowed, did the court uphold the defendant's First Amendment defense.[279]

Relatedly, the "newsworthiness" defense responds to "fairness" concerns by allowing the press, in some circumstances, to balance out the communicative abilities of celebrities with a countervailing force. In assessing newsworthiness, courts indirectly inquire into fairness by asking whether the defendant's expression "concerns a matter of public interest" and is "informative."[280] Newsworthy speech can be viewed as speech that potentially counters already established voices in the communicative marketplace. For example, judges show special solicitude for unauthorized use of celebrity press conferences or interviews, reasoning that the media serves an important function in disseminating information that the persona at issue would like to restrict or at least manage differently.[281]

So how might the more balanced and defendant-focused approach to free speech concerns described above look in practice if applied to current initiatives to regulate online privacy? Some proposed "Do Not ***795** Track" legislation would restrict the use of online search histories to create targeted advertisements.[282] Despite the apparent constitutionality of a "Do Not Call" registry,[283] a law limiting online advertising would definitely raise free speech concerns.[284] Other "Do Not Track" provisions limit the collection of information about a person's online activities.[285] This could produce free speech challenges, as well.[286] A full description of how to evaluate the constitutionality of all pending data-privacy legislation is beyond the scope of this Article. Below is an initial sketch of a better, more balanced scheme, relying on the three approaches employed in intellectual property law and using potential "Do Not Track" legislation as its chief example.

In a preliminary analysis of new data-privacy laws, a court should consider the first two approaches discussed in this Article--categorization of the data at issue and evaluation of the data collector's intent. Using these two approaches, courts should find some legislation prohibiting data collection and tracking uncontroversial. Certain data subject matters (financial information, health records) are already likely to be deemed "sensitive" and weighty enough to survive a First Amendment challenge. Similarly, proof of intent to defraud data subjects should render any free speech appeals null. Further, constitutional analysis would not be required.

Most cases will not involve such extreme examples. Instead, most online data use involves everyday, nonsensitive information, and most data collectors specify their collection practices in opaque terms of service rather than engaging in out and out fraud. Hence, additional First Amendment review will be needed. It should not be enough, however, to determine that the data collection at issue in these situations is "speech." This was the move suggested by the Court in Sorrell, and it gave overwhelming deference to the expressive rights of data users and short shrift to both state and consumer interests. Rather than automatically validating the free speech interests of data miners and online advertisers because the information they collect seems less than sensitive and they do not act in "bad faith," a court interrogating "Do Not Track" or another kind of data-privacy law should note the commercial motive behind such data collection and further review the law under an intermediate level of scrutiny.

***796** The court should then examine how the data will be used by defendants, paying special attention to autonomy and fairness concerns. Autonomy concerns should rate low in a court's estimation of the free speech interests of most commercial data users. Rather than furthering a personal point of view, data mining is used simply to pinpoint consumer interests in the hopes of finding a viable marketing target. On the other hand, from the perspective of consumers, autonomy is the main justification for a "Do Not Track" regime. It prevents unwanted surveillance and revelations that are undesired and unintended. At the least, it

allows consumers to choose just how their personal information should be exposed to others and what the particular audience for that exposure should be. Just as courts construing the right of publicity have chosen to weigh the autonomy interests of celebrities and downstream speakers in determining whether an unauthorized use is transformative or newsworthy, a similar approach should be undertaken with regard to tracking restrictions and free speech arguments.

Fairness concerns also need to be part of the decision, even though they were not considered in Sorrell.[287] The newsworthiness defense concerns itself with power imbalances. Celebrity speakers wield immense power over the dissemination of their personas in society. A privilege for newsworthy uses of those personas is an attempt to inject a counterbalance to that power, making possible alternative and uncontrolled communications about public figures. Under a fairness perspective, it is important to recognize that, without protections like "Do Not Track," consumers have little opportunity to shape how their personal information is used by others. As discussed earlier, nonparticipation or resort to contractual safeguards is not a realistic option for those individuals seeking some protection from the efforts of online data collectors.[288]

A focus on the defendant's use of online data would not defeat all First Amendment challenges to data privacy laws. In some situations, the data user's autonomy interests may loom larger. Scientific research using collected individual data suggests greater autonomy concerns on the part of data users, as such users seek to use aggregated information to present important expressive content. Although a long way from practical implementation, technological innovations portend potential ways to give consumers more control over their data disclosures, regardless of the privacy policies of the Web sites they consult.[289] If such technologies take hold, the fairness calculation between consumers and data collectors may need to be reconceived.

***797** This speaks to a larger point about the need for an adaptable method for calibrating information privacy with the First Amendment. "Transformativeness" and "newsworthiness" are broad concepts. Rather than this ambiguity being a detriment, it permits a certain amount of flexibility as legal decision-makers respond to greater knowledge of existing technology. Whereas judges may once have viewed simply creating an avatar based on a real-life celebrity as transformative, this may no longer, by itself, represent a significant expressive contribution and, hence, merit less speech protection.[290] Similarly, uses of personal data that once seemed innovative may become commonplace and, therefore, deserve less regulatory deference. The key is to implement a richer framework for balancing information privacy and free speech. Otherwise, despite the significant harms that can arise from data collection and use, First Amendment arguments will always legitimate such behavior. By borrowing from intellectual property's playbook, information privacy law can support a constitutionally level playing field between consumers and commercial actors.

VI. CONCLUSION

There is an inherent tension between the desire to keep information private and the desire to share that information with others. Online technology amplifies the clash between the two desires by both allowing for more and more data to be compiled on individual consumers and by making it easier for that data to be repackaged and communicated to others. In figuring out how to resolve this tension, courts and legislatures do not need to reinvent the wheel. A similar tension exists between the legal system's award of rights in intangible creations to individual actors and the need for downstream actors to utilize those creations. One side wants to hold on to information; the other wants to broadcast it to others. As a result, intellectual property law has developed and refined a variety of approaches for addressing free speech concerns.

One approach, best represented by copyright law, weighs free speech interests by focusing on the subject matter of the plaintiff's communication. Another offers defendants a variety of speech-protective ***798** defenses that depend on whether the defendant acted under a proscribed motivation. A final approach evaluates the defendant's expressive output. Defenses for "transformativeness" and "newsworthiness" examine the societal contribution offered by the defendant's speech, forcing courts to analyze the costs and benefits of the defendant's expression from a variety of perspectives. These approaches for accommodating free expression are not mutually exclusive. Instead, they can all be implemented to offer a richer framework for constitutionally calibrating new data privacy laws. Moreover, these approaches, when considered as a group, offer balance, something lacking in the Sorrell decision and needed if courts are to uphold new and necessary data-privacy measures.

Footnotes

a1 Professor of Law, SUNY Buffalo Law School. This Article profited from presentations at Yale Law School's First Annual Freedom of Expression Scholars Conference, New York University Law School's Fourth Annual Tri-State Region IP Workshop, the 2014 Works-in-Progress in Intellectual Property Colloquium at Santa Clara University Law School, the 2013 Arizona State University Legal Scholars Conference, and the 2013 Law and Society Annual Meeting. Particular thanks to Ashutosh Bhagwat, Bryan Choi, Deven Desai, Shubha Ghosh, Margot Kaminski, Peter Lee, and Katherine Strandburg. Brian McSherry and Jay Organek provided valuable research assistance.

1 See Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It 4 (2009).

2 See, e.g., United States v. Miller, 425 U.S. 435, 442-44 (1976); see also Pátricia Sanchez Abril, Private Ordering: A Contractual Approach to Online Interpersonal Privacy, 45 Wake Forest L. Rev. 689, 702 (2010) ("[C] ourts have generally held that one cannot have a reasonable expectation of privacy in materials published online."); Jane B. Baron, Property as Control: The Case of Information, 18 Mich. Telecomm. & Tech. L. Rev. 367, 379 (2012) ("The law does not ensure that individuals will control the personal data collected about them."); Ronald J. Krotoszynski Jr., The Polysemy of Privacy, 88 Ind. L.J. 881, 885 (2013) ("[T]he surreptitious collection of private information regarding web surfing habits, or medical records, is generally legal.").

3 Dustin D. Berger, Balancing Consumer Privacy with Behavioral Targeting, 27 Santa Clara Computer & High Tech. L.J. 3, 7-8 (2011); Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1936-41 (2013).

4 Berger, supra note 3, at 11-13; Peter Whoriskey, Every Click You Make, Wash. Post (Apr. 4, 2008), http://articles.washingtonpost.com/2008-04-04/news/36854706_1_web-sites-service-providers-consumer-data.

5 Daniel J. Solove et al., Information Privacy Law 623 (2d ed. 2006); Steven C. Bennett, Regulating Online Behavioral Advertising, 44 J. Marshall L. Rev. 899, 901 (2011).

6 See Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010); Michael Barbaro & Tom Zeller Jr., A Face is Exposed for AOL Searcher No. 4417749, N.Y. Times, Aug. 9, 2006, at A2; Bruce Schneier, Why 'Anonymous' Data Sometimes Isn't, Wired (Dec. 13, 2007), http://www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_ 1213. In an example that should concern anyone paying for health insurance, one researcher was able to unmask participants in an anonymous study of genetic information just by matching the participant's birth date, gender, and zip code with publicly available records. Gina Kolata, Hunt for DNA Sequences Leaves Privacy Compromised, N.Y. Times (Jan. 17, 2013), http://www.nytimes.com/2013/01/18/health/search-of-dna-sequences-reveals-full-identities.html.

7 Berger, supra note 3, at 21-22; Robert Sprague & Corey Ciocchetti, Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws, 19 Alb. L.J. Sci. & Tech. 91, 101-02 (2009).

8 The word "privacy" can mean many things. Even when narrowed to its legal definition, the word can implicate the right to be free from unreasonable government searches and seizures, the right to make certain essential human decisions without government interference, or the right to have your home be free from certain trespasses and surveillance. In this Article, I am only interrogating one type of privacy concern: control over personal information.

9 Turow et al., supra note 1, at 3-4. This holds true even for young adults who grew up with the Internet. Id. at 16. Moreover, even if the demographic data were more mixed, I am not sure that we would want to simply wait for norms to change to justify privacy intrusions. To a large degree, the law, just by being there, helps inform social norms. Charles Fried argued long ago that privacy requires a sense of personal security, and this sense can only be supplied by providing individuals with concrete legal protections. Charles Fried,Privacy, 77Yale L.J.475, 493 (1968). So as lawyers, as policymakers, and as business leaders, we should think about what an appropriate safeguard of privacy would look like and not just "react." It will be easier for technologists to embody appropriate norms in code once we figure out what those norms are, and one way to do that is through law. Pamela Samuelson, Privacy as Intellectual Property?, 52Stan. L. Rev.1125, 1169 (2000).

10 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change iv (March 2012); see also Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Books and on the Ground, 63 Stan. L. Rev. 247, 289-90 (2011) (discussing the FTC's recent willingness to use its regulatory authority to prevent online data collection and dissemination practices that are out of line with consumer expectations).

11 Application Privacy, Protection, and Security Act, H.R. 1913, 113th Cong. (2013); Data Accountability and Trust Act, H.R. 1841, 112th Cong. (2011); see also S. 501, 2013 Leg. (Cal. 2013) (requiring social networking Web sites to remove personal identifying information upon request). Relatedly, the European Union is moving toward creation of a "right to be forgotten," giving online subjects the right to have their collected data erased. Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 16(1), at 33 (Jan. 25, 2012), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF.

12 Do-Not-Track Online Act, S. 418, 113th Cong. (2013); Consumer Right to Financial Privacy Act, H.R. 2571, 113th Cong. (2013); Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011); see also Cal. Bus. & Prof. Code § 22575 (West 2013) (requiring disclosure as to how a commercial Web site responds to a browser's "do not track" signals).

13 Do Not Track Kids Act, H.R. 1894, 112th Cong. (2011); see also S. 568, 2012-13 Leg. (Cal. 2013) (California bill requiring Web sites to permit minors to remove posted content upon request).

14 Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011); Fred H. Cate, Privacy in the Information Age 30 (1997) (describing privacy as "an antisocial construct ... [that] conflicts with other important values within the society, such as society's interest in facilitating free expression...."); Jane Yakowitz Bambauer, Is Data Speech?, 66 Stan. L. Rev. 57 (2014); David Post, **Cyberprivacy**, or What I (Still) Don't Get, 20 Temp. Pol. & Civ. Rts. L. Rev. 249, 251 (2011) ("[O]ne person's privacy is very often another person's infringement of the freedom to speak."); Neil M. Richards, Intellectual Privacy, 87 Tex. L. Rev. 387, 390 (2008) ("Indeed, when it comes to database regulation, many feel that any government regulation of private information flows raises serious First Amendment issues."). These concerns over the free speech implications of data privacy apply to even the most recent regulatory proposals. As described by law professor Jeffrey Rosen, "[Do Not Track] represents the biggest threat to free speech on the Internet in the coming decade." Jeffrey Rosen, The Right to Be Forgotten, 64 Stan. L. Rev. Online 88, 88 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf.

15 In a number of cases, the Court has cited the public's interest in the free exchange of information to prevent government regulation of advertising. E.g., Sorrell, 131 S. Ct. at 2670-71; Thompson v. W. States Med. Ctr., 535 U.S. 357, 374 (2002); Linmark Assoc., Inc. v. Willingboro, 431 U.S. 85, 97 (1977); Va. State Bd. of Pharm. v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 769-70 (1976).

16 Am. Tradition P'ship v. Bullock, 132 S. Ct. 2490, 2491 (2012); Citizens United v. FEC, 130 S. Ct. 876, 899-900 (2010). This makes some sense given that many corporations are media organizations and nonprofit political advocacy organizations. Eugene Volokh, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52 Stan. L. Rev. 1049, 1083 (2000). On the other hand, there is scholarly literature criticizing the equivalence between corporate and individual speech rights in the Court's jurisprudence. See, e.g., Tamara R. Piety, Against Freedom of Commercial Expression, 29 Cardozo L. Rev. 2583 (2008).

17 Bambauer, supra note 14, at 59-60.

18 Sorrell, 131 S. Ct. 2653.

19 Id. at 2659.

20 Id. at 2659-60.

21 Id. at 2660.

22 Id. at 2681 (Breyer, J., dissenting) (quoting Vt. Stat. Ann. tit. 18, § 4631(a)).

23 Id. at 2664 (majority opinion).

24 Id. at 2672.

25 There is some dispute over the effect of the Sorrell decision. While some commentators viewed it as a signal of defeat for privacy advocates, others suggested that the Vermont statute's unique characteristics limited the decision's reach. Compare Ashutosh Bhagwat, Sorrell v. IMS Health: Details, Detailing, and the Death of Privacy, 36 Vt. L. Rev. 855 (2012) (speculating that Sorrell would preempt forthcoming privacy regulation), with Agatha M. Cole, Note, Internet Advertising After Sorrell v. IMS Health: A Discussion on Data Privacy and the First Amendment, 30 Cardozo Arts & Ent. L.J. 283, 304 (2012) (maintaining that the Sorrell "decision was narrow and left much to be resolved").

26 Sorrell, 131 S. Ct. at 2666 (quoting IMS Health Inc. v. Ayotte, 550 F.3d 42, 52-53 (1st Cir. 2008)).

27 Id. at 2667.

28 Previous scholarship suggesting that dissemination of online data is not "speech" for First Amendment purposes, see, e.g., Neil M. Richards, Reconciling Data Privacy and the First Amendment, 52 UCLA L. Rev. 1149 (2005), appears not to have swayed the Court. See also CBS Interactive Inc. v. Nat'l Football League Players Ass'n, Inc., 259 F.R.D. 398, 417-18 (D. Minn. 2009) (finding that the First Amendment protects not only names and likenesses, but also "biographical data").

29 See Cole, supra note 25, at 305.

30 Sorrell, 131 S. Ct. at 2663-64.

31 Bambauer, supra note 14, at 71 (criticizing Sorrell decision for its lack of guidance on how to balance speech and privacy); Jane Yakowitz Bambauer, The New Intrusion, 88 Notre Dame L. Rev. 205, 265 (2012) ("Scholars have struggled to make sense of the public disclosure tort's interaction with the First Amendment for decades."); Ashutosh Bhagwat, Details: Specific Facts and the First Amendment, 86 S. Cal. L. Rev. 1, 14 (2012) ("the privacy cases leave many unanswered questions about the scope of protection for disclosure of private facts...."); Christina M. Gagnier, On Privacy: Liberty in the Digital Revolution, 11 J. High Tech. L. 229, 248 (2011).

32 Bambauer, supra note 14, at 71.

33 Danielle Keats Citron, Mainstreaming Privacy Torts, 98 Calif. L. Rev. 1805, 1828-29 (2010); Neil M. Richards, The Limits of Tort Privacy, 9 J. Telecomm. & High Tech. 357 (2011). See, e.g., Fla. Star v. B.J.F., 491 U.S. 524, 533-37 (1989) (holding the First Amendment barred liability for publishing name of rape victim obtained from police report).

34 See, e.g., Bartnicki v. Vopper, 532 U.S. 514 (2001) (holding the First Amendment prevented application of anti-wiretapping statute to media defendants); see Richards, supra note 14, at 388.

35 Bambauer, supra note 14, at 72 ("Very few cases have raised First Amendment challenges to data privacy statutes."); Bennett, supra note 5, at 931. The overall problem lies in the statutes' narrow nature. Most of the statutes were enacted before the phenomenon of

targeted online advertising took hold and only cover specific regulated entities like hospitals and banks, not all online data users. William McGeveran, Disclosure, Endorsement, and Identity in Social Marketing, 2009 U. Ill. L. Rev. 1105, 1138-39 (2009). For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (codified in scattered sections of 18, 29, and 42 U.S.C.) only applies to "covered entities" that do not include most health-related Web sites or the data miners who provide consumer information to such sites. Id. at 1139. When asked to interpret existing privacy statutes in a manner broad enough to encompass data miners and associated advertisers, courts have balked. See In re Pharmatrak, Inc. Privacy Litig., 320 F.3d 9, 21 (1st Cir. 2003); In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001).

36 Not only that, but such laws are likely content-based, thereby justifying particularly searching First Amendment review. Mark Bartholomew & John Tehranian, An Intersystemic View of Intellectual Property and Free Speech, 81 Geo. Wash. L. Rev. 1, 67-68 (2013); Jed Rubenfeld, The Freedom of Imagination: Copyright's Constitutionality, 112 Yale L.J. 1, 5-6 (2002).

37 Although less discussed, patent and trade-secret protection also have the potential to silence speakers. See Neil Weinstock Netanel, Copyright's Paradox 170 (2008); Dan L. Burk, Patenting Speech, 79 Tex. L. Rev. 99, 142-45 (2000).

38 See Bambauer, The New Intrusion, supra note 31, at 229; Citron, supra note 33, at 1835-36. The history of proposed hate speech laws is instructive. As documented by Anita Bernstein, proposed hate speech torts failed to win approval, in part, because they appeared to be too much of a departure from tort law in general and, relatedly, too inconsistent with traditional free speech doctrine. Anita Bernstein, How To Make a New Tort: Three Paradoxes, 75 Tex. L. Rev. 1539, 1546, 1557 (1997).

39 Citron, supra note 33, at 1835-36; Melanie R. Kay, Environmental Negligence: A Proposal for a New Cause of Action for the Forgotten Innocent Owners of Contaminated Land, 94 Calif. L. Rev. 149, 169 (2006).

40 E.g., Golan v. Holder, 132 S. Ct. 873, 890-91 (2012); Eldred v. Ashcroft, 537 U.S. 186, 219-21 (2003); S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 565 (1987) (Brennan, J., dissenting) (explaining that the descriptive fair-use defense prevents trademark law from restricting an excessive amount of speech).

41 E.g., Daniel J. Solove, Understanding Privacy 27 (2008) (stating general objection to extending intellectual property concepts to personal information); Bambauer, The New Intrusion, supra note 31, at 222 (contending that the intellectual property analogy is inapt because IP laws prohibit the propertization of the "raw facts" that would be the target of data privacy laws).

42 Note that the perceived incompatibility of intellectual property and privacy regulation is a particularly American view. By contrast, in Europe, there has been a greater willingness to construe both types of protection in similar terms. See Arthur Rizer, Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber?, 60 Cath. U. L. Rev. 77, 82 (2010).

43 See Christopher A. Cotropia & James Gibson, The Upside of Intellectual Property's Downside, 57 UCLA L. Rev. 921, 922 n.2 (2010); Mark A. Lemley, The Economics of Improvement in Intellectual Property Law, 75 Tex. L. Rev. 989, 993 (1997).

44 See James Gibson, Once and Future Copyright, 81 Notre Dame L. Rev. 167, 217 (2005).

45 Chris Jay Hoofnagle & Nathan Good, The Web Privacy Census, Berkeley Law (Oct. 2012), http://law.berkeley.edu/privacycensus.htm (finding use of tracking cookies on every one of the 100 most-visited online Web sites). Even attempts to cover one's online tracks are likely to fail. Online evidence of adultery forced the resignation of CIA Director David Petraeus, even though Petraeus and his paramour were careful not to exchange emails, instead composing messages in an electronic draft folder that could be checked by either party. Donna Leinwand Leger & Yamiche Alcindor, Petraeus and Broadwell Used Common E-mail Trick, USA Today (Nov. 13, 2012, 9:40 PM), http://www.usatoday.com/story/tech/2012/11/13/petraeus-broadwell-email/1702057/.

46 E.g., Mark A. Lemley, Private Property, 52 Stan. L. Rev. 1545, 1550 (2000). Others make a somewhat different argument,

contending that, by giving individuals a property right in their data modeled on intellectual property rights, the law would force the commoditization of something that is inherently personal. Baron, supra note 2, at 398. Under this view, personal data should be quarantined from marketplace forces, not traded like stocks and bonds. Samuelson, supra note 9, at 1138.

47 For example, copyright law allows a co-author of a copyrighted work to license the work without the other co-author's approval. The licensor need only provide her co-author with a proportional percentage of revenue secured by the license. The reason for such a rule is to encourage distribution of copyrighted works to society at-large. Julie E. Cohen et al., Copyright in a Global Information Economy 122 n.5 (3d ed. 2010). It would not make sense to adopt a parallel rule for private information created jointly, perhaps by two individuals involved in an intimate relationship. See Sonja R. West, The Story of Us: Resolving the Face-Off Between Autobiographical Speech and Information Privacy, 67 Wash. & Lee L. Rev. 589, 616-17 (2010). Likewise, trademark law requires that a mark be used in a public fashion before rights can attach. Karl Storz Endoscopy-Am., Inc. v. Surgical Techs., Inc., 285 F.3d 848, 855 (9th Cir. 2002). A similar rule would not make sense for personal data, which the data subject wants to keep private.

48 See West, supra note 47, at 606 (contending that merely granting a right does not tell lawmakers/courts how to resolve the tradeoff with other rights).

49 Police Dep't of Chi. v. Mosley, 408 U.S. 92, 95-96 (1972).

50 See William Fisher, Theories of Intellectual Property, in New Essays in the Legal and Political Theory of Property 168 (Stephen R. Munzer ed., 2001).

51 See Brett Frischmann & Mark P. McKenna, Intergenerational Progress, 2011 Wis. L. Rev. 123, 129-30.

52 U.S. Const. art. I, § 8, cl. 8.

53 See Bertford Mfg., Inc. v. Smith Sys. Mfg. Corp., 419 F.3d 576, 579 (7th Cir. 2005).

54 Hart v. Elec. Arts, Inc., 717 F.3d 141, 151 (3d Cir. 2013).

55 Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 81-84 (2010); Samuelson, supra note 9, at 1128.

56 M. Ryan Calo, The Boundaries of Privacy Harm, 86 Ind. L.J. 1131, 1133, 1142 (2011). Some have made the case that failure to safeguard online privacy will drive suspicious consumers away from the Internet. See Bennett, supra note 5, at 906. But this argument is much less prevalent than arguments based on autonomy and dignitary concerns.

57 Samuelson, supra note 9, at 1143; West, supra note 47, at 615. Another concern is that using IP-style protections to protect an individual's dignitary interest in personal information will make intellectual property law as a whole more incoherent. See Samuelson, supra note 9, at 1140.

58 See Nita A. Farahany, Searching Secrets, 160 U. Pa. L. Rev. 1239, 1255 (2012) (arguing that copyright law seeks to vindicate privacy interests and, therefore, should be employed as a metaphor for search-and-seizure law).

59 J. Thomas McCarthy, The Rights of Publicity and Privacy § 2:1 (2d ed. 2009); Roberta Rosenthal Kwall, Preserving Personality and Reputational Interests of Constructed Persons Through Moral Rights: A Blueprint for the Twenty-First Century, 2001 U. Ill. L. Rev. 151, 158-60; Mark P. McKenna, The Right of Publicity and Autonomous Self-Definition, 67 U. Pitt. L. Rev. 225, 231 (2005).

60 See Jeanne C. Fromer, A Psychology of Intellectual Property, 104 Nw. U. L. Rev. 1441, 1447 (2010); Justin Hughes, The Philosophy of Intellectual Property, 77 Geo. L.J. 287, 305 (1988).

61 Mark A. Lemley & Mark P. McKenna, Owning Mark(et)s, 109 Mich. L. Rev. 137, 154 (2010).

62 See John Tehranian, Infringement Nation: Copyright 2.0 and You 38 (2011); Wendy J. Gordon, A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property, 102 Yale L.J. 1533, 1548-49 (1993).

63 See Bambauer, The New Intrusion, supra note 31, at 231.

64 West, supra note 47, at 615.

65 Volokh, supra note 16, at 1116; see also Harry Kalven Jr., Privacy in Tort Law--Were Warren and Brandeis Wrong?, 31 L. & Contemp. Probs. 326, 327 (1966) (criticizing privacy as a "less precise way of approaching more specific values" like freedom of speech).

66 Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. 2087, 2087 (2001).

67 17 U.S.C. § 102(b) (2006) (stating that copyright protection does not extend to ideas).

68 Nichols v. Universal Pictures Corp., 45 F.2d 119, 121 (2d Cir. 1930); Rubenfeld, supra note 36, at 14.

69 See Ann Bartow, Likelihood of Confusion, 41 San Diego L. Rev. 721, 761-64 (2004); Barton Beebe, An Empirical Study of the Multifactor Tests for Trademark Infringement, 94 Calif. L. Rev. 1581, 1583-84 (2006).

70 In broader terms, we should not be overly influenced by the word "property" and somehow assume that every facet of a system of property rules is incompatible with a system of liability rules. The description of intellectual property rights as "property" does not prevent a comparison with any other legal protection that does not have the word "property" stamped on it. The distinction between property and nonproperty legal regimes can be a bit of a red herring. As Bill McGeveran points out, any legal protection or restriction can be construed as a "property" right. McGeveran, supra note 35, at 1163; see also Jane B. Baron, The Contested Commitments of Property, 61 Hastings L.J. 917 (2010) (suggesting academics have largely ignored questions about property's stability over time and "its very status as a distinctive field of study").

71 The explicit recognition of intellectual property in the Constitution does not make the way intellectual property negotiates the First Amendment somehow inapplicable to the data privacy-free speech interface. Although information privacy is not explicitly recognized in the Constitution, neither is trademark protection or the right of publicity.

72 See, e.g., McGeveran, supra note 35, at 1158; Samuelson, supra note 9, at 1171; Volokh, supra note 16, at 1057-61; see also In re U.S. for Historical Cell Site Data, 724 F.3d 600, 614-615 (5th Cir. 2013) (finding no constitutional barrier to government acquisition of cellphone location data and urging consumers to find a "market" solution to their privacy needs); M. Ryan Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87 Notre Dame L. Rev. 1027 (2012) (exploring use of "visceral notice" to address online privacy concerns).

73 Cohen v. Cowles Media Co., 501 U.S. 663 (1991); see also Abril, supra note 2, at 708 (noting that the Supreme Court has repeatedly upheld self-imposed speech restrictions, even when the information is of legitimate public concern).

74 Volokh, supra note 16, at 1061.

75 Bamberger & Mulligan, supra note 10, at 254.

76 Cole, supra note 25, at 287-88.

77 Charlie Warzel, For Privacy, Americans Trust Facebook Less Than the NSA, BuzzFeed (Sept. 12, 2013, 4:15 PM), http://www.buzzfeed.com/charliewarzel/survey-for-privacy-americans-trust-facebook-less-than-the-ns (discussing recent survey showing that 61 percent of respondents "do not trust Facebook at all" to protect their personal information and privacy, a poorer showing than other entities such as Google, the Internal Revenue Service, and the National Security Agency).

78 Josh Constine, Facebook's Growth Since IPO in 12 Big Numbers, Techcrunch (May 17, 2013), http://techcrunch.com/2013/05/17/facebook-growth/; Lee Spears & Sarah Frier, Facebook Set for Public Debut After IPO Seals $104 Billion Value, Bloomberg.com (May 18, 2012), http://www.bloomberg.com/news/2012-05-18/facebook-set-for-public-debut-after-ipo-seals-104-billion-value.html.

79 McGeveran, supra note 35, at 1126; West, supra note 47, at 611. Some maintain that the unilateral nature of online contracting can be changed, thereby providing consumers with more control over their data and alleviating concerns over government restrictions on how consumer data is used. Two scholars propose a privacy-contracting regime akin to the Creative Commons model used to facilitate licensing of copyrighted works. See Abril, supra note 2, at 722; Shubha Ghosh, Informing and Reforming the Marketplace of Ideas: The Public-Private Model for Data Production and the First Amendment, 2012 Utah L. Rev. 653, 703-05. But other problems with the market for online terms make this unlikely. First, private ordering is more plausible in the IP context because data subjects face a more coercive, less robust bargaining process than holders of intellectual property. Second, consumers face particular cognitive difficulties when attempting to bargain for greater privacy. These difficulties may cause them to overlook or even reject contractually available privacy safeguards. See infra notes 83-91 and accompanying text.

80 See McGeveran, supra note 35, at 1127.

81 Turow et al., supra note 1.

82 Bennett, supra note 5, at 937; see also Berger, supra note 3, at 22 (maintaining that such sharing among corporate partners and contractors is routine).

83 Calo, supra note 56, at 1133-35; Ohm, supra note 6.

84 Berger, supra note 3, at 8; Richards, supra note 3, at 1938-40.

85 Calo, supra note 56, at 1149; H. Brian Holland, Privacy Paradox 2.0, 19 Widener L.J. 893, 899 (2010).

86 Solove, supra note 41, at 118; Bennett, supra note 5, at 905; Berger, supra note 3, at 4; Calo, supra note 56, at 1149; Steve Lohr, How Privacy Vanishes Online, N.Y. Times (Mar. 16, 2010), available at http://www.nytimes.com/2010/03/17/technology/17privacy.html?_r=1&.

87 Neil M. Richards, The Perils of Social Reading, 101 Geo. L.J. 689, 698-99 (2013); Charles Duhigg, Psst, You in Aisle 5, N.Y. Times Mag., Feb. 12, 2012, at § 6, at 30.

88 Berger, supra note 3, at 24; Holland, supra note 85, at 897, 907; see also Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393, 1452 (2001) (contending that consumers frequently lack the ability to assign the proper value to their personal information).

89 Calo, supra note 56, at 1149 n.106 (arguing that consumers sell their data too often and too cheaply because of "privacy myopia"); Holland, supra note 85, at 903 (citing evidence of human difficulty in forecasting long-term risks).

90 Berger, supra note 3, at 28; Gagnier, supra note 31, at 251-52.

91 Chris Jay Hoofnagle & Jennifer King, What Californians Understand About Privacy Online (Sept. 3, 2008) (unpublished article), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130; Holland, supra note 85, at 899; see also Somini Sengupta, Letting Down Our Guard with Web Privacy, N.Y. Times, Mar. 30, 2013 (discussing academic research revealing inability of consumers to understand online privacy policies). The calculation required of online consumers assessing privacy policies is arguably more difficult than the challenge of evaluating the benefits of a bargain faced by a copyright holder. An artist giving up rights in her work may not know exactly how it will be used, but the basic contours of the work are self-evident. Music is meant to be listened to, books are meant to be read, sculptures are meant to be put on display and visually appreciated. Even if someone not part of the original contract between creator and buyer ends up with the work, the probable use by the ultimate possessor of the copyright is relatively clear. There are of course exceptions, but even an artist who would rather not have her work used in a particular fashion (e.g., as an advertisement for a product that is personally unappealing to the artist) knows that she runs this risk by assigning her copyright to someone else. An online shopper, however, has very little sense of who will ultimately review her personal data or for what purpose.

92 Abril, supra note 2, at 715.

93 Suggestions have been made to remedy this contract law shortcoming by imposing an additional "duty of confidentiality" on third parties that use personal data. See Daniel J. Solove & Neil M. Richards, Rethinking Free Speech and Civil Liability, 109 Colum. L. Rev. 1650, 1667 (2009). Yet under American law, duties of confidentiality can only apply to parties in an existing relationship. Citron, supra note 33, at 1850. In addition, even when a confidential relationship exists, if the information at issue comes to be possessed by a third party, the individual can no longer claim a reasonable expectation of privacy in the information. Solove, supra note 41, at 139. In other words, a duty of confidentiality might be imposed on the original Web site that took your information, but not on the data broker who purchased and used your information. Moreover, if the data at issue becomes known to anyone else and the original Web site is not responsible for the initial dissemination, the Web site cannot be liable for breach of confidentiality. See id. at 139-40.

94 See Solove, supra note 41, at 132 (discussing how the potential for unforeseen uses of personal data "generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability"); Calo, supra note 56, at 1142 (arguing that the mere perception of being observed online can cause significant psychological harm).

95 Abril, supra note 2, at 706-07; see also Solove, supra note 41, at 127-28 (discussing judicial reluctance to recognize data "insecurity" as a legally cognizable problem).

96 Another problem with a contractual solution is that it would likely increase the complexity of the marketplace for privacy, thereby compounding the cognitive challenges faced by concerned consumers. As Jane Baron has noted, one of the strengths of property law is its use of strong, relatively crude signals to create social ordering. Baron, supra note 2, at 388; see also Thomas W. Merrill & Henry E. Smith, The Morality of Property, 48 Wm. & Mary L. Rev. 1849 (2007) (arguing any property system must have an element of moral significance in order to survive). The law of trespass is a blunt tool, but people know what it means. By contrast, a regime made up of millions of individual contracts tailored to each consumer's unique privacy preferences increases the costs of online commerce, as well as the costs of governing, when entities, unknowingly or not, commit an infraction. Baron, supra note 2, at 388. Too much individual privacy tailoring poses insurmountable challenges for contract law. Basing privacy protection on personal preferences would create an unstable legal environment, ultimately harming both data subjects and data users. Solove, supra note 41, at 70.

97 See Andrew J. McClurg, Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality, 74 U. Cin. L. Rev. 887, 908 (2006). For example, evidence shows that restrictions on the disclosure of patient medical records can hamstring medical research, delaying the discovery and removal of dangerous drugs from the marketplace. See Barbara J. Evans, Seven Pillars of a New Evidentiary Paradigm: The Food, Drug, and Cosmetic Act Enters the Genomic Era, 85 Notre Dame L. Rev. 419, 456 (2009).

98 This is not to say that contract has no role to play in addressing privacy concerns. Intellectual property law diagnoses situations where increased formalities are meant to improve the bargaining process. For example, assignment of a copyright cannot be oral. It has to be in writing. 17 U.S.C. § 204 (2006). The same is true of trademark assignments. 15 U.S.C. § 1060(a)(3) (2012). When asked to relax these rules based on industry custom or an analysis on the subjective mindset of the contracting parties, courts have balked. E.g., Effects Assocs., Inc. v. Cohen, 908 F.2d 555, 557 (9th Cir. 1990); MVP Entm't Inc. v. Frost, 149 Cal. Rpt. 3d 162, 164-66 (Cal. Ct. App. 2012). Similar formalities may need to be legislated in online privacy contracts to put consumers and data users on a more equal footing.

99 See James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1178-87 (2009) (contending that efforts to improve Facebook's disclosure policies will be ineffective in resolving privacy concerns).

100 See, e.g., Fortune Dynamic, Inc. v. Victoria's Secret Stores Brand Mgmt., 618 F.3d 1025, 1030 (9th Cir. 2010) (stating that likelihood of confusion is the "core element of trademark infringement").

101 Courts routinely assess "mark strength" in the likelihood of confusion analysis, investigating the degree of both inherent distinctiveness and acquired marketplace distinctiveness a mark possesses. E.g., Virgin Enters. Ltd. v. Nawab, 335 F.3d 141, 147 (2d Cir. 2003).

102 E.g., Raymen v. United Senior Ass'n, 409 F. Supp. 2d 15, 23 (D.D.C. 2006); Joe Dickerson & Assocs., LLC v. Dittmar, 34 P.3d 995, 1003 (Colo. 2001). On the other hand, courts largely ignore the type of trademark at issue when determining a defendant's eligibility for any of trademark's three affirmative defenses to infringement. This omission is particularly striking given the obvious free speech concerns at stake in granting trademark rights in a merely descriptive trademark. See generally Lisa P. Ramsey, Descriptive Trademarks and the First Amendment, 70 Tenn. L. Rev. 1095 (2003).

103 Eastwood v. Superior Court, 149 Cal. App. 3d 409, 423 (1983).

104 Wash. Rev. Code §§ 63.60.020, 63.60.040 (2012).

105 Id. But under most analyses, the prominence of the celebrity persona is not specifically acknowledged in deciding how to balance First Amendment concerns with the right of publicity. Instead, to state a claim under the right of publicity, a plaintiff must merely show the defendant's unauthorized use of her identity and resulting injury. Browne v. McCain, 611 F. Supp. 2d 1062, 1069 (C.D. Cal. 2009). As we will see, instead of categorizing the plaintiff's expression, in the main, publicity rights law relies on very different mechanisms to accommodate free speech interests. See infra Part V.

106 Golan v. Holder, 132 S. Ct. 873, 890-91 (2012); Eldred v. Ashcroft, 537 U.S. 186, 221 (2003); Harper & Row, Inc. v. Nation Enters., 471 U.S. 539, 560 (1985); see also Silvers v. Sony Pictures Entm't, Inc., 402 F.3d 881, 893 (9th Cir. 2005) (describing the dichotomy as a "major First Amendment protection"); Neil Weinstock Natanel, First Amendment Constraints on Copyright After Golan v. Holder, 60 UCLA L. Rev. 1082, 1086 (2013) ("First Amendment scrutiny of copyright law is unwarranted so long as the idea/expression dichotomy and fair use privilege ... remain 'undisturbed.'" (quoting Golan v. Holder, 132 S. Ct. 873, 890-91 (2012))).

107 E.g., Hoehling v. Universal City Studios, Inc., 618 F.2d 972, 978-89 (2d Cir. 1980).

108 E.g., Morrissey v. Procter & Gamble Co., 379 F.2d 675, 679 (1st Cir. 1967) (granting summary judgment for defendant because of limited number of ways to express sweepstakes rules).

109 Pamela Samuelson, Copyright and Freedom of Expression in Historical Perspective, 10 J. Intell. Prop. L. 319, 320 n.6 (2003).

110 E.g., Benay v. Warner Bros. Entm't, Inc., 607 F.3d 620, 624-25 (9th Cir. 2010); Hoehling, 618 F.2d at 979.

111 2 William F. Patry, Patry on Copyright § 4:28 (2012).

112 Rucker v. Harlequin Enters., No. 4:12-cv-01135, 2013 WL 707922 (S.D. Tex. Feb. 26, 2013).

113 2 Patry, supra note 111, at § 4:26; Computer Associates Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992).

114 Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 552-54 (1985).

115 17 U.S.C. § 107 (2012). If anything, the fair-use defense looms even larger in the judicial imagination as a surrogate for First Amendment concerns than the idea/expression dichotomy. As stated by the Second Circuit, "absent extraordinary circumstances, 'the fair use doctrine encompasses all claims of first amendment in the copyright field.'" Sarl Louis Feraud Int'l v. Viewfinder, Inc., 489 F.3d 474, 482 (2d Cir. 1997) (quoting Twin Peaks Prods., Inc. v. Publ'ns Int'l, Ltd., 996 F.2d 1366, 1378 (2d Cir.1993)).

116 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994).

117 17 U.S.C. § 107(3) (2012).

118 Peter Letterese & Assocs. v. World Inst. of Scientology Enters., 533 F.3d 1287, 1314-15 (11th Cir. 2008); NXIVM Corp. v. Ross Inst., 364 F.3d 471, 480 (2d Cir. 2004).

119 Letterese & Assocs., 533 F.3d at 1314-15.

120 Id.

121 Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 565 (1985).

122 E.g., 4 Patry, supra note 111, at § 10:151 (2012); Rogers v. Koons, 960 F.2d 301, 312 (2d Cir. 1992); Infinity Broad. Corp. v. Kirkwood, 150 F.3d 104, 111 (2d Cir. 1998).

123 See infra subsection V.A.1.

124 E.g., Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 350 (1991); Harper & Row, 471 U.S. at 560; Meshwerks, Inc. v. Toyota Motor Sales USA, Inc., 528 F.3d 1258, 1264 (10th Cir. 2008).

125 Veeck v. S. Bldg. Code Cong. Int'l, Inc., 293 F.3d 791, 800-01 (5th Cir. 2002) (en banc).

126 Id. at 801-02.

127 Worldwide Church of God v. Phila. Church of God, 227 F.3d 1110, 1115 (9th Cir. 2000) ("The public interest in the free flow of information is assured by the law's refusal to recognize a valid copyright in facts." (quoting Harper & Row, 471 U.S. at 558)).

128 Veeck, 293 F.3d at 802.

129 Feist Publ'ns, 499 U.S. at 349-50, 363-64.

130 Stewart v. Abend, 495 U.S. 207, 237 (1990) ("[F]air use is more likely to be found in factual works than fictional works."). For example, the fair-use defense favored a plaintiff that held copyright in video games and disfavored a plaintiff suing for infringement of the copyright in its aircraft maintenance manuals. Gulfstream Aerospace Corp. v. Camp Sys. Int'l, Inc., 428 F. Supp. 2d 1369, 1378 (S.D. Ga. 2006); Sega Enters. v. MAPHIA, 948 F. Supp. 923, 934 (N.D. Cal. 1996).

131 Barton Beebe, An Empirical Study of U.S. Copyright Fair Use Opinions, 1978-2005, 156 U. Pa. L. Rev. 549, 611 (2008).

132 See id.

133 Warner Bros., Inc. v. RDR Books, 575 F. Supp. 2d 513, 551 (S.D.N.Y. 2008).

134 New Era Publ'ns Int'l, ApS v. Carol Publ'g Grp., 904 F.2d 152, 157 (2d Cir. 1990).

135 Id. at 154.

136 Id. at 157.

137 See Abril, supra note 2, at 696 ("U.S. privacy tort law is configured to protect privacy as defined by content, rather than social relationships or interpersonal understandings of confidentiality.").

138 Restatement (Second) of Torts § 652D (1977). Even if personal details are revealed that the plaintiff finds highly upsetting, much more is needed before the "highly offensive" element of the tort is satisfied. Sidis v. F-R Publ'g Corp., 113 F.2d 806, 809 (2d Cir. 1940). As noted supra, scholars argue that this tort is largely ineffective at protecting personal information, both in the offline and online realms. See also Rodney A. Smolla, Privacy and the First Amendment Right to Gather News, 67 Geo. Wash. L. Rev. 1097, 1101 (1999) (stating that the tort exists "more 'in the books' than in practice").

139 For example, the Health Insurance Portability and Accountability Act (HIPAA) sets out very specific privacy rules regarding "individually identifiable health information" for those in the health care and insurance industries. 45 C.F.R. §§ 160.102-160.103 (2012). Other statutes regulate disclosure of financial information, but only in very specific contexts. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2012); Fair Credit Reporting Act, 15 U.S.C. § 1691b(b) (2012).

140 See Trans Union Corp. v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001); Individual Reference Servs. Corp. v. FTC, 145 F. Supp. 2d 6 (D.D.C. 2001), aff'd sub nom. Trans Union LLC v. FTC, 295 F.3d 42 (D.C. Cir. 2002); see also Richards, supra note 28, at 1164 n.67 (discussing application of intermediate scrutiny in credit-reporting cases).

141 Trans Union Corp., 245 F.3d at 819.

142 Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985); Individual Reference Servs. Corp., 145 F. Supp. 2d at 40-41.

143 Trans Union Corp., 245 F.3d at 818-19; Toomer v. Garrett, 574 S.E.2d 76, 82-83, 90 (N.C. Ct. App. 2002) (upholding privacy claim against state officials for disclosing personnel file that included "sensitive" information, including employee's credit history).

144 What data collectors were actually doing with the credit-report information--translating it into customized marketing lists to be sold to outside businesses--was relatively unimportant to this analysis. This is notable given the credit-report regulation's obvious role in restricting a particular kind of speech--advertising--that enjoys First Amendment protection in a multitude of other contexts. E.g., Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 564 (2001); 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996).

145 See, e.g., Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dep't of Health & Human Servs., 224 F. Supp. 2d 1115, 1125 (S.D. Tex. 2002) (finding no constitutional violation from "Privacy Rule" promulgated by Department of Health and Human Services that restricted doctor communications). But see Beverly Cohen, Regulating Data Mining Post-Sorrell: Using HIPAA to Restrict Marketing Use of Patients' Private Medical Information, 47 Wake Forest L. Rev. 1141, 1173 (2012) (questioning whether the Sorrell decision places some HIPAA privacy restrictions in jeopardy).

146 Calo, supra note 56, at 1131.

147 Somini Sengupta, Facebook Objects to a Privacy Law, N.Y. Times (Oct. 8, 2012), http://query.nytimes.com/gst/fullpage.html?res=9A03E5D91F38F93BA35753C1A9649D8B63.

148 Calo, supra note 56, at 1142-46; Richards, supra note 3, at 1948-52.

149 See Do Not Track Kids Act of 2011,H.R. 1895, 112th Cong.§ 3(a)(2)(A) (2011);Andrew Couts, Facebook Says Child Privacy Law Shouldn't Apply to "Like" Button, Digital Trends (Oct. 2, 2012), http://www.digitaltrends.com/social-media/facebook-coppa-like-button/.

150 Bhagwat, supra note 25, at 876.

151 Planned Parenthood of Columbia/Williamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058 (9th Cir. 2002) (en banc).

152 Id. at 1088.

153 Id.

154 According to established doctrine, speech can only be a "true threat" if it demonstrates an intent to commit violence. Virginia v. Black, 538 U.S. 343, 359 (2003). However, there was no evidence in the facts of the case that the abortion protestors that operated the Web site intended to commit violence. Planned Parenthood, 290 F.3d at 1091-92 (Kozinski, J., dissenting).

155 See McGeveran, supra note 35, at 1138 (maintaining that most social-networking sites would hesitate before using sensitive financial or sexual information out of fear of offending potential customers).

156 William F. Patry & Shira Perlmutter, Fair Use Misconstrued: Profit, Presumptions, and Parody, 11 Cardozo Arts & Ent. L.J. 667, 685 (1992). In general, however, such inquiries into defendant intent are rare. Beebe, supra note 131, at 607-08 ("The data suggest that considerations of fairness, propriety, and good or bad faith have not played a significant role in our fair use case law--notwithstanding the frequency with which opinions intoned that fair use is an 'equitable doctrine.'").

157 Estate of Presley v. Russen, 513 F. Supp. 1339, 1359-60 (D.N.J. 1981).

158 Hensley Mfg., Inc. v. Propride, Inc., 579 F.3d 603, 609 (6th Cir. 2009).

159 See KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc., 543 U.S. 111 (2004).

160 Zatarains, Inc. v. Oak Grove Smokehouse, Inc., 698 F.2d 786 (5th Cir. 1983).

161 WCVB-TV v. Bos. Athletic Ass'n, 926 F.2d 42, 46 (1st Cir. 1991).

162 Id.

163 15 U.S.C. § 1115(b)(4) (2006).

164 Century 21 Real Estate Corp. v. Lendingtree, Inc., 425 F.3d 211, 225-26 (3d Cir. 2005).

165 Id. at 227 n.7.

166 New Kids on the Block v. News Am. Publ'g, 971 F.2d 302, 308 (9th Cir. 1992).

167 Douglas L. Rogers, Ending the Circuit Split over Use of a Competing Mark in Advertising--The Blackstone Code, 5 J. Marshall Rev. Intell. Prop. L. 157, 192 n.214 (2006).

168 Lendingtree, 425 F.3d at 243 (Fisher, J., dissenting).

169 17 U.S.C. § 107(1) (2012).

170 E.g., Compaq Computer Corp. v. Ergonome Inc., 387 F.3d 403, 408-09 (5th Cir. 2004); New Era Publ'ns Int'l, ApS v. Henry Holt and Co., 873 F.2d 576, 591 (2d Cir. 1989).

171 4 Melville B. Nimmer & David Nimmer, Nimmer on Copyright § 13.05[A][[[1][c] (2012).

172 Id.

173 L.A. News Serv. v. CBS Broad., Inc., 305 F.3d 924, 939 n.13 (9th Cir. 2002).

174 Sony Corp. of America v. Universal City Studios, Inc, 464 U.S. 417, 449 (1984).

175 Am. Geophysical Union v. Texaco, Inc., 802 F. Supp. 1, 12 (S.D.N.Y. 1992) (interpreting the Sony decision).

176 John Doe v. TCI Cablevision, 110 S.W.3d 363 (Mo. 2003).

177 Id. at 366.

178 Id. at 374.

179 E.g., Matthews v. Wozencraft, 15 F.3d 432, 440 (5th Cir. 1994) (explaining that fictional novel could violate individual's publicity rights if it was "a disguised advertisement for the sale of goods or services" (quoting Rogers v. Grimaldi, 875 F.2d 994, 1004 (2d Cir. 1989))); Estate of Presley v. Russen, 513 F. Supp. 1339, 1360 (D.N.J. 1981) (rejecting First Amendment defense for Elvis tribute act because "the primary purpose" was to expropriate the value of the likeness of the singer).

180 E.S.S. Entm't 2000, Inc. v. Rock Star Videos, Inc., 547 F.3d 1095, 1099 (9th Cir. 2008).

181 E.g., id. at 1100; Roxbury Entm't v. Penthouse Media Grp., Inc., 669 F. Supp. 2d 1170, 1176 (C.D. Cal. 2009).

182 E.g., Mattel, Inc. v. MCA Records, Inc., 296 F.3d 894, 899-900 (9th Cir. 2002); Twin Peaks Prods., Inc. v. Publn's Int'l, Ltd., 996 F.2d 1366, 1379 (2d Cir. 1993); Volkswagen AG v. Dorling Kindersley Publ'g, Inc., 614 F. Supp. 2d 793, 801-02, 810 (E.D. Mich. 2009).

183 Facenda v. N.F.L. Films, Inc., 542 F.3d 1007, 1018 (3d Cir. 2008); 6 J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition § 31:144.50 (4th ed. 2012).

184 To be fair, courts sometimes also take an objective approach, basing their decision on the type of product bearing the defendant's expression. They typically view use of a trademark in a film or song as noncommercial. See, e.g., Mattel, 296 F.3d at 900-02; Winchester Mystery House v. Global Asylum, Inc., 210 Cal. App. 4th 579, 590-94 (Cal. Ct. App., Oct. 24, 2012); see also Jordan v. Jewel Food Stores, Inc., 851 F. Supp. 2d 1102, 1105 (N.D. Ill. 2012) (page in Sports Illustrated issue paid for and created by grocery store chain congratulating Michael Jordan on his basketball achievements considered "non-commercial speech" exempt from trademark false-endorsement claim because it did not tout a particular product). On the other hand, more tangible merchandise such as T-shirts and coffee mugs is usually deemed commercial and, hence, not eligible for Rogers' protection. Univ. of Ala. Bd. of Trs. v. New Life Art, Inc., 683 F.3d 1266, 1279-80 (11th Cir. 2012); Mut. of Omaha Ins. Co. v. Novak, 836 F.2d 397, 398-99, 403 (8th Cir. 1987). But see Smith v. Wal-Mart Stores, Inc., 537 F. Supp. 2d 1302, 1339-40 (N.D. Ga. 2008).

185 Facenda v. N.F.L. Films, Inc., 542 F.3d 1007, 1018 (3d Cir. 2008).

186 Id. at 1014.

187 Id. at 1016.

188 Id. at 1017.

189 Id. at 1018.

190 Id. at 1017.

191 Id. at 1016, 1018. See also Dillinger, LLC v. Elec. Arts, No. 1:09-cv-1236-JMS-DKL, Inc., 2011 WL 2457678, at *4 n.1 (S.D. Ind. June 16, 2011) (describing Rogers test as interrogating "intentional use of another's intellectual property for commercial profit").

192 White v. Samsung Elec. Am., Inc., 971 F.2d 1395 (9th Cir. 1992).

193 Id. at 1397.

194 Id. at 1401.

195 Id. at 1396.

196 Id. at 1400.

197 Id. at 1401.

198 Id. at 1400-01.

199 Id. at 1401.

200 Id. On the other hand, without evidence of commercial intent, Rogers can be an effective tool for defendants. To take one example, when high-end resort operator Club Med sued the maker of a film titled Club Dread for trademark infringement, the court looked favorably on the filmmaker's Rogers defense. In determining whether there was a likelihood of confusion, the court faulted Club Med for failing to offer any evidence of the filmmaker's intent to confuse consumers. Most significant for our purposes, later on in the opinion, the court highlighted the evidence of such intent (or lack thereof) to hold that the filmmaker was "likely to succeed on its First Amendment claim under Rogers and its progeny." Club Meditéranée, S.A. v. Fox Searchlight Pictures, Inc., No. 04-20273-CIV, 2004 WL 5589591, at *4 (S.D. Fla. Feb. 17, 2004).

201 Bhagwat, supra note 31, at 47.

202 Larry Alexander, Free Speech and Speaker's Intent, 12 Const. Comment. 21 (1995).

203 See Richards, supra note 14, at 394 (describing these as the "two principal theories of the First Amendment ... recognized by courts and scholars").

204 Speaker mental state has been used by the Supreme Court as the constitutional fulcrum to reconcile some aspects of tort law with the First Amendment. In actions for libel, defamation, and intentional infliction of emotional distress, the publisher's "actual malice" must be demonstrated; otherwise, the publisher's First Amendment interest prevails. New York Times Co. v. Sullivan, 376 U.S. 254, 287-88 (1964); Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 56 (1988). Similarly, the Supreme Court allows punishment of speech that incites violence but only after proof of specific intent. Virginia v. Black, 538 U.S. 343, 359 (2003); Brandenburg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam).

205 See supra notes 39-40 and accompanying text.

206 See, e.g., Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Bos., 515 U.S. 557, 573 (1995); see also C. Edwin Baker, Scope of the First Amendment Freedom of Speech, 25 UCLA L. Rev. 964, 1000 (1978) ("[I]n a just social order the law must respect one's choice of speech content."); Robert Post, Equality and Autonomy in First Amendment Jurisprudence, 95 Mich. L. Rev. 1517, 1525 (1997) ("To compromise individual autonomy is to compromise the foundation of the democratic value of collective self-determination.").

207 Leslie Kendrick, Free Speech and Guilty Minds (unpublished manuscript) (on file with author); see also Restatement (Third) of Torts: Products Liability § 19 cmt. d (1998) ("Most courts express[ ] concern that imposing strict liability for the dissemination of false and defective information would significantly impinge on free speech....").

208 Kendrick, supra note 207, at 23.

209 New York Times Co., 376 U.S. at 279; Leslie Kendrick, Speech, Intent, and the Chilling Effect, 54 Wm. & Mary L. Rev. 1633 (2013).

210 Bambauer, The New Intrusion, supra note 31, at 207-08; Solove, supra note 41, at 47.

211 Bambauer, The New Intrusion, supra note 31, at 231.

212 Id.

213 Id.

214 Solove, supra note 41, at 47.

215 See id.; Daniel Solove, The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure, 53 Duke L.J. 967, 976-77 (2003).

216 For example, some legal authorities already maintain that all uses of online data are "commercial," suggesting a relatively free hand for government regulation. E.g., Trans Union Corp. v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001); see McGeveran, supra note 35, at 1163; Richards, supra note 14, at 1192. But this is completely at odds with the approach taken by the Supreme Court in Sorrell. The pharmaceutical marketers in that case were engaged in commercial activity, but the Court had no trouble asserting that important First Amendment interests were at stake, enough so to strike down Vermont's data privacy law. Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2670 (2011).

217 As Bill McGeveran notes, some courts have merely reused their analysis of the intent factor from the likelihood-of-confusion analysis to determine "good faith" for purposes of the fair-use defense. See William McGeveran, Rethinking Fair Use, 94 Iowa L. Rev. 49, 86 (2008).

218 E.M.I. Catalogue P'ship v. Hill, Holliday, Connors, Cosmopulos, Inc., 228 F.3d 56, 66-67 (2d Cir. 2000); see also McCarthy, supra note 183, at § 11:49 (discussing statutory descriptive fair use).

219 E.M.I., 228 F.3d at 66-67.

220 Tdata Inc. v. Aircraft Tech. Pub., 411 F. Supp. 2d 901, 910-12 (S.D. Ohio 2006).

221 West, supra note 47, at 638.

222 Bambauer, The New Intrusion, supra note 31, at 231-35.

223 See, e.g., Randolph v. ING Life Ins. & Annuity Co., 973 A.2d 702, 711 (D.C. 2009); Hudson v. S.D. Warren Co., 608 F. Supp. 477, 481 (D. Me. 1985).

224 Bailer v. Erie Ins. Exch., 687 A.2d 1375, 1380-81 (Md. Ct. App. 1997); Restatement (Second) of Torts § 652B.

225 See Citron, supra note 33, at 1828.

226 Sorrell v. IMS Health Inc., 131 S. Ct. 2653 (2011).

227 See, e.g., E.S.S. Entm't 2000, Inc. v. Rock Star Videos, Inc., 547 F.3d 1095 (9th Cir. 2008).

228 E.g., Bd. of Trs. of N.Y. v. Fox, 492 U.S. 469, 480 (1989).

229 With some justices calling for the general abandonment of the commercial speech doctrine, see 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 517 (1996) (Scalia, J., concurring in part); id. at 522-23 (Thomas, J., concurring in part), learning the particular lessons of intellectual property law with regard to commercial motivation becomes all the more imperative if meaningful data privacy protection is to be realized.

230 Cf. Joseph Blocher, Nonsense and the Freedom of Speech: What Meaning Means for the First Amendment 51 (unpublished manuscript) (on file with author) (discussing value of clarity in First Amendment doctrine).

231 6 McCarthy, supra note 183, at § 31:139.

232 Id.

233 Id.

234 E.g., Utah Lighthouse Ministry v. Found. for Apologetic Info. & Research, 527 F.3d 1045, 1057 (10th Cir. 2008); MasterCard Int'l v. Nader 2000 Primary Comm. Inc., 70 U.S.P.Q.2d 1046, 1050-51 (S.D.N.Y. 2004).

235 Comedy III Prods., Inc. v. Gary Saderup, Inc., 21 P.3d 797, 800-01, 809 (Cal. 2001).

236 Id. at 809.

237 Other courts have followed the California Supreme Court's lead. In determining whether an artist's representation of Tiger Woods was transformative, and therefore immune from an infringement suit, the Sixth Circuit ignored whether the artist intended to profit from Woods's celebrity. What was critical in determining the proper weight of the expressive interests at play was the presence of "substantial transformative elements," which meant that the work was "entitled to the full protection of the First Amendment." See, e.g., ETW Corp. v. Jireh Pub., Inc., 332 F.3d 915, 951 (6th Cir. 2003).

238 Kirby v. Sega of Am., Inc., 144 Cal. App. 4th 47, 59 (2006).

239 In re NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1276 (9th Cir. 2013); Hart v. Electronic Arts, Inc.,717 F.3d 141, 166 (3d Cir. 2013) ("If we are to find some transformative element, we must look somewhere other than just the in-game digital recreation of Appellant."); Davis v. Electronic Arts, Inc., No. 10-03328 RS, 2012 WL 3860819 (N.D. Cal. Mar. 29, 2012); Keller v. Electronic Arts, Inc., No. C 09-1967 CW, 2010 WL 530108 (N.D. Cal. Feb. 8, 2010).

240 Winter v. DC Comics, 69 P.3d, 473, 476 (Cal. 2003).

241 Id.

242 Id. at 479-80.

243 Id. at 479.

244 Id.

245 Romantics v. Activision Publ'g, Inc., 574 F. Supp. 2d 758, 762, 766 & n.3 (E.D. Mich. 2008).

246 Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1168 (9th Cir. 2007).

247 Cariou v. Prince, 714 F.3d 694, 706 (2d Cir. 2013).

248 Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 923 (2d Cir. 1995). In other cases, courts have recognized exact copies made for a completely, separate purpose from the original as being transformative under the first fair-use factor. E.g., Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).

249 Texaco, 60 F.3d at 919-20 (alteration in original) (internal quotation marks omitted).

250 See, e.g., Toffoloni v. LFP Publ'g Grp., LLC, 572 F.3d 1201, 1208 & n.2 (11th Cir. 2009); Titan Sports, Inc. v. Comics World Corp., 870 F.2d 85, 87-88 (2d Cir. 1989).

251 The Supreme Court explicitly rejects any special First Amendment defense in copyright cases for news reporting. Harper & Row, Inc. v. Nation Enters., 471 U.S. 539, 557 (1985); see also Monge v. Maya Magazines, Inc., 688 F.3d 1164, 1183 (9th Cir. 2012) ("Waving the news reporting flag is not a get out of jail free card in the copyright arena."). In fact, courts adjudicating fair-use defenses are quite willing to second-guess journalistic assertions regarding the importance of particular copyrighted material to a particular news article or broadcast. E.g., L.A. News Serv. v. KCAL-TV Channel 9, 108 F.3d 1119, 1123 (9th Cir. 1997); see Bartholomew & Tehranian, supra note 36, at 18-21.

252 Davis v. Electronic Arts, Inc., No. 10-03328 RS, 2012 WL 3860819, at *6-*7 (N.D. Cal. Mar. 29, 2012); Keller v. Electronic Arts, Inc., No. C 09-1967 CW, 2010 WL 530108, at *5-*6 (N.D. Cal., Feb. 8, 2010).

253 See, e.g., Hilton v. Hallmark Cards, 580 F.3d 874 (9th Cir. 2009).

254 Davis, 2012 WL 3860819, at *7; Gionfriddio v. Major League Baseball, 94 Cal. App. 4th 400, 410 (2001); Dora v. Frontline Video, Inc., 15 Cal. App. 4th 536, 543 (1993).

255 Lerman v. Flynt Distrib. Co., 745 F.2d 123, 131-32 (2d Cir. 1984).

256 E.g., C.B.C. Distribution & Mktg., Inc. v. Major League Baseball Advanced Media, L.P., 505 F.3d 818, 823-24 (8th Cir. 2007); Chapman v. Journal Concepts, Inc., 528 F. Supp. 2d 1081, 1084-85, 1096 (D. Haw. 2007); Time Inc. v. Sand Creek Partners, L.P., 825 F. Supp. 210, 213 (S.D. Ind. 1993).

257 Fraley v. Facebook, 830 F. Supp. 2d 785, 804-05 (N.D. Cal. 2011).

258 Messenger ex rel. Messenger v. Gruner Jahr Printing & Publ'g, 727 N.E.2d 549, 552 (N.Y. 2000) (internal quotation marks omitted).

259 Montana v. San Jose Mercury News, Inc., 40 Cal. Rptr. 2d 639, 642, 643 n.2 (Cal. Ct. App. 1995).

260 See supra Part III.B.

261 See supra note 2 and accompanying text.

262 See Mark Bartholomew, A Right is Born: Celebrity, Property, and Postmodern Lawmaking, 44 Conn. L. Rev. 301, 309-11 (2011).

263 See Richards, supra note 28, at 1155.

264 See id.

265 West, supra note 47, at 628.

266 Diane L. Zimmerman, Requiem for a Heavyweight: A Farewell to Warren & Brandeis's Privacy Tort, 68 Cornell L. Rev. 291 (1983).

267 New Kids on the Block v. News Am. Pub., Inc., 971 F.2d 302, 309-10 (9th Cir. 1992).

268 Hoffman v. Capital Cities/ABC, Inc., 255 F.3d 1180, 1185-86 (9th Cir. 2001).

269 Fraley v. Facebook, 830 F. Supp. 2d 785, 805 (N.D. Cal. 2011).

270 Ghosh, supra note 79, at 705-06; Tamara R. Piety, ''A Necessary Cost of Freedom"? The Incoherence of Sorrell v. IMS, 64 Ala. L.

Rev. 1, 5 (2012).

271 ETW Corp v. Jireh Publ'g, Inc., 332 F.3d 915, 955 (6th Cir. 2003).

272 Hebrew Univ. of Jerusalem v. Gen. Motors, 903 F. Supp. 2d 932, 937 (C.D. Cal. 2012) (internal quotation marks omitted).

273 Id. at 933.

274 Id. at 941.

275 Id. at 937.

276 See Sorrell v. IMS Health, Inc., 131 S. Ct. 2653, 2671 (2011).

277 Cardtoons v. Major League Baseball Players Ass'n, 95 F.3d 959, 970 (1996).

278 Id. at 272.

279 Id. at 974-75.

280 Davis v. Electronic Arts, Inc., No. 10-03328 RS, 2012 WL 3860819, at *6-*7 (N.D. Cal. Mar. 29, 2012); Dora v. Frontline Video, Inc., 15 Cal. App. 4th 536, 543-44 (1993).

281 See, e.g., Cher v. Forum Int'l, Ltd., 692 F.2d 634, 637 (9th Cir. 1982); Falwell v. Penthouse Int'l, Ltd., 521 F. Supp. 1204, 1210 (W.D. Va. 1981); Current Audio, Inc. v. RCA Corp., 337 N.Y.S.2d 949, 953-55 (Sup. 1972).

282 Peter Swire, Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment, 90 N.C. L. Rev. 1371, 1400-02 (2012).

283 Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228 (10th Cir. 2004).

284 Rosen, supra note 14, at 88; Swire, supra note 282, at 1400-01.

285 See Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the International Association of Privacy Professionals Second Annual Conference: The FTC and Consumer Privacy Protection (Dec. 7, 2010), available at www.ftc.gov/speeches/brill/101207iapp.pdf.

286 Swire, supra note 282, at 1400-02.

287 Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011)

288 See supra Part II.C.

289 See, e.g., Malcolm Burnley, How to Protect Your Privacy Online, Atlantic, June 2013 (describing browser add-ons that display icons informing online users as to how each Web site visited will treat their data); Drew Olanoff, Burn Note Comes Back with a Vengeance, Aims to Protect Your Private Messages with New Mobile Apps, TechCrunch (Mar. 26, 2013) (discussing concept of "ephemeral messaging," whereby emails, photos, and other shared data are automatically destroyed after a set period of time), available at http://techcrunch.com/2013/03/26/burn-note-comes-back-with-a-vengeance-aims-to-protect-your-private-messages-with-new-mobile-apps/; Ryan Tate, Why Facebook Would Pay $3 Billion for Snapchat (And Why It Shouldn't), Wired, Nov. 13, 2013 (discussing Snapchat and potential difficulties in integrating it with Facebook).

290 See Hart v. Electronic Arts, Inc., 717 F.3d 141, 166 n.39 (3d Cir. 2013).

2013 WL 3759820

Aspatore
***1** August, 2013

UNDERSTANDING THE LEGAL ISSUES OF COMPUTER FORENSICS
LEADING LAWYERS ON UNDERSTANDING REGULATIONS CONCERNING THE COLLECTION, PRESERVATION, AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

THE GLOBALIZATION OF PRIVACY AND SECURITY IN CYBERSPACE: GOVERNMENT, LAW, AND SOCIETY IN THE TWENTY-FIRST CENTURY ONLINE WORLD

Nicholas W. Allard[a1]

Joseph Crea Dean and Professor of Law, Brooklyn Law School, and Partner
Patton Boggs LLP

Introduction

By 2030, everyone will need basic scientific and technology literacy to interact with the government and enjoy a reasonable and rising quality of life. Advanced nations have always required there to be a certain number of scientists and inventors. In contrast, the near future, to be enfranchised, for society to function, all citizens will require basic information technology literacy. The key to a productive and inspired citizenry will be giving every citizen access to affordable advanced mobile broadband communications and ensuring they have a working understanding of how to use it. This observation, which is increasingly commanding the attention of global think tanks, educators, and policymakers, is fundamental to the future of our society. It will also completely overhaul the very nature of government, law, and the practice of law. Because of the impact of technology on the rule of law and how it is practiced, it will drive how government officials and practicing lawyers alike operate to bring order from disorder. At the same time, as online activities by organizations and an online presence by individuals become de facto mandatory and universal, governments and lawyers must deal with finding multinational solutions to privacy and security data protection laws for the world because geopolitical boundaries are completely porous to the flow of data over computer networks.

Impact of Technology on Government and its Implications for Legal Advocacy about Lawmaking and Policy

The International Four-Dimensional Chess Game

It is a cliché to say the world is increasingly a global community. Due to advanced online networks more than ever before, legal skills are needed to address the multinational nature of issues. First, and most obviously, there are more multinational interests: Overseas firms, for example, that wish to expand and invest in the United States, and US-based concerns that have interests abroad. These global players require sophisticated multinational government advocacy representation. They also require expert compliance advice and risk assessment among other needed government relations and regulatory services, especially those relating to privacy and security.

Second, on many large issues, such as financial regulatory reform, and climate change or energy policy, for example, the policy advocacy has become a three-or four-dimensional chess game. The core reason that the G7 became the G20 was because it was understood that it is not possible to effect financial regulatory changes unilaterally. Washington cannot act alone unless London, Brussels, and Asia are moving in roughly parallel directions. The same can be said for spectrum policy, Internet privacy and security, and a host of other issues. Consequently, if you want to influence the US government on privacy or security rules, it helps to persuade other governments, including the so-called BRK countries, and vice versa.

New Technology: Broadband Interconnectivity

***2** Another major change is that increasingly the public interacts with the government electronically, often directly, without a middleman. The "face-to-face meeting" by a lawyer representing a client with an official and simply providing raw information to clients, such as texts of bills and hearings, are diminished in value. This puts a premium on expert analysis of ever increasingly available information, as well as professional advice and advocacy. There are also powerful new advocacy techniques that we are only beginning to fully appreciate. Witness how Google and others stopped the proposed anti-piracy legislation in its tracks recently. Consider that the powerful Motion Picture Association of America backed the Stop Online Piracy Act (SOPA). In 2012, this legislation was a train on a fast track, supported by the powerful Hollywood studio interests, but it was killed overnight by new media techniques. Internet users also managed to block the Cybersecurity Act of 2012 with online grass roots techniques. The activities, cyber lobbying, will increase as the one-hundred thirteenth and later congresses take up several privacy/security measures such as updating and reform to 1986 laws; the Electronic Computer Fraud and Abuse Act[1] and the Electronic Communications Privacy Act (ECPA).[2] Consider also how President Obama uses very effectively, as do many increasingly political campaigners, new media to campaign and raise money. Similar techniques can be used in legal and government relations advocacy campaigns.

Some Other Big Questions

Q: Do we run the government like *American Idol*?

A: We essentially have the technological capability to run a referendum on innumerable issues. But should we? The issue of whether government officials are mere delegates or representatives is not new. Hopefully, we will remember the wisdom of Sir Edmund Burke, who told the electors of Bristol in 1774, "your representative owes you, not his industry only, but his judgment, and he betrays, instead of serving you, if he sacrifices it to your opinion." (Of course, Sir Edmund did, in fact, lose his next election.)

Q: Do we treat all blogs and Tweets alike? Those with money and new media savvy can flood the media with their messages and drown out others who lack the online means to join "the great melody" of public discourse.

A: The answer is that the government is wrestling with how best to weigh and evaluate all the input it now seeks and receives electronically outside the time-worn contours of the traditional legislative and administrative process. Law journals are filling up with articles discussing whether and how electronic comments and blogs should be considered and weighed within the dusty four corners of the Administrative Procedures Act.

Q: What do we do about the information "have-nots"? Without access to affordable new mobile broadband technology and the know-how to use it, technology "have-nots" lack the keys to both opportunity and participatory democracy.

***3** A: It is imperative to find ways to close, what we used to call and still should, the digital divide to prevent them from becoming disenfranchised. Lawyers also can play a role in ensuring that the voices of the less advantaged are heard, and helping all to be heard effectively.

Impacts of Technology on the Legal Profession and Legal Education

The recent economic downturn--i.e., the so-called "Great Recession"--has placed enormous pressures on the practice of law, but that pressure only exacerbated cracks that were being opened and driven by the increasingly disruptive power of technology. Indeed, technology changes the way in which all types of business are conducted--including the practice of law. Today, clients are increasingly less inclined to pay lawyers to perform certain tasks. For instance, they are not going to pay for new lawyers to be trained, to learn on the job, and they are not going to pay for work such as routine searches, proofreading, basic document management or scheduling, that software and non-lawyers can just as effectively and more efficiently accomplish.

The good news is that clients still need and are willing to pay for expert advice, analysis, and advocacy--what I call the "Three

A's.'DD' In other words, they still need people who have legal skills to apply critical thinking to a problem, and to exercise their experience and judgment in solving that problem. I believe that this trend indicates that the practice of law is shifting and becoming an increasingly worthwhile profession, because lawyers must now practice at a very high level. In fact, the legal profession has been fundamentally changed in dramatic ways by technology--i.e., it increasingly involves the supervision of people who are non-lawyers, such as the increasingly routine practice of lawyers managing massive electronic discovery projects with teams of non-lawyers, and it is likely to explode into new fields such as risk management or the field of legal computer forensics, which did not exist a decade ago.

Technology has also had an impact on the area of legal education. *New York Times* columnist and author David Brooks recently analyzed, with respect to all university and colleges, the dichotomy between practical and theoretical training, and how practical training is something that is not necessarily teachable or obtainable through technology. Rather, it depends on experience and hands-on human interaction; while the more theoretical, lecture-type training that universities typically rely on may soon become obsolete. Consequently, it is likely that in the next twenty to thirty years we will see a fundamental overhaul in terms of the educational process that turns law students into lawyers. Legal educators everywhere are considering innovative ways to provide professional training through practical experiential learning, how to prepare new lawyers for how computers are used as a tool in practice, and how consistent with somewhat outdated ABA and state bar rules, to appropriately educate students online.

***4** In summary, broadband/mobile technology is fundamentally overhauling our system of government, our democracy, the nature and practice of law, and the nature of legal education. It has also contributed to a virtual shrinking of the globe, and the erasure of the significance of borders in the practice of law, which now has a much more international aspect. At the same time, we have seen a major shift toward pressure for instantaneous decision making in the business world and a trend to instant gratification in all aspects of life, a phenomenon that challenges the profession to keep up while infusing client services with quality and ethics.

Understanding Privacy and E-commerce Issues in the Cyberlaw Realm

A major technology-based substantive trend that is impacting the legal profession at this time concerns the rising importance of privacy and security issues and concerns--issues that all lawyers need to address. Personally, I believe that the civil rights issue of our age is equal and fair access to education, while the civil liberties issue of our age is privacy--and we are just beginning to come to grips with the significance of that issue in the face of advanced technology. The flip side of that trend involves the need for the US and other governments to address all of the issues that are posed by security threats emanating in the online world.

Government officials are just beginning to grasp that online privacy is a tremendous concern, and that we need new rules of the road to address the threats to privacy that exist because of our new digitized, online networked forms of communications. A very powerful book, *The Virtue of Forgetting in the Digital Age*,[3] posits that throughout most of the history of mankind, it was always easy to forget and hard to remember, but now with the advent of interconnected computer networks and databases it is easy to remember and hard to forget. Mayer-Schönberger, both an Oxford don at the Oxford Internet Institute and an accomplished lawyer, proposes a number of very practical steps that would make it harder to freely access someone's personal information, and easier to "forget" private information collected digitally. These include requiring those who collect the data to delete it over time, incorporating into electronic storage devices, like cell phones, cameras, and computers, automatic delete functions that work automatically after pre-set expiration dates, and for mechanisms for individuals to choose their own privacy settings--settings that determine the degree and terms for maintaining and sharing information prior to giving it up. In brief, software, practices, and laws that make it a little easier to forget in the digital age.

It is important to keep in mind that there is a new and vast array of international and national laws pertaining to privacy and security on the Internet--and if you operate an online business you have to assume that the laws in other jurisdictions might well apply to you. Around the world, there are at least three fundamentally different privacy regimes, and the privacy regime that we are familiar with in the United States is not the general rule in other countries. We believe that freedom of speech and the right to know is more important than the right to privacy; the only exceptions where we have great areas of consensus are with respect to protecting private information concerning children, financial records, and health records. In Europe, on the other hand, protecting the privacy of all types of personal information is the general rule, with exceptions essentially involving informed consent. Meanwhile, in totalitarian regimes, the government has total control over the distribution of information, and the concept of protecting the personal privacy of information is totally anathema to the interests of the state.

***5** Within the United States alone, there are many seemingly inconsistent laws with respect to information privacy and security. For example, when you discover that your database has been hacked into by an unfriendly party, you need to keep in mind that there are forty-six different state laws in the United States that address what your obligations are in terms of notifying your customers about such a security breach. Therefore, it is extremely important for clients to work with a good lawyer who understands completely the constantly changing overlapping privacy and security rules that apply to businesses and who can help them figure out how to navigate those rules. A new trend is the increasing concern over companies that collect information, even """"public" information such as people's location in stores, roadways and public transportation, the use of computer monitors by customers, tracking personal computer searches, and retail shopping and acquisitions. This area of concern will proliferate new enforcement cases, precedents, and regulations. Several bills have already been introduced in both the US House and Senate concerning geo-positional privacy and restructuring law enforcements' right to access e-mail without a warrant.

Helping Clients Navigate Information Privacy and Security Regulations

To help clients navigate the myriad information privacy and security regulations that apply in cyberspace, a lawyer should first try to understand the client's business and try as best as possible to find common ground among the different laws that may apply to it. It certainly helps to have an international, global perspective on this issue, and to understand the client's business objectives. You need to minimize the client's risk of non-compliance and help the client figure out the best course of action when it comes to developing an information privacy/security compliance plan. An important approach is to build into the management culture of a company, its governance software, if you will, the capacity to consider and adhere to privacy and security issues on a daily, dynamic basis. The most common error companies make is to adopt privacy policies, disclose them, and then either disregard them or fail to update them as the company's business model changes. This conduct has been and remains an enforcement priority for the Federal Trade Commission (FTC) and state attorneys general--who red-flag companies that say they will treat personal information a certain way, but in practice do something different. Another good approach is to adhere to the basic privacy principles that more or less are universal across national and state borders: notice, consent, review and correction, security and enforcement or redress.[4]

Unfortunately, in many companies, the concept of information security/privacy compliance is not a high priority, or the chief privacy officer is not completely engaged with what is happening on the business side of the company. Most successful businesses are dynamic and change on a frequent basis; therefore, a privacy policy has to be dynamic, vibrant, and capable of change as well--it cannot be static. If a company adopts a privacy policy but it is not really part of its corporate business operations and management, and it does not check compliance regularly, then the company is headed down a risky path.

***6** Also, there are increasing numbers of new and entrepreneurial online ventures emerging--and all too often, the managers of those businesses do not engage lawyers at the take-off point; they only hire them once their business crashes to help them with the clean-up process. Consequently, one challenge for privacy lawyers in this practice area is to be more amenable and useful to entrepreneurs at the launch of an online business. Likewise, online entrepreneurs need to understand that there is some value in embracing lawyers at the beginning stage, especially if they are planning an innovative global business venture. This is especially so with regard to privacy and security issues. In the wildly competitive and ever changing cyber markets, those businesses that are branded as safe, reliable, and fair with regard to personal privacy and security should have an advantage and be sought out by customers.

Understanding New Computer Crime and Intellectual Property Laws and Protections

It is also important for both lawyers and clients who operate in this area to keep in mind that the laws applicable to computer crime and the protection of intellectual property (IP) in the online realm are in need of serious updating, as they are not sufficiently technology neutral. Basically, the laws still on the books are too wedded to the past, and they are not adequate to deal with the new issues that exist in this area. That is why Congress and the current administration are taking a hard look at making a number of changes to update these laws.

I believe that you should never assume that you know what the rules are in this area. Rather, you must constantly check to see whether the rules that are applicable to protecting children's privacy online have been updated, as the Federal Trade

Commission (FTC) has just done.[5] Likewise, it is important to be aware that the White House adopted a new executive order in February relating to cybersecurity.[6] If you are entering into a new online business venture, you also need to be aware that there are a number of proposals to amend and update the Computer Fraud and Abuse Act. Proposed amendments to EPA would for example, ensure that privacy protections apply to the content of social media that did not exist at the time the statute was enacted, and that e-mails older than 180 days get greater protection than available under current cases and practice. In addition, we have recently seen the passage of the Cyber Intelligence Sharing and Protection Act, and it is quite possible that some changes will be made with respect to that statute. Proposals under consideration would expand exceptions to privacy laws for intelligence, anti-terrorism, and law enforcement purposes. Notwithstanding serious concerns from civil liberty and consumer groups, anti-hacking legislation is also on the table, and we very much need a federal cyber breach notification law--largely because we have forty-six different state laws that need to be consolidated so that we will have some clear rules of the road in that area.

***7** To date, many if not most of the so-called cyberlaw privacy bills deal with either corporate intellectual property or security, or protection of government functions, as opposed to individuals' rights and liberties. Curiously, there is not yet a powerful, vocal constituency for the protection of individual privacy in the United States. There are privacy think tanks, groups, and advocates, but there is no single group that is arguing for greater privacy protection comparable to other consumer or civil rights groups. The American Civil Liberties Union (ACLU) speaks out in a very powerful way about freedom of speech and some privacy issues, but there is much more effective lobbying and an alignment of interests with respect to security and corporate IP issues that are implicated by online business ventures than there are efforts aimed at protecting individual rights and liberties in cyberspace. This may be changing as people become more aware of their exposure to increased means to monitor their location, behavior, and communications on a minute-by-minute basis.

Jurisdiction Issues in Cyberspace

The traditional concepts of jurisdiction and conflicts of law are rapidly evaporating in the cyberspace era, because online technology knows no borders. Therefore, you should probably assume that the rules of different jurisdictions with respect to online privacy and security are potentially applicable to your business dealings on the Internet. The enforcement of those rules is limited by some fundamental due process rights--i.e., whether there is some minimal fair basis to contend that the rules of a particular jurisdiction should apply in a given situation. That said, the advance of global interconnected technology has greatly undercut the due process check on multiple jurisdictions claiming relevance to a particular issue. Companies that do business online must do so in an atmosphere of legal chaos, governed by the applicability of myriad legal systems.

Most businesses are operating in a global market these days; far fewer businesses are completely local--even businesses that are not multi-jurisdictional will often cross jurisdictions in their communications. While it is not possible to research every applicable law of every geopolitical entity, it is possible to make reasonable and prudent guesses about compliance and legal exposure by considering factors such as where a client maintains a physical presence, the location of employees, and the location of assets and flow of financial assets. This, as Winston Churchill famously once said, is not the end, or the beginning of the end, but it is the end of the beginning of needed legal analysis.

Conclusion

Efforts aimed at protecting the security and privacy of information in the Unite States are on a slower track than they are in the rest of the world--and, this is largely because so far the United States does not yet have an organized and determined public constituency that is advocating for the protection of individual privacy rights. In addition, the issue of information security is a ticking time bomb; there are probably many large and medium-sized companies in the United States that are not even aware that their data has been compromised by industrial or governmental espionage or criminal activity. Personally, I am very concerned about the integrity of our nation's critical infrastructure, and I think that these are issues that need to be addressed in a comprehensive and forthright manner at the national and international level, and with great alacrity and purpose.

***8** As noted, there has been some progress in this area. For instance, the FTC recently issued new rules under the Children's Online Privacy Protection Act; proposed amendments to the Cyber Intelligence Sharing and Protection Act which are still pending; the Department of Justice (DOJ) has proposed amendments to the Consumer Fraud and Abuse Act; the Department of Commerce has issued a notice of inquiry to encourage companies to engage in voluntary cyber security programs; and the

Pentagon is finalizing rules of engagement that will clarify the authority the military has with respect to responding to an enemy cyber-attack. At the same time, the Electronic Computer Privacy Act of the 1980s that Senator Leahy originally proposed needs to be updated and made apparent to ever advancing technology and usage. Many other privacy initiatives are currently pending in the United States and abroad.

If you want a really interesting legal career where you can make a difference, and where the law will be evolving rapidly in a very exciting and important way, then you should do everything you can to become an expert in **cyberprivacy** and cybersecurity. If you are a young lawyer or someone who is just graduating from law school, you have a great opportunity to get in on the ground floor of a practice that will be incredibly important for the next two to three generations. My personal advice for those getting started is to read history, and to start by considering books such as those of Professor Mayer-Schönberger and Tom Standage, the author of *The Victorian Internet* (1998). You will learn that many, if not most, of the questions encountered today have been experienced over the ages every time new communications technology is introduced. As the saying goes, in some respects, for all the marvel of digital technology, there is no new thing under the sun.

Key Takeaways

• Keep in mind that there is a new and vast array of international and national laws pertaining to privacy and security in the Internet realm--and if you operate an online business you have to assume that the laws in other jurisdictions apply to you. Assist clients in navigating all of these different and often apparently inconsistent rules.

• Understand the client's business to determine different laws that may apply to it. Minimize the client's risk of non-compliance and help the client ascertain a practical, workable course of action when it comes to developing an information privacy/security compliance plan.

• Inform clients that they may need to give adequate notice to their customers in the event of a security breach of personal information on corporate data bases, but the rules vary dramatically state-by-state and depending on the facts. Clients must also ensure that what they say about their privacy policy is consistent with what they actually do. A privacy policy that is adopted and enforced internally has to be dynamic, vibrant, and capable of change--it cannot be static.

***9** • Be more amenable and useful to entrepreneurs at the launch of an online business; and help online entrepreneurs understand that there is some value in embracing lawyers to help with privacy issues at the beginning stage, especially if they are planning an innovative global business venture.

• Never assume that you know what the rules are in this privacy and security field, as they are changing rapidly. Keep abreast of changes to the laws that affect cybersecurity and privacy issues.

Footnotes

a1 *Nicholas W. Allard became the eighth Joseph Crea Dean of Brooklyn Law School on July 1, 2012. Since joining the Law School, he has been a champion for entrepreneurship and innovation both inside and outside of the classroom. He is also a powerful voice on the issue of graduate employment. A globally recognized expert in the field of legislative, regulatory, and administrative matters in the areas of telecommunications, information technology, health, energy, environmental law, and higher education, Dean Allard has been a partner at Patton Boggs LLP since 2005 and continues as a partner in the firm's New York and Washington, DC offices. At Patton Boggs, he chaired the Public Policy Department and co-chaired the Government Advocacy Practice. Before joining Patton Boggs, he was a partner at Latham & Watkins LLP, where he chaired the firm's Government Relations Group. He previously served as administrative assistant and chief of staff to the late Senator Daniel Patrick Moynihan and as minority staff counsel to the Senate Committee on the Judiciary, where he was legal counsel to the late Senator Edward Kennedy. Dean Allard began his career as a law clerk for Chief US District Judge Robert F. Peckham in San Francisco and for US Circuit Judge Patricia M. Wald in Washington, DC.*
Dean Allard has received multiple honors and awards including a top ranking in Government Relations by Chambers USA in 2012*; a 2010 Visionary Award from the* National Journal-Legal Times*; recognition as one of DC's Top Lobbyists by* The Hill *in 2008,*

2009, 2010, and 2011; and a Hermes Award for Contribution to Study of Communications from the Syracuse University College of Law. He is a Fellow of the ABA Law Foundation, a member of the American Law Institute, and serves on the ABA Standing Committee on the Law Library of Congress, the New York City Bar Association Task Force on New Lawyers in a Changing Profession, and the ABA Administrative Law Section Task Force on the Regulation of Attorney Lobbyists. Also, he is a trustee of the Shakespeare Theatre Company in Washington, DC. Dean Allard is a graduate of Princeton University, Oxford University (where he was also a Rhodes Scholar), and Yale University Law School.

Acknowledgment: *I am especially grateful to my colleagues in the Techcomm practice of Patton Boggs LLP, whose trailblazing work is at the forefront of practice in the field of advanced communications. I also thank the faculty and students of Brooklyn Law School who provide endless inspiration to thinking about where law is heading.*

1 P.L. 99-474 (1986).

2 18 U.S.C. § 2510 (2002).

3 Victor Mayer-Schönberger, The Virtue of Forgetting in the Digital Age (Princeton University Press 2009).

4 *See e.g.*, FEDERAL TRADE COMMISSION, PRIVACY ONLINE - A REPORT TO Congress (1998), *available at* http://ftc.gov/reports/privacy3/priv-23a.pdf.

5 *See* Press Release, Federal Trade Commission, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Children's Online Privacy Protection Rule, (Dec. 19, 2012) *available at* http://www.ftc.gov/opa/2012/12/coppa.shtm.

6 *See* Exec. Order No. 13636, 78 FR 11739 (Feb. 12, 2013).

ASPATORE

End of Document