Cyberspace law covers a lot of territory. Virtually every legal issue that is relevant to a business lawyer must be examined afresh when digital networked communications technologies become involved. Due to the breadth of that territory, our annual survey must be selective in subject matter as well as time. Nevertheless, the contributions to this year’s survey cover a wide range of topics: cybersecurity and privacy, social media, contracting and payments, copyright, intermediary liability, and ransomware.

Cybersecurity and privacy. Cybersecurity intrusions have continued to plague both businesses and governments. David Silverman reviews the somewhat confused landscape of decisions about the sorts of harm that will confer Article III standing on a plaintiff whose personal information is compromised in a data breach. While some courts denied standing despite allegations of actual misuse of the exposed information, other courts found that a heightened risk of future injury could constitute sufficient injury for standing. Silverman also discusses the courts’ treatment of various theories of damages arising from exposure of personal data, as well as contract claims predicated on incorporation of privacy policies and on business associate agreements.

The contribution by Roland Trope and Lixian Hantover focuses on the erosion of trust in the security of computer-based data systems that has resulted from the frequent reports of cybersecurity intrusions, citing as examples the theft of Bangladesh Central Bank funds via the SWIFT money transfer system, the theft of virtual currency tokens from an online venture-capital fund, and Volkswagen’s “dieselgate” compromise of the emissions-control systems in its own vehicles. The authors also discuss the Seventh Circuit decision in Remijas v. Neiman Marcus Group, LLC, which is helpful for plaintiffs seeking to establish Article III standing in a data breach suit, the California attorney general’s data security recommendations, a case against money transmitter Dwolla for false claims about its data security practices, and the federal Defend Trade Secrets Act of 2016.

* Associate Professor, Wayne State University Law School.
The next two essays address privacy developments. John Black and James Steel begin with the U.S. Supreme Court’s decision in *Spokeo, Inc. v. Robins*, which addresses the requirements of Article III standing in the context of a civil action under the Fair Credit Reporting Act. The Court’s clarification of the “concreteness” requirement is relevant to a wide range of statutory causes of action. Black and Steel go on to discuss some notable privacy enforcement actions by the Federal Trade Commission and other government agencies, as well as actions brought by private parties. They end with a discussion of some key legislative developments, including enactment of the USA Freedom Act of 2015, which extends certain provisions of the Patriot Act while imposing limitations on the bulk collection of telecommunication metadata in the wake of Edward Snowden’s disclosures.

In his contribution, Gregory Voss reviews several important privacy-related developments in Europe. He first offers a summary of the major provisions of the recently adopted General Data Protection Regulation, a comprehensive data privacy law that will replace the Data Protection Directive, which has been in place since 1995. Voss next discusses the invalidation by the Court of Justice of the European Union (“CJEU”) of the EU-U.S. Safe Harbor, which was instituted in 2000 to allow transfers of data between the European Union and the United States that would meet the requirements of the Directive, and its replacement by a new system called the EU-U.S. Privacy Shield. Finally, Voss addresses ongoing controversies arising from the CJEU’s 2014 decision requiring search engines to “delist” search results pointing to outdated prejudicial information at the request of a natural person.

**Social media.** Christopher Hart begins with a discussion of an ongoing lawsuit testing whether an “appropriation” artist may help himself to photographs posted on Instagram and create his own works based on them. He next assesses the impact of an FTC Policy Statement on “native advertising” and other types of advertising that frequently appear on social media, which are formatted in such a way that they do not appear to be advertisements. Next, he looks at several applications of the First Amendment’s Free Speech Clause to government action restricting social media postings, including a state law that prohibits the posting of a filled-out ballot in online media. Finally, he addresses some workplace and discovery issues involving social media.

**Contracting and payments.** Nancy Kim surveys the current crop of cases dealing with online contracting. As she explains, these cases do not change the basic rules for determining whether there was assent to an online contract, but rather introduce additional nuance into the application of these rules. The focus in

---

these recent cases is on website design and the presentation of contractual terms. The courts demand persuasive evidence that the purported contract was actually presented to the consumer, differentiate between types of notice based upon their purpose, and closely scrutinize the presentation of terms to assess whether a reasonably prudent user would be aware of them.

The next essay, by Stephen Middlebrook, Tom Kierner, and Sarah Jane Hughes, focuses on several developments relating to electronic payments and their regulation by federal and state law. The piece discusses guidance from the Federal Deposit Insurance Corporation about brokered deposits, from several agencies on customer identification program obligations of banks that issue prepaid cards, and from FinCEN applying to nonbank sellers of prepaid cards. After touching on the Seventh Circuit’s disapproval of a sheriff’s effort to coerce Visa and MasterCard into withholding payment services from an online forum for adult services, the authors cover developments relating to virtual currencies, daily fantasy sports operators, and the potential personal liability of corporate compliance officers for the company’s failure to follow anti-money laundering rules.

Copyright. In his contribution, Jonathan Rubens reviews developments involving copyright law. He begins with three cases on fair use. In the first, the Second Circuit upheld the district court’s determination that Google’s book digitization activities were non-infringing fair use of the books. In the second, the Eleventh Circuit holds that online publication of a photograph that the subject (who was the copyright owner) considered unflattering was fair use. In the third case, a district court upheld a jury verdict finding that Google’s use of the Java APIs in its Android platform was fair use. Rubens goes on to discuss a case on what constitutes good faith in the submission of a takedown notice under the Digital Millennium Copyright Act’s safe harbor system, and he reviews the most recent triennial rulemaking under the DMCA’s anticircumvention provisions.

Intermediary liability. Venkat Balasubramani surveys new decisions applying the Section 230 immunity for online service providers. After beginning with a set of cases that have applied Section 230 in a straightforward manner, Balasubramani discusses cases that have denied the defense on the grounds that the intermediary had a role in creating the challenged content or did not act as a neutral conduit. Next is a discussion of several cases in which the plaintiff seeks to overcome Section 230 immunity by alleging actions by the intermediary other than content creation. The final section deals with cases in which the First Amendment played a role.

Ransomware. Lastly, Edward Morse and Ian Ramsey deliver a primer on the growing menace of ransomware—malicious software that encrypts the data on

---

the victim’s computer and then conveys a demand for a money payment as the price for restoring access to the data. The authors set out some of the legal risks that a victim contemplating paying the ransom must bear in mind. They have suggestions as to the types of assistance that are available from government agencies and recommend measures that will reduce the likelihood of a successful ransomware attack.

Developments in Data Security Breach Liability

By David L. Silverman*

I. INTRODUCTION

It was another very active year in the federal courts on the class action data security breach front, although we have yet to see a case of this type go to trial.1 In November 2015, Target settled with the consumer class for $10 million plus $6.75 million in attorney’s fees.2 In May 2016, it settled with the last third of the issuing banks, the ones that did not accept the settlement brokered by the credit card companies, for nearly $60 million, with just under $20 million in fees and expenses for plaintiffs’ counsel.3 Home Depot settled its consumer claims at $19.5 million for damages and prevention plus around $8.5 million in fees and costs.4 These high-dollar settlements have presumably stimulated enthusiasm for these cases among the plaintiff’s bar, although the initial hurdles remain high, and the uncertainty of prevailing on the merits has led to some lower-than-expected settlements.5 Meanwhile, in the courts the battle raged on over when the heightened risk of future harm from a data breach confers standing, and new ground was broken on such issues as incorporating privacy notices into contracts of insurance and third-party beneficiary status against health insurance plan administrators.

---

II. STANDING

A well-pleaded instance of actual data misuse, such as identity theft or fraud, resulting from a data security breach will usually state an injury in fact sufficient for Article III standing, but 2015–2016 produced a few opinions that denied standing in spite of alleged actual misuse. The related issue of whether heightened risk of future harm may alone be sufficient remains controversial, without even a consensus on whether the circuits are split, and this year also featured grants of standing to plaintiffs who had yet to see any misuse. Claims based solely on heightened risk from a defendant’s weak data security, absent any breach or misuse, remain subject to dismissal. The idea that actual misuse of the data security breach plaintiff’s data is a prerequisite for standing likely received additional support from the U.S. Supreme Court’s recent decision in Spokeo, Inc. v. Robins, which held that even when the legislature says a particular injury creates a private right of action, to be considered “concrete” for standing purposes, the injury “must be ‘de facto’; that is, it must actually exist.”

Cases such as In re: SuperValu, Inc., Customer Data Security Breach Litigation reflect the strict approach to standing. The grocery chain, which also provided payment processing for Albertson’s stores, suffered two separate breaches involving malware installed on its payment card transactions server, but only one named plaintiff claimed to have suffered a fraudulent credit card transaction. The fact that someone installed malware specifically to gather payment data suggested nefarious intent, and other courts have ruled that when data thieves have expended substantial time and effort, the risk of future harm is more imminent. However, the SuperValu court considered the single instance of misuse

6. For the idea that pleading actual misuse and consequent damages establishes standing, see, for example, Resnick v. Avmed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).
9. 136 S. Ct. 1540, 1548 (2016) (FCRA violation). Like a data security breach plaintiff with no actual misuse, the plaintiff in Spokeo complained of the risk that a wildly inaccurate profile of him in the defendant’s database would lead to adverse consequences, such as denial of employment. Justice Ginsburg’s dissent agreed that the risk of future harm made the injury sufficiently concrete. Id. at 1555–56 (Ginsburg, J., dissenting).
11. Id. at *1–2.
unpersuasive with respect to the risk of future harm.\textsuperscript{13} Later-acquired evidence of other instances of misuse, introduced on a motion to reconsider, was excluded.\textsuperscript{14} Similarly, in Whalen v. Michael Stores Inc., two instances of attempted credit card fraud in a foreign country, supposedly resulting from an attack on the retailer’s payment processing system, were insufficient for standing.\textsuperscript{15} The risk of further fraud was not “certainly impending” because the plaintiff had canceled the affected card and suffered no out-of-pocket loss from the two attempted instances.\textsuperscript{16} In the Zappos.com data breach litigation, most potential plaintiffs were dismissed without leave on their third attempt because a single instance of unauthorized access to a named plaintiff’s contact list and its subsequent use for spam was insufficient to allege injury in fact.\textsuperscript{17} Two new named plaintiffs with more substantive allegations of actual fraud pleaded injuries, but overly broad class allegations were stricken; any fourth amended complaint must narrow the class to cases of actual fraud, identity theft, or the like.\textsuperscript{18}

One way to neutralize a pleaded instance of actual misuse is for lack of causation, as in Fernandez v. Leidos, Inc.\textsuperscript{19} This case involved backup tapes stolen from a parked car. The encrypted tapes, which required specialized software for access, contained health insurance data of military personnel: Social Security numbers, home addresses, birthdates, and medical information. One named plaintiff claimed actual identity theft because his credit report showed unknown addresses and unfamiliar large purchases as well as an attempt to open a bank account in his name. Denying standing, the court ruled that the alleged misuse as pleaded was not “fairly traceable” to the data breach\textsuperscript{20} and that the opportunistic nature of the underlying crime made the risk of future harm less than certainly impending.\textsuperscript{21} Identity thieves may aggregate data from multiple sources, so causation in these cases is fact-specific and rarely amenable to resolution on a motion to dismiss.\textsuperscript{22}

\begin{itemize}
  \item \textsuperscript{13} SuperValu, 2016 WL 81792, at *6–7.
  \item \textsuperscript{14} In re: SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586, 2016 WL 1588105 (D. Minn. Apr. 20, 2016) (denying motion to reconsider), appeal docketed, No. 16-2378 (8th Cir. May 26, 2016).
  \item \textsuperscript{15} No. 14-CV-7006 (JS) (ARL), 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015), appeal docketed, No. 16-352 (2d Cir. Feb. 5, 2016).
  \item \textsuperscript{16} Id. at *5.
  \item \textsuperscript{17} In re Zappos.com, Inc., Customer Data Sec. Breach Litig., No. 12-MDL-2357, 2016 WL 2637810, at *3 (D. Nev. May 6, 2016) (hereinafter Zappos II).
  \item \textsuperscript{18} Id. at *4 (finding injury in fact), *8 (striking class allegations).
  \item \textsuperscript{19} 127 F. Supp. 3d 1078 (E.D. Cal. 2015), appeal docketed, No. 15-17285 (9th Cir. Nov. 19, 2015).
  \item \textsuperscript{20} Id. at 1086.
  \item \textsuperscript{21} Id. at 1087–88 (citing and following In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14 (D.D.C. 2014)).
\end{itemize}
Corona v. Sony Pictures Entertainment, Inc.\textsuperscript{23} illustrates the view that Clapper v. Amnesty International\textsuperscript{24} left room to grant standing to data security breach plaintiffs based on risk of future harm if the facts as pleaded are sufficiently egregious to make the heightened risk certainly impending. The Sony breach exposed sensitive information about the studio’s employees, such as Social Security numbers, bank account numbers, and medical information, and the data were widely circulated online. On these facts, the defense could not claim it was unknowable whether the data would ever be misused, so all the affected people had an injury in fact. The court concluded that “it was reasonable to infer that the data breach and resulting publication of Plaintiffs’ PII drastically increased their risk of identity theft.”\textsuperscript{25} Similarly, in Smith v. Triad, LLC, after a hospital employee stole patient data and sold it on the Internet, five separate instances of false tax returns were sufficient to establish injury in fact.\textsuperscript{26} Another egregious breach, this one involving a benefits administrator who left a database of Dillard’s employee information searchable online for a prolonged period, convinced the defense to postpone any challenge to standing and move instead to dismiss on other grounds in Dolmage v. Combined Insurance Co.\textsuperscript{27} The theft of multiple human resources laptops over a period of years by a rogue Coca-Cola employee, together with multiple alleged instances of identity theft and attempted fraud, was sufficient for standing in Enslin v. Coca-Cola Co.\textsuperscript{28} In the Home Depot data breach litigation, the defendant’s alleged choice to ignore repeated warnings made the breach seem egregious; given that, harm was foreseeable, and an independent duty arose under Georgia law that allowed potential recovery in tort despite the economic loss rule.\textsuperscript{29}

The U.S. Court of Appeals for the Seventh Circuit embraced the heightened-risk view of standing in Remijas v. Neiman Marcus Group, LLC and affirmed it in Lewert v. P.F. Chang’s China Bistro, Inc.\textsuperscript{30} The lower court in Lewert had granted the defense motion to dismiss for lack of standing, but the panel reversed the decision.\textsuperscript{31} The breach appeared less damaging than in Corona but similar to that in Remijas: it exposed credit and debit card data from the restaurant chain’s payment systems. One named plaintiff alleged four fraudulent transactions within two months of using his card at the defendant’s restaurant; the other observed no fraudulent charges and did not cancel his cards after using them at the

\begin{itemize}
\item No. 14-CV-09600 RGK (Ex), 2015 WL 3916744 (N.D. Cal. June 15, 2015).
\item 133 S. Ct. 1138, 1147 (2013).
\item Corona, 2015 WL 3916744, at *4.
\item 136 F. Supp. 3d 654 (E.D. Pa. 2015).
\item 819 F.3d 963 (7th Cir. 2016) (following Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015)).
\item Id.
\end{itemize}
same location. The Remijas panel found two kinds of future injury sufficiently imminent to satisfy the criteria for Article III standing: increased risk of fraud and increased risk of identity theft. The Lewert court followed Remijas in distinguishing Clapper on the facts because the interception of communications at issue in Clapper was speculative whereas the fact of the data breaches in Remijas and this case reified the risks of future harm. The Lewert panel quoted the inferential reasoning from Remijas that the primary incentive for hackers is “sooner or later to make fraudulent charges or assume those consumers’ identities,” so a substantial risk of harm may be inferred from the fact of the breach itself. Even in the Seventh Circuit, however, at least one court has declined to follow Remijas as incompatible with Clapper.

Judge Koh, whose approach to the heightened risk issue has now been embraced by the Seventh Circuit, addressed a question of class composition in the two Anthem rulings: when courts may assume there are class members in every state even if no named plaintiffs reside in that state. The defendants were the central administrator for Blue Cross/Blue Shield (“BCBS”) health insurers and plan administrators nationwide and various affiliated and non-affiliated BCBS entities from different states. Anthem, with its history of data security problems, was not a sympathetic defendant; the latest breach, in December 2014 and January 2015, exposed sensitive data from approximately 80 million people. The court had dismissed all claims against non-Anthem defendants against whom there were no factual allegations, but instead of finding named plaintiffs from these states, the plaintiffs amended the complaint to include enrollment data, which illustrated that non-Anthem BCBS affiliates typically had subscribers from other states. For example, although there was no named plaintiff from Illinois who had insurance through BCBS of Illinois, that entity was alleged to have enrolled over 200,000 California residents and over 80,000 New York residents. As such, the named plaintiffs from New York and California could stand for the class of people in both states who had business with this entity, keeping it in the case. The Anthem II court thus followed the

32. Lewert, 819 F.3d at 965.
33. Id. at 967.
34. Id. at 966. The court in Remijas held that time spent resolving fraudulent charges may be compensable even if the customer is not ultimately liable for those charges and that instances of identity theft may be the basis for compensation even if the victim suffers no monetary loss. 794 F.3d at 692 (“there are identifiable costs associated with the process of sorting things out”).
35. Lewert, 819 F.3d at 967.
37. In re Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953 (N.D. Cal. 2016) [hereinafter Anthem I]; In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783 (N.D. Cal. May 27, 2016) [hereinafter Anthem II]. At this writing Judge Koh’s nomination to the Ninth Circuit was pending Senate confirmation.
38. Anthem I, supra note 37, at 967 (noting that Anthem’s predecessor WellPoint suffered a data security breach in 2009 and the Department of Health and Human Services fined Anthem $1.7 million for alleged HIPAA violations in 2013).
39. Anthem II, supra note 37, at *5.
Target court, allowing the allegation that there were affected persons in every state to suffice at this early stage of the case.40

III. DAMAGES THEORIES

A. BENEFIT OF BARGAIN, OVERPAYMENT, AND “WOULD NOT HAVE SHopped”

The Sony Playstation Network case established in 2012 that people who provide their data in exchange for an otherwise free service cannot seek benefit-of-the-bargain damages for related purchases after exposure of the data.41 However, even when a contemporaneous payment is made, courts are skeptical of claims that a data security breach places those payments at issue. Depicting a portion of the payment as allocable to data security has proven difficult when the sale of goods (as opposed to services) is at issue and harder still when plastic card customers pay no premium over cash customers. The plaintiff-friendly opinion in Lewert ruled out reliance on such damages,42 as did the Whalen court;43 payments for services did not get a free pass in the Leidos, Case, and Chambliss cases. The Leidos court could not determine whether any portion of the insurance premium was intended to cover data security or that a higher premium would have bought better data security.44 Similarly, the Case court doubted that payments for hospital services “explicitly or implicitly included the cost of data protection,” emphasizing that most of the plaintiff’s hospital bill had been paid by her insurer.45 The Chambliss court found no meeting of the minds regarding allocating a portion of insurance premiums for data security.46

However, claims sounding in quasi-contract or contract, in which benefit of the bargain is the default measure, fit the overpayment theory better.47 Although contract damages must be quantifiable, the Anthem II court said failure to earmark part of an insurance premium did not make quantifying overpayment impossible; the inability to ascertain damages with mathematical precision at the outset of the case is not fatal if the fact of damages is well pleaded.48 The defen-

40. Id. at *6 (citing In re Target Corp. Data Sec. BREach Litig., 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014)).
42. Lewert v. P.F. Chang’s China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) (noting that theory is applicable only to defective or dangerous products).
47. Anthem I, supra note 37, at 985 (benefit of the bargain damages available for California UCL claims), 995–96 (also for claims under New York General Business Law § 349).
48. Anthem II, supra note 37, at *12–14.
dants in *Anthem II* argued that damages based on overpayment of insurance premiums would be barred by preemptive regulatory schemes. Such damages were barred with regard to the New Jersey contract claims by that state’s filed rate doctrine, which prohibits courts from entertaining challenges to regulated rates, but they were not barred by ERISA, which preempts state claims involving “benefits” (such as payments to health care providers) as distinct from premiums. Compare *Enslin*, which allowed a potential award in restitution even though the employees had made no payments to Coca-Cola, and contrast *Zappos.com*, in which data provided incident to sales transactions (even if inherently valuable) conferred no separate benefit on the retailer such as might support a claim for unjust enrichment.

**B. Remedial, Consequential, and Prophylactic Expenditures**

These cases typically include claims for expenditures to repair credit, obtain new payment cards, or purchase protective services; compensation for lost time is also sought. Such damages are duly rejected by courts that have already judged the risk of future harm to be less than certainly impending. The *Lewert* court said in *dicta* that these were one type of “easily quantifiable” damages the plaintiffs could recover. The *Corona* court rejected any claims for lost time but recognized actual prophylactic and remedial expenditures as compensable. The *Anthem II* court allowed potential prophylactic and remedial expenditures that it called “consequential.” It strongly condemned the defense argument that this type of damages was unjustified because for many plaintiffs, other data breaches might have been at play; allowing such arguments would create a perverse incentive for businesses to relax their data security measures.

**C. Loss of Inherent or Market Value of PII**

The claim that personal information has some intrinsic monetary value to the individual, quantifiable with reference to high prices on the invisible illegal market, has met with widespread skepticism, even when some data security breach...
class actions claims are allowed to proceed. 57 Usually, the defense prevails because plaintiffs have not alleged that they ever could have sold or intended to sell their personal information into such a market, and so they were not deprived of any inherent value. 58 The Anthem II court broke from this position and held that because such extensive PII as was stolen in the Anthem breach is demonstrably traded for value on the illegal market, exposing the information to that market causes an economic injury. 59 It was sufficient that there was an illegal market for the plaintiff’s information; it was not also required that the plaintiff intended to or could have sold her information in that market. 60 The Anthem II court also said that this type of damages would be available for the New Jersey contract claims because that state recognizes a property right in one’s name and likeness. 61

IV. CONTRACT DRAFTING AND FORMATION ISSUES

A. INCORPORATION OF PRIVACY POLICIES AND ANNUAL NOTICES

The court in Anthem I dismissed contract claims (with leave) because the plaintiffs failed to plead facts indicating that the privacy notices had been incorporated into the contracts, 62 and the Anthem plaintiffs took the hint. The California contract claim was among the ten selected for treatment on a motion to dismiss, and the defense maintained that the annual notices and other privacy policies were not part of the contract of insurance. 63 However, the summary of benefits expressly referred to the privacy statements, and that specificity pointed to incorporation. 64 The contracts stated that the insurer would handle information “subject to all applicable confidentiality requirements” and cited the Notice of Privacy Practices as encompassing its practices and policies with respect to information privacy and security. 65 The defense argued that an integration clause precluded incorporating the privacy policies; however, the clause as drafted failed in its purpose because it incorporated other documents that contained specific references to the privacy policies, making them part of the contract. 66 The defense also argued that the privacy policies, especially the annual notice, were not enforceable as merely articulating legal obligations imposed on the insurers by ap-

57. See, e.g., Lewert, 819 F.3d at 968 (“the only authority to which they direct us . . . says nothing of the kind”).
58. See, e.g., Zappos I, supra note 12, at 954 (complaint fails to explain “how [plaintiffs’] personal information became less valuable as the result of the breach”); Zappos II, supra note 17, at *3 (plaintiffs failed to plead facts showing loss of inherent value, so could not establish injury in fact; allegation that they would choose to sell PII, if choosing between such sale and misuse, was conjectural).
59. Anthem II, supra note 37, at *14.
60. Id. at *14–15.
61. Id. at *25–26.
62. Anthem I, supra note 37, at 979–81.
63. Anthem II, supra note 37, at *7–8.
64. Id. at *9 (“You have the right to receive a copy of the Notice of Privacy Practices.”).
65. Id.
plicable law. This argument failed because the policies did not expressly limit the insurer’s data privacy obligations to the requirements of applicable law but included comfort language that could be interpreted as promising to go further.67 In contrast, the Zappos.com court deemed the online retailer’s privacy policy a unilateral representation without any consideration and not part of the contract for the sale of goods.68

The Dolmage court interpreted an insurer’s integration clause that expressly excluded external documents except for “riders and endorsements,” holding that because the insurer’s Privacy Pledge was distributed with other documents appended to the insurance contract, the pledge could have been an intended rider.69 One of the other documents distributed with the policy expressly noted that it was not part of the contract, and the Privacy Pledge could have done the same. Thus, if the various attachments had been clearly labeled regarding whether they formed part of the contract, this claim could have been avoided. The defense in Dolmage argued that the privacy policy was a mere representation and could not be binding without consideration except on a quasi-contract or estoppel theory, which would have required the plaintiff to plead reliance. The court distinguished cases requiring reliance, because in this case the Privacy Pledge was incorporated into the contract, so the insurance premiums could be consideration.70 Even though the pledge was distributed after the contract was formed, it became part of the contract when the plaintiffs accepted it by continuing to perform and not cancelling their policies,71 and because the pledge went beyond the bare requirements of applicable law, it was not unenforceable on the ground that it merely required the defendant to perform its existing legal duties.72

B. BUSINESS ASSOCIATE AGREEMENTS

The Anthem II court also held as a matter of first impression that California public employees, for whom Anthem Blue Cross of California had acted as plan administrator, could claim as third-party beneficiaries of the HIPAA business associate agreement (“BAA”) between it and the California Public Employees Retirement System “(CalPERS”). The defense argued that the BAA was like the annual Notice of Privacy Practices, only a pro forma statement of legal obligations that created no contractual rights; however, the court responded that a BAA may cover more than the statute requires. Because the BAA was attached to the Administrative Services Only (“ASO”) agreement for California public employees, the ASO agreement could be read to incorporate the various privacy policies, and the class could proceed on the theory that they were third-party beneficia-

67. *Anthem II*, supra note 37, at *12.
70. Id. at *6–7.
71. Id. at *7–8.
72. Id. at *9.
ries. A third-party beneficiary must “take th[e] contract as he finds it,”73 but the public employees met this requirement because the defense admitted that CalPERS itself could have recovered damages if BCBS had breached the BAA.74 Other named plaintiffs, however, whose representatives apparently did not negotiate the wording as well as CalPERS had their California breach of third-party beneficiary ASO-based claims dismissed.75

V. CLAIMS REQUIRING INTENTIONAL DISCLOSURE

Statutes that prohibit, and torts based upon, intentional disclosure of information (as opposed to negligent retention) do not fit well in data security breach cases. The Anthem II court construed, as a matter of first impression, the Georgia Insurance Information and Privacy Protection Act.76 Because the statute on its face did not prohibit merely negligent retention, the court dismissed with prejudice the plaintiffs’ claim under the Act.77 In Enslin v. Coca-Cola Co., a claim under the federal Driver’s Privacy Protection Act failed for the same reason: an intentional act of disclosure was required.78 The Smith v. Triad court dismissed a claim for common-law invasion of privacy by public disclosure of private facts for a similar reason: the plaintiffs alleged that the defendants had intentionally failed to take proper precautions against disclosure, but they could not claim that defendants themselves had disseminated the information.79 The California Confidentiality of Medical Information Act (“CMIA”) is an exception in requiring employers to avoid both deliberate and negligent disclosure of employees’ medical information.80 Declining to dismiss a CMIA claim, the Corona court collected decisions interpreting this statute to cover losses to third parties resulting from negligent security practices.81

---

73. Anthem II, supra note 37, at *20 (quoting Marina Tenants Ass’n v. Deauville Marina Dev. Co., 226 Cal. Rptr. 321, 327 (Ct. App. 1986)) (internal quotation marks and alterations omitted).
74. Id. at *18–20.
75. Id. at *20.
77. Anthem II, supra note 37, at *40–41.
80. C A L. C I V. C O D E § 56.06(c) (West 2015) (requiring covered businesses to “maintain the same standards of confidentiality required of a provider of health care”).
Hacking Away at Trust

By Roland L. Trope* and Lixian Loong Hantover**

I. INTRODUCTION

The year covered by this essay, June 2015–May 2016, saw the continuation of two trends in cybersecurity incidents: first, increasingly sophisticated cyber intrusions that exploit vulnerabilities in critical infrastructure, and second, increasing awareness that the success of such attacks threatens to erode the trust that operators and users place in computer-based systems such as software-intensive emission controls, connected cars, and computer networks for interbank communications and fund transfers.

If users come to mistrust a digitally based system, they may limit their use of or abandon that system. For example, when hackers exploited a vulnerability and accessed customer card data in the massive Target data breach of 2013, they stole 40 million credit and debit cards and 70 million records containing the names, physical and e-mail addresses, and phone numbers of Target shoppers between November 27 and December 15, 2013. Target’s profits in the fourth quarter of 2013 dropped 46 percent compared with the year before. In addition, sales in the quarter ending February 1, 2014, dropped 3.8 percent and transactions fell 5.5 percent from the previous year. It may be that the correlation between the breach and the abrupt decline in sales and profits does not evidence causation, but it is reasonable to infer that a nontrivial number of loyal customers abandoned Target for competitors and that their desire to avoid a recurrence at Target may have been a significant motivation. However, the tipping point when customers abruptly relinquish their steadfast loyalty to a brand and

---

* Roland L. Trope is a partner in the New York City offices of Trope and Schramm LLP and an adjunct professor in the Department of Law at the U.S. Military Academy at West Point. He can be contacted at rltrope@tropelaw.com.

** Lixian Loong Hantover is Associate Counsel at IDEO. She can be contacted at lhantover@ideo.com.

The views expressed by the authors are solely their own and should not be attributed to their respective law firms or to the U.S. Military Academy, the U.S. Department of Defense, or the U.S. government. The authors thank Professors Sarah Jane Hughes and John A. Rothchild for their insights and thoughtful edits to this survey.


flee in doves to competitors should not be assumed to be a mirage or a vanishing point that recedes as fast as we approach it—legendary brand names swiftly go from market leaders to laggards—as happened with Kodak and Blackberry—and will continue to happen when customers doubt a brand can be trusted to perform as needed. An accretion of disaffection is bound to transform brand loyalty into brand disaffiliation. As Matthew Rosenquist observed, “Everyone has a threshold where purchasing decisions and brand loyalty will falter.”

Several developments highlighted the unraveling of trust in software-based technologies during the survey period. In February 2016, hackers used SWIFT credentials of Bangladesh Central Bank employees to transmit dozens of fraudulent money transfer requests to the Federal Reserve Bank of New York, causing the bank to transfer $81 million of the Bangladesh bank’s funds to accounts in the Philippines. As explained in a CERT-UK advisory, the custom-made malware used for this “cyber heist” took advantage of insufficient safeguards by the Bangladesh Central Bank. The CERT-UK advisory noted that there were reports that the bank used cheap Internet routers and had no firewalls, which likely explained why the attackers were able to gain access to the bank’s network. CERT-UK did not find that the SWIFT system itself had been compromised or was the root cause of the network breach. The malware had no impact on SWIFT’s wider network or core messaging services. However, CERT-UK noted, “An institution’s internal systems are only as secure as the network itself. If an attacker breaks into a network, as was the case here, then it is probable a malicious

3. The Economist notes that the potential for an unraveling of trust and a subsequent customer exit after a successful cyberattack is of increasing concern. See Joker in the Pack, THE ECONOMIST, July 16, 2016, at 8, 8 (“The financial system is little more than a set of promises between people and institutions. If these are no longer believed the whole house of cards will collapse and people will take their money and run. That happened in 2008 because of bad credit decisions; but the same could unfold via a sophisticated cyber-attack.”).


5. The acronym SWIFT stands for the Society for Worldwide Interbank Financial Telecommunication. SWIFT is a global member-owned cooperative that provides its community with a platform for cross-border bank payment messaging, standards for communicating, and services that “connect more than 11,000 banking and securities organisations, market infrastructures and cooperated customers.” SWIFT does not hold funds. Instead, its members use SWIFT “to communicate securely, exchanging standardised financial messages in a reliable way, thereby facilitating global and local financial flows.” Introduction to SWIFT, SWIFT, https://www.swift.com/about-us/discover-swift (last visited Sept. 19, 2016).


7. The acronym CERT-UK stands for the United Kingdom National Computer Emergency Response Team. CERT-UK has four responsibilities: (1) management of national cybersecurity incidents; (2) assisting critical national infrastructure companies to respond to, and recover from, cybersecurity incidents; (3) enhancing cybersecurity situational awareness; and (4) serving as the “single international point of contact for co-ordination and collaboration between national CERTs.” About Us, CERT-UK, https://www.cert.gov.uk/what-we-do/ (last visited Sept. 19, 2016).


9. Id.
actor could manipulate legitimate internal processes, such as those run by SWIFT software, for monetary gain.”

Thus, even though the SWIFT system was not itself compromised, this attack on one component of the SWIFT network showed the potential vulnerability of the SWIFT system and could begin to unravel the trust companies have in it: “Banks rely on [SWIFT] to guarantee the authenticity of orders to make payments from customers’ accounts. Hacking incidents at banks in Bangladesh, Vietnam and Ecuador have called that guarantee into question.”

Granted, with no immediate alternative to SWIFT, the banks have not yet “exited” after the attack on the Bangladesh Central Bank, but SWIFT reportedly is considering “suspending banks with weak security controls.”

A second unraveling of trust emerged in a virtual currency exchange as a result of an attempted theft by a hacker. In June 2016, an unknown hacker “raided an experimental online venture-capital fund called DAO” that utilizes the virtual currency platform Ethereum and stole $60 million of virtual currency “tokens.”

Ethereum developers crafted a “hard fork” (a change in protocol that invalidates previously valid transactions), which would enable recovery of the stolen “tokens” by erasing the hacker’s transactions. However, the recovery was put on hold as many investors in DAO questioned the wisdom of the stratagem, a perplexing instance in which trust mattered more than recovering stolen funds: “The reason: Undoing the theft requires altering the computer code underlying the digital currency and its platform, and some adherents think that would be a bigger sin than losing millions.”

On July 20, 2016, Ethereum implemented the hard fork, but doing so gave “miners, developers, and users” the option of adopting it (erasing the theft and restoring the tokens) or ignoring it (perpetuating the theft). Two versions of the currency thus came into existence: the older (now coined “Ethereum Classic”) and the new post-fork version.

Perhaps the year’s most severe depletion of trust emerged in Volkswagen’s “Dieselgate” debacle. In this incident, no outside hacker designed and exploited an attack on VW’s vehicles. Instead, at the apparent direction of their supervisors throughout the corporate chain of command, VW personnel designed and installed “defeat device” software in 11 million diesel passenger cars. The “device” detected when a car was operated according to lab test protocols and adjusted the car’s emission control system to meet NOX emission standards. The “device” also detected when cars were operated on the highway and shut down the car’s emissions control system, causing the car to exceed by a factor of fifteen to thirty-

10. Id.
15. Vigna, supra note 13, at C1.
five the legal limit for NO\textsubscript{X} emissions. When regulators questioned VW about the discrepancies between test lab and highway emissions, VW repeatedly issued disingenuous denials to cover up its design and installation of defeat device software.\textsuperscript{17}

With the advent of connected cars and autonomous vehicles, VW’s actions represent a corruption of software engineering and a significant threat to consumer trust in the VW brand—and potentially in all car engines since almost all such engines are now controlled by millions of lines of software code. VW, whose motto is “truth in engineering,” subverted the quality control of the design of its computer-operated onboard systems. When an automobile maker deliberately creates “corrupt code”\textsuperscript{18} for an onboard system, it must either conceal that activity from its quality control engineers or make them complicit in it. Either way, the likelihood is that the software engineers will focus on implementing the “corrupt code” and making sure the cheat works. As a result, engineers will give far less, if any, attention to protecting the vehicle and its onboard control systems against cybersecurity threats. By such practices, a manufacturer may create and fail to detect and remove vulnerabilities that hackers can exploit to gain control of a car’s safety-critical systems. In a March 2016 report, the U.S. Government Accountability Office explained the growing risks of such attacks and the large-scale harm they could inflict:

[Modern vehicles contain multiple interfaces—connections between the vehicle and external networks—that if not properly secured, can become entry points—or attack paths—for cyber attackers. Some . . . interfaces can only be accessed through direct contact with the vehicle, while others can be accessed remotely through short- and long-range wireless channels. . . . [R]eal-world attacks with safety implications could occur in the near future, particularly as automakers begin deploying autonomous (i.e., self-driving) vehicles and connected-vehicle technologies.\textsuperscript{19}]

Such concerns prompted the U.S. National Highway Traffic Safety Administration (“NHTSA”) to issue, on April 1, 2016, an Enforcement Guidance Bulletin cautioning automobile makers that the NHTSA would review any onboard system software that manifested vulnerabilities that could be exploited by hackers to gain control of a vehicle’s safety-critical systems, and if the software presented an unreasonable risk to safety, this would constitute a defect “compelling a recall.” As the NHTSA explained, a recall would be issued even if a cyber incident had yet to occur:


\textsuperscript{18} See id. at 21 (“Writing software code to create a cheat disguised as a solution represents the advent of a new insider cyber-threat. . . . What makes it unique—and a serious threat—is that it’s written to satisfy an engineering objective. . . . It helps bring substandard products to market. It confers a tremendous competitive advantage as long as the company can keep it hidden. . . . We call this corrupt code. . . . The only real counter to corrupt code is engineers with the mettle to challenge its use.”).

Even before evidence of an attack, it is foreseeable that hackers will try to exploit cybersecurity vulnerabilities. If a cybersecurity vulnerability in any of a motor vehicle's entry points allows remote access to a motor vehicle's critical safety systems (such as braking, steering, or acceleration), NHTSA may consider such a vulnerability to be a safety-related defect compelling a recall.

This survey focuses on three cybersecurity developments, each of which should prompt companies and their counsel to review and recalibrate what steps they should take to make sure that customers and investors trust that the companies are taking reasonable steps to prevent cyber attacks. These developments will also provide guidance to companies on how they might test whether a counterparty’s technology or cybersecurity is indeed trustworthy. In Part II, we examine the Seventh Circuit’s decision in Remijas v. Neiman Marcus Group, LLC and the lessons it holds for acquirers in M&A deals in which the target company may be the victim of a cyberattack that could create significant post-breach and post-closing liability. In Part III, we review the 2016 California Data Breach Report, its key recommendations, and the enforcement action against Dwolla, Inc., for falsely representing its data security practices. In Part IV, we analyze the newly enacted Defend Trade Secrets Act and discuss the subtle ways in which its provisions implicate cybersecurity and may prompt companies to modify their confidentiality agreements.

II. Remijas v. Neiman Marcus Group, LLC

On December 17, 2013, luxury department store Neiman Marcus received the first of several reports indicating fraudulent use of customer credit cards at its stores. Neiman Marcus hired a forensic investigative firm, which informed Neiman Marcus in early January 2014 that it had discovered malware in the retailer’s customer payment processing system. On January 10, 2014, Neiman Marcus publicly disclosed that between July 16, 2013, and October 30, 2013, about 350,000 customer cards “had been exposed to the hackers’ malware.” The company reported the breach to all customers who had made purchases at its stores during 2013 (and whose physical or e-mail addresses it had) and offered them a free year of credit monitoring and identity-theft protection.

Affected customers filed class action complaints, which were consolidated in the Northern District of Illinois. Plaintiffs alleged that Neiman Marcus had failed to protect them adequately against the data breach and to provide them with timely notice of it. Neiman Marcus moved to dismiss for lack of Article III

22. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 690 (7th Cir. 2015).
standing. The district court granted the motion, reasoning that although to establish standing it would be sufficient for plaintiffs to prove “future potential harm,” the harm had to be “certainly impending.” The district court, while accepting the undisputed allegation that 9,200 customers had suffered fraudulent use of their cards, nevertheless held that this did not show they were “at a certainly impending risk of identity theft.”

The district court’s conclusion seems bizarre and counterintuitive when compared to the Federal Trade Commission’s guidance to consumers on identity theft, which warns that if notified that one’s debit or credit card number has been lost or exposed by a cyber-executed data breach, one’s first response should be to immediately “[c]ontact your bank or credit card company to cancel your card and request a new one.” If 350,000 customers of one merchant have had their card numbers exposed to hackers in a concerted, sophisticated attack, the implausible inference would be that such customers are not at impending risk of identity theft.

The post-breach risk to these consumers was not lost on the U.S. Court of Appeals for the Seventh Circuit, to which the plaintiffs appealed. The circuit court concluded that the district court had erred and held that the plaintiffs had met Article III requirements for standing. The court reasoned that it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.

The Seventh Circuit supported its conclusion with findings contained in a Government Accountability Office report that observed that “stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.” The court thus held that the plaintiffs had adequately alleged standing under Article III, reversing and remanding the case.

However, the circuit court added, in dicta, something that may prove disconcerting to future data-breach vendor defendants. The court noted that Neiman Marcus had offered, at no cost, one year of credit monitoring and identity-theft protection to all potentially affected customers, and observed: “It is unlikely that it [Neiman Marcus] did so because the risk is so ephemeral that it can safely be disregarded.” Such reasoning puts vendors that suffer a data breach in a

credit card charges, and an increased risk of identity theft as well as present injuries such as time and expenses to clear up fraudulent charges and to protect themselves against future identity theft. Id. at *2–3.

24. Id. at *9.
26. Remijas, 794 F.3d at 693.
27. Id. at 694 (quoting U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-07-737: REPORT TO CONGRESSIONAL REQUESTERS—PERSONAL INFORMATION 29 (2007)).
28. Id. at 697.
29. Id. at 694.
double bind. If, on learning of a data breach, a vendor fails to offer its customers such protections, customers may later argue that the vendor acted negligently (or with reckless indifference) by not helping them mitigate the risks of harm from the data breach. However, a vendor that seeks to act responsibly and offers such protections will put itself at risk of giving plaintiffs (and courts) a basis for arguing that future harm was a concrete and particularized injury that establishes Article III standing.

The broader context of the Neiman Marcus case contains an important feature that neither the district court nor the circuit court noted. The data breach began as early as July 16, 2013, several weeks before the owners of the Neiman Marcus Group agreed, on September 8, 2013, to be acquired by a group led by Ares Management and a Canadian pension plan. The card-scraping activity of the malware ceased on October 30, 2013, five days after the acquisition of the Neiman Marcus Group closed, six weeks before Neiman Marcus began receiving Common Point of Purchase reports from MasterCard (reports of accounts for which the issuing bank and the cardholder know of fraudulent use of the card), and two months before Neiman Marcus’s forensic investigators reported the existence of malware in its system.

Thus, the acquirers of the Neiman Marcus Group probably had no awareness that as their due diligence, negotiation, and closing of the deal proceeded, so did a severe, sophisticated cyberattack on their deal’s target. These events show that prospective buyers and their counsel in M&A deals need to include cybersecurity in their due diligence reviews and to give serious consideration to the possibility of undetected, ongoing cyberattacks on the target when negotiating representations, warranties, and indemnifications that might otherwise fail to protect a buyer from substantial post-breach costs and liability.

III. 2016 CALIFORNIA DATA BREACH REPORT; ENFORCEMENT ACTION AGAINST DWOLLA

As discussed in Part I, a data breach can lead to an erosion of trust. It is thus reasonable to assume that an enforcement action by a federal or state agency against a company for inadequate security measures could similarly erode consumer trust (not to mention if that inadequate security then leads to a serious data breach). So how do companies ensure their security practices are sufficient in the eyes of government agencies? This part explores how the California Attorney General understands reasonable security measures and provides a cautionary tale regarding Dwolla, Inc., which misrepresented its security protocols and
failed to implement reasonable security measures such as those recommended by California.\(^{35}\)

A. Since 2012, businesses and agencies have been required to notify the California Attorney General of breaches affecting more than 500 Californians. The data collected and presented in the 2016 California Data Breach Report, released in February 2016, is sobering. In the past four years the Attorney General has received reports on 657 data breaches affecting over 49 million records belonging to Californians. Nearly three in five Californians were victims of a data breach in 2015 alone.\(^{36}\)

California Attorney General Kamala Harris concedes that the sophistication of cyber criminals (including nation states) makes data security a challenge, but she notes that many of the breaches reported could have been prevented had organizations taken “reasonable security measures.”\(^{37}\) But what are these reasonable security measures? For organizations looking to stay in compliance with California’s statutes, which are more rigorous than those currently under consideration at the federal level,\(^{38}\) the report offers insights into what constitutes reasonable security.

The report sets out five broad data security recommendations. The first recommendation suggests that organizations adopt the twenty controls highlighted by the Center for Internet Security’s Critical Security Controls.\(^{39}\) These controls include limiting user and administrator privileges, training employees and vendors with access to internal systems, and monitoring accounts and network logs.\(^{40}\) For organizations looking to understand what constitutes reasonable security, it is worth noting that the report states that the failure to implement all those controls that apply to an organization’s environment constitutes a lack of reasonable security.\(^{41}\)

The second recommendation is for organizations to move beyond simple username and password authentication and to implement multifactor authentication (which might include factors such as biometrics or one-time passwords) to protect critical systems and sensitive personal information.\(^{42}\) The third and fourth recommendations are to implement strong encryption and encourage those affected by a data breach to place a fraud alert on their credit files.\(^{43}\) The final recommendation encourages state policymakers to collaborate in seeking to harmonize state breach laws.\(^{44}\)

While the report is merely a series of recommendations, they nonetheless constitute a useful guide for organizations (especially those doing business in Califor-


\(^{36}\) Kamala D. Harris, California Data Breach Report iii (2016).

\(^{37}\) Id. at ii.

\(^{38}\) Id. at v.

\(^{39}\) Id. at 30.

\(^{40}\) Id. at 32.

\(^{41}\) Id. at 30.

\(^{42}\) Id. at 34–35.

\(^{43}\) Id. at 36–37.

\(^{44}\) Id. at 38.
nia) that are looking to establish adequate data security procedures and practices to avoid government actions and build trust among investors and customers.

B. Recent cases have shown that failure to implement recommendations such as those in the California Data Breach Report can lead to severe consequences, including government actions. For example, on March 2, 2016, the Consumer Financial Protection Bureau (“CFPB”) issued a consent order finding that Dwolla, Inc. had engaged in deceptive acts and practices relating to false representations about its data security practices.\(^{45}\) Dwolla had represented to consumers that its network and transactions were “safe” and “secure.”\(^{46}\) On its website and in direct communications, Dwolla said that its data security practices “exceeded industry standards”\(^{47}\) and assured customers that their data was being encrypted and stored securely.\(^{48}\) But the CFPB found that this was not true.\(^{49}\) In particular, the CFPB noted that Dwolla failed to:

- adopt and implement data-security policies and procedures reasonable and appropriate for the organization;
- use appropriate measures to identify reasonably foreseeable security risks;
- ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks;
- use encryption technologies to properly safeguard sensitive consumer information; and
- practice secure software development, particularly with regard to consumer-facing applications developed at an affiliated website, Dwollalabs.\(^{50}\)

In fact, Dwolla did not hold its first comprehensive risk assessment nor its first mandatory employee training on data security until mid-2014, four years after the company launched services in California.\(^{51}\) The CFPB ordered Dwolla to adopt and implement appropriate data security measures, pay civil penalties, maintain compliance records for at least five years, and provide those records to the CFPB upon request.\(^{52}\) Rather than spending its time misrepresenting its security practices, had Dwolla used that time to implement reasonable security measures similar to those outlined in the California Data Breach Report, these fines and onerous record requirements could have been avoided—not to mention the breach of trust that likely occurred between Dwolla and its customers.

\(^{46}\) Id. at para. 16.
\(^{47}\) Id. at para. 19.
\(^{48}\) Id. at para. 20.
\(^{49}\) Id. at paras. 23–26.
\(^{50}\) Id. at para. 27.
\(^{51}\) Id. at paras. 31, 33.
\(^{52}\) Id. at paras. 52–79.
IV. DEFEND TRADE SECRETS ACT OF 2016

On May 11, 2016, President Obama signed into law the Defend Trade Secrets Act of 2016 (“DTSA”). The DTSA amends the Economic Espionage Act of 1996 (“EEA”) to allow the owner of a trade secret that has been misappropriated to bring a civil action in U.S. District Court “if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.” Overlooked by early commentaries on the DTSA are the cybersecurity features implicit in its text, which deserve close attention by clients and counsel.

The DTSA’s use of the term “trade secret” relies on the EEA’s definition of the term, which establishes, as one condition to qualify as a trade secret, that “the owner thereof has taken reasonable measures to keep such information secret.” With the pervasive spread of cyberattacks, an enterprise that fails to take “reasonable measures” to safeguard its proprietary information from cyber intrusions may be unable to qualify such information as a trade secret. In short, companies that wish to improve protection of their trade secrets by lawsuits brought under the DTSA will need to shore up the cybersecurity protections of their proprietary information if they want it treated by courts, under the DTSA, as protectable trade secrets. The need for enhanced cybersecurity to preserve the trade secret status of certain information finds additional support in the fact that the EEA expressly defines a trade secret to include information “whether tangible or intangible, and whether or how stored . . . or memorialized physically, electronically . . . or in writing.”

The DTSA authorizes the awarding of exemplary damages for willful and malicious misappropriations of trade secrets. However, the DTSA creates two categories of defendant: (1) an “employee” of the trade secret owner and (2) all other persons. For a trade secret owner to recover exemplary damages against an employee defendant, the owner-employer must have provided the employee with notice of his or her DTSA whistleblower immunity “in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.”

55. Id. § 1836(b)(1).
58. Id. § 1839(3).
59. Id. § 1833(b)(3)(A), (C). The whistleblower notice can also be via a “cross-reference to a policy document provided to the employee that sets forth the employer’s reporting policy for a suspected violation of law.” Id. § 1833(b)(3)(B). This whistleblower immunity protects an individual from liability “under any Federal or State trade secret law for the disclosure of a trade secret,” if such discl-
The cybersecurity feature in the DTSA’s award of exemplary damages is hidden in the DTSA’s unusually broad definition of “employee,” which expressly “includes any individual performing work as a contractor or consultant for an employer.” As a result, entities such as the following appear to qualify as “employees” under the DTSA if they are under a contract with the trade secret owner:

- software development companies
- cybersecurity, privacy, and other “consultant” companies
- any supplier of goods or services.

To qualify for exemplary damages against such entities, the trade secret owner needs to include the DTSA whistleblower notice in the contract with that “employee.”

Trade secret owners will want to maximize the benefits offered by the DTSA. To do so, they will need to take an additional precaution when they want to disclose their trade secrets to an outside “employee” (a contractor or supplier) and make sure that they have conditioned such disclosures on the intended recipient’s execution of a nondisclosure agreement (“NDA”). The trade secret owner will need to update its standard NDA to address the risk that hackers might misappropriate the trade secret from the “employee.” If that happened, the hackers might seek to profit by selling the trade secrets into secondary or tertiary markets. The trade secret owner, unless notified of the breach, would be unaware that the competitive advantage and value of the trade secrets were at risk of being rapidly depleted. To address these risks, the trade secret owner should include a data breach notification provision. The provision should require that, in the event that the recipient discovers that it has been the target of a cyberattack or intrusion that might have given the hackers access to the entrusted trade secret, the recipient shall immediately notify the trade secret owner. Alerted by such notice, the trade secret owner can mitigate the following risks:

- Early start date of the DTSA’s three-year statute of limitations. The DTSA’s three-year statute of limitations starts on the date “on which the misappropriation . . . is discovered or by the exercise of reasonable diligence should have been discovered.” If the trade secret owner does not require each recipient to report a data breach that might have exposed its trade secret to hackers, a court might find that the DTSA’s statute of limitations started to run from the date when the recipient could have been required, under an NDA, to report the data breach to the trade secret owner.

sure is made “in confidence to a Federal, State, or local government official . . . or to an attorney” and “solely for the purpose of reporting or investigating a suspected violation of law.” Id. § 1833(b)(1)(A).
60. Id. § 1833(b)(4).
61. Id. § 1836(d).
62. Id.
• *Dissemination of trade secrets.* The DTSA permits the owner of a trade secret that has been “misappropriated” to bring a civil action and, upon *ex parte* application “but only in extraordinary circumstances,” to obtain an order from a district court for the “seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.”63 To establish “extraordinary circumstances” the plaintiff must show, among other things, that the “person against whom seizure would be ordered . . . would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person.”64 These provisions favor a trade secret owner who learns quickly of a misappropriation. If the trade secret is stolen by hackers from an outside “employee” who signed an NDA containing a data breach reporting provision, then there is a chance the trade secret owner might learn of the theft in time to seek a seizure order to prevent dissemination and devaluation of the trade secret. That will not happen unless the outside “employee” implements safeguards that detect a cyber breach quickly and promptly notifies the trade secret owner of the breach.

Thus, knowing the subtle ways in which cybersecurity figures into the DTSA is crucial for corporate clients and their counsel. Otherwise they may fail to take the actions necessary to qualify for the DTSA’s protections and remedies.

**V. Conclusion**

Each breach of a digital or cyber technology challenges users to mistrust and abandon the technology. User loyalty has, to date, proved remarkably enduring. But when it breaks, customers exit rapidly and in droves, as seen with Target and VW. A company’s cybersecurity safeguards protect not only its trade secrets and other intellectual property but also its reputation, brand, and goodwill. The developments in cybersecurity reviewed in this essay highlight the growing need for clients and counsel to consider that traditional stratagems of “damage control” fail in the wake of severe cyber breaches and, in the case of VW, put at risk an entire industry and its plans to deploy cyber-connected car technologies. If hackers and manufacturers start to resemble one another, customers may become so mistrustful of software-controlled engines, virtual currencies, and electronic payment devices that they refuse to adopt new, and start to discard established, cyber technologies. Users are not there yet but may not be far from it.

63. *Id.* § 1836(b)(1), (2)(A)(i).
64. *Id.* § 1836(b)(2)(A)(ii)(VII).
Privacy Developments: Private Litigation, Enforcement Actions, Legislation, and Administrative Actions

By John Black* and James Steel**

I. INTRODUCTION

In recent years, two principal areas of privacy-related legal exposure for businesses maintaining consumer personal information have been private litigation under the Telephone Consumer Protection Act (“TCPA”)¹ and enforcement actions by the Federal Trade Commission (“FTC”). However, in the last year, other federal and state regulators have become more active in policing and enforcing privacy, and plaintiffs have enjoyed success in expanding the use of existing federal and state statutes to pursue privacy litigation. This survey reviews the key developments in these areas in the past year, including the highly publicized legal battle between the U.S. Department of Justice and Apple, Inc. over access to the encrypted iPhone used by one of the terrorists in the San Bernardino attacks.

II. PRIVATE ACTIONS UNDER THE TCPA

TCPA litigation continued apace in 2015, with 3,710 filed actions in state and federal court—a 45 percent increase over the number of filings in 2014.² Plaintiffs’ firms continue to find the prospect of $500 to $1,500 in statutory damages an effective source of settlements and fee awards, while many companies, unwilling to forgo the potentially lucrative telemarketing opportunities, have continued to wrangle with an uncertain regulatory compliance landscape.

---

¹ 47 U.S.C.A. § 227 (West 2014 & Supp. 2016); see id. § 227(b)(3) (providing for a private cause of action to recover actual monetary damages or $500 for each violation, whichever is greater, and empowering the court to increase the award, by no more than three times, if the defendant willfully or knowingly violated the statute or applicable regulations); id. § 227(c)(5) (same).

In May 2016, the U.S. Supreme Court handed down one of the most anticipated decisions concerning a plaintiff’s ability to maintain a civil action under the TCPA. Unfortunately, rather than adding clarity to an area already fraught with uncertainty, the Court’s decision appears destined to spawn further legal battles.

The Supreme Court’s decision in *Spokeo, Inc. v. Robins* clarified the requirements for Article III standing. Spokeo is a regulated “consumer reporting agency” under the Fair Credit Reporting Act (“FCRA”), operating a website that enables a user to input an individual’s name, e-mail address, or phone number to conduct a broad search in a variety of databases to obtain information concerning the individual. In *Spokeo*, the plaintiff alleged an unspecified individual had conducted a Spokeo search for information about him, and that the information Spokeo provided in response contained certain inaccuracies. Upon learning of the inaccurate information, he filed a class-action complaint, alleging Spokeo willfully violated the FCRA.

Although the district court dismissed the lawsuit for lack of standing, the U.S. Court of Appeals for the Ninth Circuit reversed. The Supreme Court, in an opinion authored by Justice Alito, explained that, under existing case law, the “irreducible constitutional minimum” of standing requires three elements: (1) an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.

Focusing on the injury-in-fact requirement, the Court noted the plaintiff bore the burden of establishing an injury that is both “concrete and particularized.” While the plaintiff had established the injury caused by Spokeo’s delivery of inaccurate information was “particularized,” as it affected the plaintiff in a personal way, the Ninth Circuit’s analysis had failed to consider properly whether the injury was “concrete.” As Justice Alito noted, it is not enough that an injury be unique to an individual; the injury must also be “real” and not “abstract.” Thus, the Court drew a strong distinction between concreteness and particularization.

In considering whether an injury is concrete, the Court noted that it was not necessary to determine whether an injury resulted in tangible harm because intangible injuries may also be concrete. While the Court was deferential to a congressional determination to “elevate” an intangible harm to the status of a legally cognizable injury, the Court made it clear that Congress could not grant Article III standing to plaintiffs by fiat. Regardless of the congressional deter-

---

4. Id. at 1546 (citing 15 U.S.C. § 1681a(f)).
5. Id.
6. Id. at 1547.
7. Id. at 1548 (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).
8. Id.
9. Id. (quoting Webster’s Third New International Dictionary 472 (1971); Random House Dictionary of the English Language 305 (1967)).
10. Id. at 1549.
11. Id. (quoting Lujan, 504 U.S. at 578).
mination, Article III standing requires the existence of a concrete injury, even in the context of a statutory violation.\textsuperscript{12} The statutory context of the FCRA informed the Court that Congress “sought to curb the dissemination of false information.”\textsuperscript{13} However, an allegation of a mere violation of the FCRA’s procedural requirements would not necessarily result in concrete harm. It was the plaintiff’s obligation to allege the basis for concluding a concrete harm was suffered, and the Ninth Circuit’s duty to evaluate the sufficiency of that allegation. Because the Ninth Circuit had failed to evaluate the injury for concreteness, its decision was reversed, and the Supreme Court remanded the case for further proceedings.

\textit{Spokeo} has obvious implications for pleading sufficiency under the TCPA. According to the Court’s logic, it is not enough to allege a technical violation of the TCPA—regardless of the congressional judgment as to the nature of the harm. Rather, to satisfy Article III’s standing requirements, a plaintiff must also establish that the TCPA violation resulted in concrete harm to the plaintiff. In sum, the standing requirement of injury in fact is not obviated by a congressional determination as to the availability of statutory damages.

Not surprisingly, the battle lines on this issue have already begun to emerge. Ten days after the Supreme Court issued its \textit{Spokeo} decision, Facebook filed a motion to dismiss a TCPA class action based, in part, on the Supreme Court’s standing analysis in \textit{Spokeo}.\textsuperscript{14} In its motion, Facebook argued the plaintiff alleged only a statutory violation, consisting of text messages sent in violation of the TCPA, and failed to allege a concrete injury arising from his receipt of those messages.\textsuperscript{15} While Facebook admitted the plaintiff had alleged that he “incurs charges for incoming messages,” Facebook argued he failed to assert that he pays for each individual message or was otherwise charged more than he would have been.\textsuperscript{16} According to Facebook, the allegations were therefore insufficient under \textit{Spokeo}.

At least one court has already rejected the \textit{Spokeo} standing argument in a TCPA lawsuit. In \textit{Booth v. Appstack, Inc.},\textsuperscript{17} the court was satisfied that the plaintiffs had demonstrated a “concrete injury” in their TCPA claims. According to the \textit{Booth} court, the plaintiffs alleged that the TCPA violations forced them to waste time answering or otherwise addressing widespread robocalls. The court noted that “[t]he use of the autodialer, which allegedly enabled Defendants to make massive amounts of calls at low cost and in a short period of time, amplifies the severity of this injury.”\textsuperscript{18} The court, therefore, was satisfied that the alleged injury was sufficient to confer Article III standing.\textsuperscript{19}

\begin{itemize}
  \item \textsuperscript{12} Id.
  \item \textsuperscript{13} Id. at 1550.
  \item \textsuperscript{14} Facebook, Inc.’s Notice of Motion and Motion to Dismiss Plaintiff’s First Amended Complaint and Memorandum in Support at 8–9, Duguid v. Facebook, Inc., No. 3:15-cv-00985-JST (N.D. Cal. May 26, 2016).
  \item \textsuperscript{15} Id. at 9.
  \item \textsuperscript{16} Id. (quoting First Amended Complaint).
  \item \textsuperscript{17} No. C13-1533JLR, 2016 WL 3030256, at *5 (W.D. Wash. May 25, 2016).
  \item \textsuperscript{18} Id.
  \item \textsuperscript{19} Id.
\end{itemize}
The distinction between phone calls and text messages may be crucial. In an age of unlimited messaging plans, as Facebook argues, there may be little, if any, cognizable, concrete harm to a consumer who merely endures the occasional nuisance of a text message. Perhaps a sharp distinction will be drawn between the nuisance caused by a text message and an automated robocall, which may be an active area of inquiry for courts faced with TCPA lawsuits, as defendants seek to test the scope of permissible standing following *Spokeo*.

Many commentators expected the Court to draw a bright line limiting Article III standing. Following issuance of the opinion, some in the business community appealed to Congress for relief. With remarkable timing, the Senate Commerce Committee held a hearing on the efficacy of the TCPA two days after the Court’s decision in *Spokeo*.20 At the hearing, Senate Republicans pushed to ease TCPA restrictions and met sharp resistance from Democrats. Whether the hearing will result in action to amend the TCPA is an issue to watch in coming months.

III. FTC PRIVACY ENFORCEMENT ACTIONS

The FTC has historically been one of the federal agencies most active in protecting consumer privacy. Under section 5 of the FTC Act, which declares unlawful “unfair or deceptive acts or practices in or affecting commerce,”21 the FTC has often brought enforcement actions to address unfairness and deception in collecting, handling, and disposing of consumer personal information. As new technologies and issues have arisen, the FTC has also shifted the focus of its efforts. For example, in its January 2015 report, *Internet of Things: Privacy & Security in a Connected World*,22 the FTC examined the applicability of Fair Information Practice Principles to smart devices underlying the Internet of Things (“IoT”), signaling its concern about the adequacy of consumer privacy protections associated with these devices. In the past year, the FTC brought two particularly notable privacy enforcement actions, which reflect the shifting focus of FTC enforcement efforts.

A. ASUSTeK COMPUTER, INC.

A year after releasing its *Internet of Things* report, the FTC brought an enforcement action against a Taiwan-based computer hardware maker for producing routers with critical security flaws that put at risk the home networks of consumers. According to the complaint in *In re ASUSTeK Computer, Inc.*,23 the routers’

---


insecure “cloud” services led to the compromise of thousands of consumers’ connected storage devices, exposing sensitive personal information on the Internet. In February 2014, hackers used readily available tools to locate vulnerable ASUS routers and exploited these security flaws to gain unauthorized access to over 12,900 storage devices.

According to the complaint, the interfaces to the routers had numerous vulnerabilities, including using unencrypted means to transfer files and permitting the bypassing of authentication mechanisms and the remote retrieval of log-in credentials stored in clear text. The complaint alleged ASUS failed timely to fix these vulnerabilities or notify affected users. In addition, ASUS did not notify consumers about the availability of security updates, and often incorrectly informed consumers that their routers employed the most current firmware available. ASUS also marketed its routers as including security features that would “protect computers from any unauthorized access, hacking, and virus attacks” and “protect [the] local network against attacks from hackers.” ASUS’s router also featured services that purportedly allowed a consumer to plug a USB drive into the router to create a secure “cloud” storage accessible from any device, although the services had serious security flaws.

The FTC and ASUS entered into a consent order requiring ASUS to establish a comprehensive security program, subject to independent audits for the next twenty years. In addition, the order requires ASUS to notify consumers of software updates and other steps they can take to protect themselves from security flaws, and prohibits ASUS from misleading consumers about the security of the company’s products, including whether a product is using current software.

B. VERY INCOGNITO TECHNOLOGIES, INC.

The FTC also settled its first enforcement case under the new Asia-Pacific Economic Cooperation (“APEC”) Cross-Border Privacy Rules (“CBPR”). The CBPR system, developed by participating APEC countries to build trust in cross-border transfers of personal information, requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework’s nine information privacy principles and receive certification of compliance from an APEC-recognized accountability agent. The FTC’s complaint in In re Very Incognito Technologies, Inc. alleged that Vipvape, a maker of handheld vaporizers, violated section 5(a) of the FTC Act by falsely representing in its website privacy policy that it was certified to participate in the APEC CBPR system.

The FTC and Vipvape entered into a consent order prohibiting Vipvape and its personnel from misrepresenting its participation in any privacy or security

24. Id. at 2 & exh. A (quoting ASUS marketing materials).
program.27 The order requires Vipvape to provide a copy of the consent order to its personnel and also to maintain compliance records for twenty years.

IV. PRIVACY ENFORCEMENT ACTIONS BY OTHER REGULATORY BODIES

Although regulators, such as the FTC and the Office for Civil Rights of the Department of Health and Human Services, have been active for several years in protecting personal information, other federal and state regulatory bodies have recently become more active in promoting privacy best practices and enforcing privacy laws and regulations. Below are some of the more notable enforcement actions in the last year.

A. CFPB v. EZCORP, Inc.

The Consumer Financial Protection Bureau (“CFPB”), under its authority to prevent unfair or deceptive practices in violation of the Consumer Financial Protection Act of 2010,28 has become active in privacy enforcement. In December 2015, the CFPB entered into a consent order with EZCORP, Inc., a Texas payday/installment loan company, over deceptive and unfair business practices, including illegally disclosing the existence of the debt to third parties during collection visits to debtors’ homes and places of employment. EZCorp also exposed consumers to fees through electronic withdrawal attempts, often making three attempts electronically to withdraw money from a consumer’s bank account for a loan payment and making withdrawals earlier than promised. As a result, consumers incurred bank fees, which made it harder for them to climb out of debt when behind on payments. Under the consent order, EZCORP must refund $7.5 million to 93,000 consumers who made payments after illegal in-person collection visits or who paid fees to EZCORP or their banks because of unauthorized or excessive electronic withdrawal attempts. EZCORP must also cease both collecting or selling remaining payday and installment debt and illegal debt collection practices and pay a $3 million civil penalty to the CFPB Civil Penalty Fund.29

B. In re Cellco Partnership

In December 2015, the Federal Communications Commission (“FCC”) entered into a consent decree with Cellco Partnership (“Verizon”) to resolve its investigation into whether Verizon failed to disclose to consumers that it was inserting Unique Identifier Headers “(UIDH)” (i.e., “supercookies”) into their Internet traffic in violation of section 222 of the Communications Act and the FCC’s Open Internet Transparency Rule on informed choice. The FCC found

that Verizon began inserting the UIDH into consumers’ Internet traffic in December 2012, but did not disclose this practice until October 2014, and did not update its privacy policy until March 2015 to include information about the UIDH. The FCC also found that at least one of Verizon’s advertising partners used the UIDH for unauthorized purposes to circumvent consumers’ privacy choices by restoring deleted cookies, and that Verizon inserted the UIDH into the Internet traffic from mobile device lines that were not eligible to participate in Verizon’s targeted advertising programs. The consent decree required payment of a $1,350,000 fine, disclosure, designation of a compliance officer to monitor compliance, and the implementation of a three-year compliance plan requiring Verizon to obtain customer opt-in consent prior to sharing the customer’s UIDH with a third party to deliver targeted advertising.\(^{30}\)

**C. New York Attorney General’s Settlement with Uber**

In January 2016, the New York Attorney General announced a settlement with Uber over the Attorney General’s investigation into Uber’s collection, maintenance, and disclosure of rider personal information. The investigation arose from reports that Uber executives had access to rider locations and displayed this information in an aerial view, referred to internally as “God View.” The settlement required Uber to adopt security practices to protect personal information, including encrypting rider geolocation information and adopting multifactor authentication before employees access sensitive personal information. The settlement also included a $20,000 penalty for failing to timely notify drivers and the Attorney General’s Office of a data breach in September 2014.\(^{31}\)

**IV. Notable Privacy Litigation**

**A. Biometric Privacy Litigation**

The Illinois Biometric Information Privacy Act (“BIPA”)\(^{32}\) was adopted in 2008, but recently has become the subject of class action litigation with at least six putative class action complaints having been filed since early 2015. Among its provisions, BIPA prohibits any private entity\(^{33}\) from collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person’s biometric information or a biometric identifier, defined as “a retina or iris

---


\(^{32}\) 740 ILL. COMP. STAT. ANN. 14/1 et seq. (West 2014).

\(^{33}\) “Private entity” is defined as an “individual, partnership, corporation, limited liability company, association, or other group,” but not a state or local government agency, court, judge, or court clerk. Id. § 10.
scan, fingerprint, voiceprint, or scan of hand or face geometry,” without first informing the person in writing that biometric information or a biometric identifier is being collected or stored and the specific purpose and length of time for which it is being collected, stored, and used, and obtaining a valid written release. Under BIPA, a prevailing plaintiff can recover actual damages or liquidated damages of $1,000 to $5,000 per violation, as well as attorney’s fees and costs, which may have spurred the interest of plaintiffs’ attorneys in pursuing lawsuits for alleged violations of the Act. Only Texas has a similar biometric information statute, although other states have considered similar legislation.

Putative class actions have been brought under BIPA against Shutterfly and Facebook, among others, for collecting the facial features of non-website users from photos uploaded by users without first obtaining appropriate consent. Several of these cases recently were the subject of court decisions concerning whether the cases should continue.

In *Norberg v. Shutterfly, Inc.* the U.S. District Court for the Northern District of Illinois denied a motion to dismiss a complaint against the photo-sharing website for collecting biometrics of non-users from photos in which they appear. Shutterfly argued BIPA does not regulate “biometric identifiers, [such as] hand or face geometry, derived from photographs,” because photographs are specifically excluded as a biometric identifier under BIPA, but the court rejected this argument. Noting that a “scan of hand or face geometry” is a biometric identifier under BIPA and that protected biometric information includes “information . . . based on an individual’s biometric identifier,” the court drew a distinction between a photograph and a facial pattern derived from a scanned photograph. Based on the plaintiff’s allegation that he did not use the defendant’s website, did not agree to its privacy policy, and did not upload his facial image (which was taken from a photo uploaded by a website user), the court denied the motion to dismiss.

In *In re Facebook Biometric Information Privacy Litigation* the U.S. District Court for the Northern District of California denied Facebook’s motion for summary judgment. Facebook argued that the plaintiffs had agreed to its terms of

---

34. *Id.* “Biometric information” means “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.”

35. *Id.* § 15(b).

36. *Id.* § 20.

37. TEX. BUS. & COM. CODE ANN. § 503.001 (West 2015).


40. 152 F. Supp. 3d 1103 (N.D. Ill. 2015).

41. *Id.* at 1105.

42. *Id.* at 1106 (quoting 740 ILL. COMP. STAT ANN. 14/10 (West 2014)).

43. *Id.*

use, including a clause designating California as the applicable law for disputes, which rendered inapplicable the Illinois statute. The court applied California choice-of-law rules, according to which the contractual designation of governing law would apply unless that law is contrary to a “fundamental policy” of another state and the latter state has “a materially greater interest” in the matter than the former state.\(^{45}\) The court held that those two conditions were met, and that BIPA was therefore applicable. The court also rejected Facebook’s argument that BIPA’s exclusion of photographs from “biometric information” should encompass all information drawn from photographs, such as facial geometry from scanned photos, noting that Facebook’s reading would undercut the statutory intent to address emerging biometric technology and that BIPA’s exclusion of photographs is better understood as meaning paper prints of photographs.\(^{46}\)

**B. Yershov v. Gannett Satellite Information Network, Inc.**

In Yershov v. Gannett Satellite Information Network, Inc.,\(^{47}\) the U.S. Court of Appeals for the First Circuit reversed a district court’s dismissal of a putative class action lawsuit against Gannett Satellite Information Network, Inc. (“Gannett”), which publishes USA Today, for allegedly disclosing information about the plaintiff to a third party in violation of the Video Privacy Protection Act of 1988.\(^{48}\) The district court determined that Gannett had disclosed “personally identifiable information,” but held that the plaintiff was not a “renter, purchaser, or subscriber” of Gannett video content and therefore was not protected under the Act.\(^{49}\) The plaintiff, Alexander Yershov, was a mobile phone user who had signed up to use Gannett’s USA Today app, by which he watched video clips. Gannett would send the video title, phone identifier, and geolocation data concerning Yershov to a third party analytics company whenever Yershov downloaded a video. However, Gannett failed to obtain Yershov’s consent to share his personally identifiable information. The First Circuit determined that Yershov was a “subscriber” under the Act, even if he was not a paying customer, because he provided consideration for the app’s service in the form of his phone ID and geolocation information.\(^{50}\)

**C. United States v. Apple, Inc.**

In a widely publicized case that raised intriguing issues concerning the conflict between physical security and privacy, the U.S. Attorney for the Central District of California obtained an order compelling Apple, Inc. to assist in decrypting an Apple iPhone used by a terrorist involved in the San Bernardino attacks on

\(^{45}\) Id. at *9 (quoting Wash. Mut. Bank, FA v. Super. Ct., 15 P.3d 1071, 1079 (Cal. 2001)).

\(^{46}\) Id. at *12.

\(^{47}\) 820 F.3d 482 (1st Cir. 2016).


\(^{49}\) Yershov, 820 F.3d at 485 (quoting 18 U.S.C.A. § 2710(a)(1), (3) (defining “consumer” to mean “any renter, purchaser, or subscriber . . . ” and also defining “personally identifiable information”)).

\(^{50}\) Id. at 487–89.
December 2, 2015. The phone had been seized pursuant to a warrant executed the day after the attacks. Apple had refused to voluntarily decrypt the phone, even though the government identified Apple as the only party with the technical means to do so. The owner of the phone, the terrorist’s employer, had consented to the search and to Apple providing decryption assistance. The government feared that attempting to crack the code would trigger the phone’s auto-erase function and requested that Apple write code that would operate only for that phone to disable the auto-erase function.51

The government proceeded under the All Writs Act, “a residual source of authority to issue writs that are not otherwise covered by statute.”52 The government contended that Apple would not be unreasonably burdened and that Apple’s assistance was necessary to effectuate the warrant. In response, Apple filed a motion to vacate, which was followed by further motions on both sides. However, the government eventually found a third party that was able to provide access and so advised the court, which led to the court vacating the order on March 29, 2016.53

V. NOTABLE DEVELOPMENTS IN PRIVACY LEGISLATION AND REGULATION

A. USA FREEDOM ACT

The USA Freedom Act of 2015,54 enacted in response to the Edward Snowden revelations, extends provisions of the USA Patriot Act that had expired and imposes limits on the bulk collection of telecommunication metadata on U.S. citizens by U.S. intelligence agencies.55 The Act was adopted after active debate in the House and Senate over a two-year period, with the substantial involvement of human rights, national security, and business and trade groups. Among the key issues addressed in the Act are bulk collection, pen registers, and trap and trace devices; the FISA Court,56 and disclosure requirements.

51. Government’s Motion to Compel Apple Inc. to Comply with This Court’s Feb. 16, 2016 Order Compelling Assistance in Search at 1–7, In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 19, 2016).
53. In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. 5:16-cm-00010-SP, slip op. at 1 (C.D. Cal. Mar. 29, 2016) (vacating order of Feb. 16, 2016).
56. The FISA Court, a U.S. federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978, addresses applications submitted by the U.S. government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. See About the Foreign Intelligence Surveillance Court, U.S. FOREIGN INTELLIGENCE SURVEILLANCE Cr., www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court (last visited Sept. 21, 2016).
Title I bans bulk collection under section 215 of the USA Patriot Act,\(^57\) requiring the government to apply for call detail records from electronic communication service or remote computing service providers based on a “specific selection term” identifying “a person, account, address, or personal device” to limit “the scope of information sought.”\(^58\) It permits the government to apply for records that are within one or two degrees of separation from the suspect. The government may apply for an initial set of call records from the providers if the government (1) states “reasonable grounds to believe that the call detail records sought to be produced based on [a] specific selection term . . . are relevant to [an authorized] investigation,”\(^59\) and (2) has “a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor.”\(^60\)

This first set of selection terms may then be sent as query requests to providers to obtain a second set of call records, but the government must first apply for the second set of records by specifying “session-identifying information or a telephone calling card number identified by the specific selection term”\(^61\) used to produce call detail records within the first set. As a safeguard, the government is required to “adopt minimization procedures” calling for “the prompt destruction of all call detail records” determined not to be “foreign intelligence information.”\(^62\)

In addition, the FISA Court may impose “additional, particularized minimization procedures” for any “nonpublicly available information concerning unconsenting United States persons.”\(^63\) Also, pen registers and trap and trace devices are banned per Title II, unless obtained by an application based on a “specific selection term.”\(^64\) The effect of these amendments is to require the government to apply to the FISA Court for specific individual call detail records for surveillance, rather than to obtain such metadata on bulk basis.

Reforms of the FISA Court are addressed in Title IV, one of which is the appointment of amici curiae to assist the FISA Court on a limited basis, such as providing “legal arguments or information regarding . . . area[s] relevant to the issue presented to the court,” if the FISA Court desires assistance in cases involving novel or significant legal interpretations.\(^65\) Limited appellate review of FISA Court decisions is permitted by both the FISA Court of Review and the U.S. Supreme Court.\(^66\) Title IV also requires the Director of National Intelligence

\(^{58}\) Id. § 1841(4)(A).
\(^{59}\) Id. § 1861(b)(2)(C)(i).
\(^{60}\) Id. § 1861(b)(2)(C)(ii).
\(^{61}\) Id. § 1861(c)(2)(F)(iv).
\(^{62}\) Id. § 1861(c)(2)(F)(vii)(I); see id. § 1861(c)(2)(F)(vii)(II) (requiring the destruction of such records).
\(^{63}\) Id. § 1861(g)(3).
\(^{64}\) Id. § 1842(c)(3).
\(^{65}\) Id. § 1803(i)(4)(C).
\(^{66}\) Id. § 1803(b). The FISA Court of Review is composed of three federal judges designated by the Chief Justice. Id.; see id. § 1871(e)(2).
to perform a declassification review of any opinion by the FISA Court or the FISA Court of Review that includes a “significant construction or interpretation of any provision of law” and, following such declassification review, make certain parts of any such opinion publicly available.67 The effect of these amendments is to provide additional support to assist the FISA Court in addressing novel or significant legal issues and to expand the opportunity for appellate review of FISA Court decisions.

Title VI prescribes additional disclosure about applications to and orders issued by the FISA Courts. Under sections 601 and 602, the U.S. Attorney General must disclose to specified congressional committees specific information about FISA Court activity, including the number of orders sought and received, estimates of the number of people targeted and affected by surveillance, and the number of appointments of amici curiae.68

Title VII addresses the targeting of non-United States persons, creating an emergency exception as to non-United States persons lawfully targeted and located outside the United States who suddenly appear in the United States. Those persons may be targeted for a brief period after they appear in the United States, provided “a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person.”69

B. FAST ACT

The FAST Act,70 which was enacted to improve the country’s transportation infrastructure, contains four notable privacy-related provisions. First, the Act modifies annual privacy notice requirements under the Gramm-Leach-Bliley Act, providing an exception if a financial institution does not share nonpublic personal information with non-affiliated third parties (other than as permitted under certain enumerated exceptions) and its policies and practices for disclosing nonpublic personal information did not change since its last distribution of its policies and practices to customers.71 Also, any investment advisers and private funds that meet these criteria need not provide annual privacy notices.72 Second, the act directs the Department of Energy to address the cybersecurity of electricity and defense electric ity critical infrastructure.73 Third, the act includes the Driver Privacy Act, which provides that data on a data event re- corder in a vehicle belongs either to the vehicle’s owner or lessee and cannot be accessed without consent, except under limited circumstances.74 Fourth, the Act provides funding for intelligent transportation systems to “assist in

67. Id. § 1872.
68. See id. §§ 1862, 1871, 1881f.
69. Id. § 1805(f)(1)(A).
72. See id.
74. Id. § 24302, 49 U.S.C.A. § 30101 note (West 2016).
the development of cybersecurity research . . . to help prevent hacking, spoofing, and disruption of connected and automated transportation vehicles,” and directs that a report be created on how the IoT may improve transportation services, including a discussion of IoT security and privacy.76

C. FCC PROPOSED PRIVACY RULES FOR ISPs

In April 2016, the FCC released a notice of proposed rulemaking regarding the privacy of broadband users and the related requirements for Internet service providers (“ISPs”). The notice proposes to protect consumer privacy through greater transparency in the ISPs’ privacy policies concerning disclosures of practices for collecting and sharing personal information, heightened protections for financial information or geolocation data, choice, and data security applied to customer proprietary information. Data breach notifications would also be required. The rulemaking would protect customer proprietary network information, including geolocation information, MAC and IP addresses, and personally identifiable information that ISPs acquire from customers. To address security, all providers would be required to establish and perform regular risk management assessments and promptly address any weaknesses identified, train employees, contractors, and affiliates that handle customer personal information, appoint a senior manager to oversee security, establish and use robust customer authentication procedures, and take responsibility for the use of customer personal information by third parties with whom the information is shared.

76. Id. § 3024.
78. Id. at 23408–10 (to be codified 47 C.F.R. §§ 64.7001–64.7005).
79. Id. at 23410–11 (to be codified at 47 C.F.R. § 64.7006) (addressing broadband internet access service providers (BIAS)); see also id. at 23407–08 (to be codified at 47 C.F.R. § 64.2011) (addressing telecommunications carriers).
80. Id. at 23408 (to be codified at 47 C.F.R. § 64.7000) (defining “customer proprietary information” or “customer PI”); see also id. at 23363–64 (seeking comment on proposal to interpret CPNI with respect to BIAS as including MAC (Media Access Control) and IP (Internet Protocol) addresses).
81. Id. at 23410 (to be codified at 47 C.F.R. § 64.7005); see also id. at 23386 (seeking comment on how to ensure security, confidentiality, and integrity of customer personal information once a BIAS provider shares it with a third party).
European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting

By W. Gregory Voss*

I. INTRODUCTION

Some of the most significant European data privacy law developments that have emerged since the European Union adopted the Data Protection Directive¹ in 1995 occurred during the past year. These include the adoption of the European Union’s General Data Protection Regulation (“GDPR”),² the invalidation by the Schrems decision of the U.S.–EU Safe Harbor cross-border data-transfer framework,³ and the subsequent replacement of the Safe Harbor framework with the EU-U.S. Privacy Shield.⁴ The “right to delisting,” which the 2014 Google Spain decision created, also experienced continued development.⁵ This survey reviews the GDPR’s main provisions—arguably the most important recent development—and then discusses the other developments noted above.

II. ADOPTION OF THE GENERAL DATA PROTECTION REGULATION

On April 27, 2016, the European Union finally adopted the GDPR, more than four years after the European Commission proposed it. The regulation came into

---

* W. Gregory Voss is a professor of business law at Toulouse University, Toulouse Business School, and an associate member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC) in Toulouse, France.

force on May 24, 2016, and it will become applicable starting May 25, 2018, when it will repeal the current Data Protection Directive. This gives companies until May 2018 to adapt to its new provisions.

European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as “data subjects,” with respect to their personal data processing. The GDPR defines both “processing” and “personal data” broadly and in adherence with the Data Protection Directive, even though it reorganizes and updates the Data Protection Directive’s definitions. Processing with respect to personal data may include, but is not limited to, the following: “collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.” The relevant personal data are “any information relating to an identified or identifiable natural person (‘data subject’),” and may include location data, online identifiers, and other forms of information that may be used to identify a data subject directly or indirectly, in addition to classic identifying data such as names and identification numbers.

The following sections address a few of the GDPR provisions that differ significantly from the Data Protection Directive and are important for businesses.

A. TERRITORIAL SCOPE

The GDPR’s territorial scope is larger than that of the Data Protection Directive. The personal data processing place no longer controls the analysis; instead, under the GDPR, processing merely must occur “in the context of the activities of an establishment of a controller or a processor in the Union,” a definition that expands the analysis to include the activities of the processor that processes personal data on behalf of the data controller. The GDPR also applies to the “processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union” so long as the processing is related to “the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union” or the monitoring of such data subjects’ behavior “as far as their behaviour takes

6. GDPR, supra note 2, art. 99(1), at 87 (“This regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.”). The date of its publication in the Official Journal of the European Union was May 4, 2016.
7. Id. art. 99(2), at 87.
8. Id. art. 94(1), at 86.
9. Id. art. 1(1)–(2), at 32; id. art. 4(1), at 33.
10. Id. art. 4(2), at 33. Compare Directive 95/46, supra note 1, art. 2(b), at 38 (defining “processing of personal data”).
11. GDPR, supra note 2, art. 4(1), at 33. Compare Directive 95/46, supra note 1, art. 2(a), at 38 (defining “personal data”).
12. GDPR, supra note 2, art. 3(1), at 32. Compare Directive 95/46, supra note 1, art. 3, at 39 (addressing scope). The consideration of a processor’s activities in determining the territorial scope of the GDPR reflects the greater accountability of processors under the GDPR, when compared to the Data Protection Directive.
place within the [European] Union.” For example, the GDPR applies to a U.S.
provider’s cloud-based-services offering to individuals in the European Union,
even where the offering requires no payment and the provider has no establish-
ment in the European Union, to the extent that the offering involves processing
those individuals’ personal data.

B. PERSONAL DATA PROCESSING PRINCIPLES

Although the GDPR’s personal data processing principles are similar to those
in the Data Protection Directive, there are a few differences. For example, the
GDPR explicitly requires data to be processed “in a transparent manner,” but
the Data Protection Directive only implicitly requires transparency. In addi-
tion, the GDPR specifies that inaccurate data must be erased or rectified “without
delay,” adding a time element to the “accuracy” principle already contained in
the Data Protection Directive. Finally, the “accountability” principle requires the
controller to be able to demonstrate compliance with the other personal data
processing principles. This latter provision ties into the new GDPR record-
keeping obligations discussed in Section II.G.

C. STORAGE OF PERSONAL DATA FOR PUBLIC INTEREST, SCIENTIFIC,
HISTORICAL, OR STATISTICAL PURPOSES

The GDPR also amends the “storage limitation” principle. Whereas the Data
Protection Directive allowed Member States to determine personal data storage
periods for “historical, statistical or scientific use,” the GDPR establishes a spe-
cific regime for personal data processing “for archiving purposes in the public
interest, scientific or historical research purposes or statistical purposes.” It ex-
empts such data from the general requirement that personal data may only be
kept in identifiable form “for no longer than is necessary for the purposes for
which the... are processed.” Instead, the data may be stored for longer pe-
riods subject to “implementation of the appropriate technical and organisational
measures required... to safeguard the rights and freedoms of the data subject.”
These measures implement the “data minimization” principle, and they may in-
clude the use of pseudonymization (for de-identification), where relevant.

In addition, the GDPR allows Member States or the European Union to deroga-
tate from a data subject’s rights to access or correct his or her personal data, and

13. GDPR, supra note 2, art. 3(2), at 33.
14. GDPR, supra note 2, art. 5(1)(a), at 35 (“processed lawfully, fairly and in a transparent man-
ner”). Compare Directive 95/46, supra note 1, art. 6(1)(a), at 40 (“processed fairly and lawfully”).
15. GDPR, supra note 2, art. 5(1)(d), at 35. Compare Directive 95/46, supra note 1, art. 6(1)(d),
at 40.
16. GDPR, supra note 2, art. 5(2), at 36.
17. Directive 95/46, supra note 1, art. 6(1)(e), at 40.
18. GDPR, supra note 2, art. 5(1)(e), at 36.
19. Id.
20. Id.
21. Id. art. 89(1), at 84–85.
object to or restrict its processing, where the derogation is for scientific or historical research purpose—or statistical purposes if the data subject’s exercise of such rights is “likely to render impossible or seriously impair the achievement of the specific purposes,” subject to the safeguards mentioned above. Another provision permits certain derogations for archiving purposes in the public interest. Where the processing has multiple purposes, the derogation will only apply to the corresponding purposes.

D. Legitimate Processing Bases, Including Consent

The GDPR retains the requirement that a legitimate basis must exist in order for personal data processing to be lawful. It further develops the “purpose limitation” principle, allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject’s consent. This compatibility determination considers, among other things, links between the two purposes, context (including the relationship between the data subject and the controller), the data’s nature (specifically, whether special data categories are involved), possible consequences for the data subject, and the existence of “appropriate safeguards,” which could include data encryption or pseudonymization.

Where consent is the processing basis, it must be unambiguous. The Data Protection Directive provided that “the data subject’s consent” meant “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.” The GDPR similarly defines data subject “consent” but provides the additional requirement that the data subject’s wishes be “unambiguous” and manifested “by a statement or by a clear affirmative action.”

The GDPR sets out additional conditions for such consent beyond those contained in the Data Protection Directive, including a requirement that the controller be able to demonstrate that the data subject has given his or her consent. If a declaration that covers other matters contains a consent request, the request must be clearly written and distinguishable from those matters, with one risk for non-compliance being that the declaration’s consent request will be non-binding. These requirements encourage good recordkeeping and proper document drafting.

22. Id. art. 89(2), at 85.
23. Id. art. 89(3), at 85.
24. Id. art. 89(4), at 85.
25. Id. art. 6, at 36–37. Compare Directive 95/46, supra note 1, art. 7(f), at 40 (“[P]ersonal data may be processed only if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party . . . .”) (emphasis added).
26. GDPR, supra note 2, art. 6(4), at 37.
27. Directive 95/46, supra note 1, art. 2(h), at 39.
28. GDPR, supra note 2, art. 4(11), at 34.
29. Id. art. 7(1), at 37.
30. Id. art. 7(2), at 37.
Under the GDPR, data subjects also must be informed of their right to withdraw consent prospectively, and this right must be as easy to exercise as it was for the data subject to initially give consent. When determining whether a data subject has freely given consent, a reviewing authority will take “utmost account” of whether contract performance (including for a service) “is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” Finally, where a child under sixteen years old is concerned, processing is lawful only if “the holder of parental responsibility over the child” gives or authorizes consent. Member States may lower this age threshold to no lower than thirteen. The controller must make reasonable efforts to verify that any such holder has given or authorized consent.

E. DATA-SUBJECT RIGHTS

The GDPR requires transparency in the provision of information to data subjects about their rights and the means of exercising them. This requirement applies regardless of whether data are collected directly from the data subject or indirectly from a third party. Under the GDPR, data subjects continue to benefit from rights they had under the Data Protection Directive, such as the right to access, the right to object to processing (which they may exercise at any time when the processing is for direct-marketing purposes), and from the transparency- and accuracy-principle requirements discussed above, as well as the related right to rectification “without undue delay.” A data subject has the right not to be subject to a “decision based solely on automated processing including profiling, which produces legal effects concerning him or her or . . . significantly affects him or her,” subject to certain exceptions, such as where the data subject provides explicit consent or where automated processing is necessary for a contract between the controller and the data subject.

The GDPR creates several new rights for data subjects beyond those provided by the Data Protection Directive. First, it creates a “right to erasure (‘right to be forgotten’)” This right is often dependent on the data subject meeting the criteria set out in the relevant clause (e.g., it is subject to there being no overriding legitimate grounds for the processing, where the data subject exercises his or

31. Id. art. 7(3), at 37.
32. Id. art. 7(4), at 37.
33. Id. art. 8(1), at 37. The age sixteen threshold specified in this provision does not affect the general law relating to the legal capacity of a child to enter a contract. Id. art. 8(3), at 38.
34. Id. art. 8(2), at 38.
35. Id. art. 12, at 39–40.
36. Id. art. 13, at 40–41.
37. Id. art. 14, at 41–42.
38. Id. art. 15, at 43. Compare Directive 95/46, supra note 1, art. 12, at 42.
40. GDPR, supra note 2, art. 16, at 43. Compare Directive 95/46, supra note 1, art. 12(b), at 42.
41. GDPR, supra note 2, art. 22, at 46. Compare Directive 95/46, supra note 1, art. 15, at 43.
42. GDPR, supra note 2, art. 17, at 43–44; see also Voss & Castets-Renard, supra note 5, at 297–98, 334–36 (terming the “right to be forgotten” as including a “right to digital oblivion”).
her right to object to it\(^4^3\), and may become inapplicable where processing is necessary for exercising the right of freedom of expression and information,\(^4^4\) for certain reasons based on the public interest,\(^4^5\) or for establishing, exercising, or defending legal claims.\(^4^6\) Furthermore, “taking account of available technology and the cost of implementation,” a controller that has made data public before being required to erase it shall take “reasonable steps . . . to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of,” such data.\(^4^7\)

Moreover, a right to restrict processing may apply, either for a period of time for purposes set out in Article 18 of the GDPR, or as an alternative to data erase.\(^4^8\) The GDPR also creates a right to data portability, which allows data subjects to request the controller to return their data in a commonly used, machine-readable format, and to request that the controller transmit such data to another controller if the processing was based on consent and was carried out by automated means.\(^4^9\) The right does not apply to processing that was necessary for public interest or official authority tasks, and it must not “adversely affect the rights and freedoms of others.”\(^5^0\)

Finally, European Union or Member State law may restrict certain data subject rights when the restriction “respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society” to safeguard, among other things, national security, defense, the fight against crime, and the furtherance of justice.\(^5^1\)

F. RESPONSIBILITIES: CONTROLLERS, JOINT CONTROLLERS, AND PROCESSORS

Under the GDPR, most data protection obligations remain the responsibility of data controllers.\(^5^2\) Unlike the Data Protection Directive, the GDPR explicitly requires joint controllers to allocate (likely through a written contract) compliance

\(^{43}\) GDPR, supra note 2, art. 17(1)(c), at 44.
\(^{44}\) Id. art. 17(3)(a), at 44.
\(^{45}\) Id. art. 17(3)(b)-(d), at 44.
\(^{46}\) Id. art. 17(3)(e), at 44.
\(^{47}\) Id. art. 17(2), at 44.
\(^{48}\) Id. art. 18, at 44-45.
\(^{49}\) Id. art. 20(1)-(2), at 45.
\(^{50}\) Id. art. 20(3)-(4), at 45.
\(^{51}\) Id. art. 23, at 46-47. The GDPR was part of a legislative package that includes a directive regarding data protection specifically in the context of justice and the fight against crime that entered into force on May 5, 2016, and must be implemented in Member State national law by May 6, 2018: Directive (EU) 2016/280 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89 (EU).

\(^{52}\) GDPR, supra note 2, art. 24, at 47; see, e.g., id. art. 7(1), at 37. The various data subject rights discussed above refer consistently to action to be taken by the controller. See, e.g., id. art. 12, at 39–40.
responsibilities between them, although data subjects may exercise their rights against each of them.53 In addition, the GDPR sets forth certain processor responsibilities, such as imposing them when a processor engages another processor, which might occur in complex processing activities.54 Both controllers and processors must cooperate with supervisory authorities upon request,55 and both are responsible for processing security (including, where appropriate, encryption, pseudonymization, testing, etc.).56 If a controller or processor is not established in the European Union, but falls within the territorial scope of the GDPR under Article 3(2), as discussed above, it will have to designate a representative to receive communications from data subjects and supervisory authorities, unless an exception applies.57

G. RECORDKEEPING; DATA PROTECTION BY DESIGN AND BY DEFAULT

The GDPR does away with the Data Protection Directive’s requirement that controllers notify supervisory authorities before carrying out processing activities,58 but it imposes new recordkeeping obligations.59 Recordkeeping obligations regarding processing activities (and cross-border data transfers outside of the European Union, where applicable) apply to both controllers and processors.60 These recordkeeping requirements should not be viewed in isolation and apply to requirements that demonstrate compliance (such as where a data subject has given consent to processing) and transparency requirements, discussed above.

In addition to compliance obligations related to recordkeeping requirements, a new provision obliges controllers to “implement appropriate technical and organisational measures” to ensure data protection by design and by default, incorporating data protection principles such as data minimization.61 Controllers may rely on voluntary certification by an approved certification mechanism as an element to demonstrate compliance.62

53. Id. art. 26, at 48.
54. Id. art. 28, at 49–50.
55. Id. art. 31, at 51. A “supervisory authority” is an independent public authority “responsible for monitoring the application” of the GDPR so as to protect data subjects’ data protection rights, which are considered “fundamental rights.” Id. art. 51(1), at 65. An example would be the French data protection authority—the CNIL. See W. Gregory Voss, After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change, 71 BUS. LAW. 281, 283–84 (2015).
56. GDPR, supra note 2, art. 32, at 51–52.
57. Id. art. 27, at 48–49. The relevant exception for companies concerns “occasional” processing and does not include large-scale processing of certain sensitive data. See id. art. 27(2)(a), at 48.
58. Directive 95/46, supra note 1, art. 18, at 43–44.
60. GDPR, supra note 2, art. 30, at 50–51.
61. Id. art. 25(1)–(2), at 48.
62. Id. art. 25(3), at 48.
H. Data Protection Impact Assessments; Prior Consultation; Data Protection Officers

The GDPR introduces a new requirement under which controllers must conduct a data protection impact assessment (“DPIA”) regarding proposed processing operations’ impact where “a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.”63 A DPIA is required where profiling is concerned,64 where there is large-scale processing of special, sensitive-data categories,65 and for data relating to criminal convictions or offenses.66 A DPIA requires four elements:

• a systematic description of the processing;
• evaluation or assessment of the respective risks referred to above;
• measures to address the risk (including safeguards, security measures, and mechanisms to ensure data protection and regulatory compliance); and
• an assessment of the “necessity and proportionality of the processing operations in relation to the purposes.”67

Controllers must consult with supervisory authorities prior to engaging in processing activities in cases where a DPIA “indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.”68 In addition, Member States may adopt laws that require consultation with—and prior authorization from—the relevant supervisory authority “in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.”69

If a controller or processor has core activities relating to either (a) “processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale,”70 or (b) “processing on a large scale of special categories of data . . . and personal data relating to criminal convictions and offences,”71 then they are required to designate a data protection officer (“DPO”), who may be an employee of the controller or processor or an external service provider hired under contract.72 European Union or Member State law may also require DPO designation in other

63. Id. art. 35(1), at 53.
64. Id. art. 35(3)(a), at 53.
65. Id. art. 35(3)(b), at 53.
66. Id.
67. Id. art. 35(7), at 54.
68. Id. art. 36(1), at 54.
69. Id. art. 36(5), at 55.
70. Id. art. 37(1)(b), at 55.
71. Id. art. 37(1)(c), at 55.
72. Id. art. 37(6), at 55.
However, one DPO may serve multiple entities: “[a] group of undertakings may appoint a single DPO provided that a DPO is easily accessible from each establishment.” The DPO must be designated based on professional qualities and expert knowledge of data protection law and practices.

The controller and the processor must also ensure that the DPO “is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.” The DPO performs his or her duties independently, shall not be penalized or dismissed for performing his or her tasks, and reports to the highest management level. DPOs are bound by an obligation of secrecy or confidentiality concerning their tasks. These tasks include, *inter alia*, informing and advising the controller or processor about its obligations under the GDPR, monitoring compliance with and engaging in awareness raising and relevant staff training, and serving as the supervisory authority’s contact point.

### I. DATA BREACH NOTIFICATIONS

Under the GDPR, the controller is obligated to notify the supervisory authority of any personal data breach “without undue delay and, where feasible, not later than 72 hours after having become aware of it...unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.” If the controller does not notify the supervisory authority within this prescribed time period, it must provide a justification for the delay. The processor must notify the controller “without undue delay” after discovering a data breach, and the latter must document any personal data breaches to allow the supervisory authority to verify compliance. If a data breach is “likely to result in a high risk to the rights and freedoms of natural persons,” the controller must also notify the relevant data subject of the breach “without undue delay,” unless an exception applies.

### J. ENFORCEMENT VIA ADMINISTRATIVE FINES

The GDPR dictates that those who are at fault for data protection violations can be charged substantial fines—in certain circumstances up to €20 million or 4 percent of an undertaking’s total worldwide annual turnover in the preceding financial year.
whichever is higher. Companies may take measures that may result in decreased fines. For example, supervisory authorities deciding whether to impose fines—and determining fine amounts—must give due regard to, *inter alia*, (1) “any action taken by the controller or processor to mitigate the damage suffered by data subjects”; (2) the controller or the processor’s degree of responsibility, “taking into account technical and organisational measures implemented by them”; and (3) adherence to approved conduct codes or certification mechanisms.

The preceding sections address only a few of the GDPR’s 99 articles, which also include 173 recitals. Interested parties should review the entire GDPR and use the time from now until its application to assess and prepare for the requirements placed upon them.

### III. INVALIDATION OF THE SAFE HARBOR: THE SCHREMS CASE

The Data Protection Directive introduced a provision that “the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection.” In 1995, the European Union did not consider the United States to be a country that ensured an adequate protection level for personal data.

In 2000, the U.S. Department of Commerce (“DoC”) and the European Commission negotiated the U.S.–EU Safe Harbor, which the European Commission then established under an “adequacy” decision in order to allow personal data transfers to U.S. companies that self-certified their compliance with the substance of EU data protection law. Companies did so by subscribing to the Safe Harbor Privacy Principles (contained in Annex I to the adequacy decision), guaranteeing certain subject rights. In *Schrems v. Data Protection Commissioner*, the Court of Justice of the European Union (“ECJ”) addressed concerns about access to personal data by U.S. authorities in connection with mass surveillance and subsequently invalidated the Safe Harbor, leaving thousands of companies without a legal basis for their cross-border personal data transfers.

---

87. *Id.* art. 83(5)–(6), at 83.
88. *Id.* art. 83(2)(c), at 82.
89. *Id.* art. 83(2)(d), at 82.
90. *Id.* art. 83(2)(j), at 82.
The ECJ emphasized that “the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person’s rights and freedoms in regard to the processing of personal data relating to him,” but found that the European Commission’s Safe Harbor decision denied these powers to the DPAs. The resulting Safe Harbor invalidation created uncertainty about data transfers to the United States by companies processing personal data.

EU Justice Commissioner Vra Jourová was quick to express willingness to work with the DoC “to complete a revamped data agreement,” and the parties commenced negotiations on what was then referred to as “Safe Harbor 2.0.”

IV. THE PRIVACY SHIELD

The European Commission/DoC negotiations led to the establishment of the “EU-U.S. Privacy Shield” and the corresponding European Commission draft adequacy decision. Attached to the draft adequacy decision are seven annexes from U.S. government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations. One improvement from a data subject perspective is greater opportunity for recourse through an independent recourse mechanism provided by the data controller. In addition, under this new framework, an individual data subject may invoke binding arbitration of claims pursuant to the Privacy Shield principles under certain conditions. Furthermore, the Federal Trade Commission (“FTC”) will review non-compliance allegations “to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated,” potentially resulting in enforcement action under the FTC Act. Moreover, the DoC has committed to providing greater oversight and Privacy Shield compliance monitoring.

Following data protection authority comments, the parties modified the EU-U.S. Privacy Shield to include “additional clarifications on bulk collection of data,

95. Schrems, supra note 93, at paras. 99–102.
96. Mark Scott, In Europe-U.S. Clash on Privacy, a Longstanding Schism, N.Y. TIMES (Oct. 7, 2015), http://nyti.ms/1Q93jJM.
97. Voss, supra note 93, at 11.
98. See Transatlantic Data Flows, supra note 4, at 3.
102. Id. at 7.
103. Id. at 24.
strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers,”105 and they adopted the final implementing decision with revised annexes.106 The Privacy Shield became operational on August 1, 2016.107

V. GOOGLE AND THE “RIGHT TO DELISTING”

In the 2014 Google Spain case,108 the court granted a natural person the right to compel delisting of newspaper pages containing information prejudicial to him when Internet users searched for his name using a search engine. Google sought to limit the right’s geographic scope to European web domains, while the French data protection authority (“CNIL”) sought to have the delisting extended to all relevant domains including “.com.” The CNIL issued an order to that effect, which Google contested, prompting the CNIL to commence a formal procedure against it.109

On March 10, 2016, the CNIL Restricted Committee imposed a €100,000 fine on Google. In doing so, it rejected Google’s offer that it would “filter results based on the geographic origin of the person performing the search,” meaning that “people using the search engine from the same country [as] the plaintiff’s country [could] not access the delisted result anymore.”110 The CNIL commented that “[o]nly delisting on all of the search engine’s extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold” the right to privacy.111 Google announced that it was appealing the decision to the highest French administrative court.112

109. See Voss, supra note 55, at 283–84.
111. Right to Be Delisted, supra note 110.
112. See Mark Scott, Google Appeals French Privacy Ruling, N.Y. TIMES (May 19, 2016), http://nyti.ms/2527XoV (“In France, Google’s appeal, which will be heard by the Conseil d’État, the country’s highest administrative court, in the coming months, is unlikely to resolve the continuing standoff over people’s right to privacy online. A decision in the case is expected next year.”).
VI. CONCLUSION

The European Union has finally adopted data protection law reform, and now is the time for companies to adapt to the new landscape before the GDPR applies in May 2018. Many of the GDPR’s provisions address companies’ compliance obligations and require greater accountability and recordkeeping. Some provisions may require changes to internal organization (e.g., DPOs, DPIAs, and procedures that allow for proper data breach notifications). The United Kingdom’s DPA issued a checklist of steps to prepare for the GDPR. These include raising awareness, documenting held personal data, reviewing privacy notices to bring them into conformity with the GDPR, checking that procedures cover all data subject rights and adapting them to cover handling data subject requests, identifying legal bases for processing, implementing systems to verify ages of children and to gather parental or guardian consent, implementing procedures regarding data breaches, designating DPOs if required, and identifying any applicable supervisory authorities.113

With respect to cross-border personal data transfers, companies may now self-certify under the Privacy Shield. They should monitor developments regarding the right to delisting, as this affects access to information on the Internet.

In conclusion, it is clear that EU data protection and privacy law reform over the past year will necessarily require adaptation by companies and others for years to come.

Social Media Law: Significant Developments

By Christopher Escobedo Hart*

I. INTRODUCTION

“Social media law” is not a monolith. It is, instead, an amalgam of constitutional law, employment law, criminal law, administrative law, intellectual property law, tort law, and even the rules of discovery as applied to the ubiquitous—and relatively recent—presence and use of online and mobile platforms for sharing and creating content. Individuals use social media—Facebook, LinkedIn, Twitter, among other platforms—to keep in touch with friends and family, make professional connections, and communicate their personal, political, religious, or other views. Institutions use social media to extend their brand, recruit talent, sell their products, or communicate their message. One’s “online presence” can be a consequential factor in his or her ability to be hired. Groups of people can turn to social media to organize political protests or campaigns. Law enforcement can turn to social media as part of an investigation. And would-be fraudsters, hackers, or cyberterrorists can seek the private information embedded in users’ online accounts to carry out their schemes. The reach of social media in ordinary citizens’ lives is surprisingly vast—so too can be the reach of law into the use of social media.

Despite not being, strictly speaking, its own area of law, the term “social media law” usefully captures this complex interplay between different areas of law and social media platforms. This survey provides an overview of significant developments in social media law over the past year, concerning multiple categories: copyright, fair competition, First Amendment (including its intersection with criminal law), and employment. While these areas of law do not together comprise the universe of topics implicated by the use of social media, they are among the ones that most frequently arise in litigation.

One important takeaway from the cases examined below is the clear evidence that social media spaces, while relatively new and technologically unique, are treated similarly to other real-world spaces. Courts have not created brand new rules and paradigms to grapple with social media ubiquity and complexity, but rather have consistently applied existing legal standards to the social media space. Whether they have done so well is a separate issue, but they have done so consistently. If nothing else, this consistent application of well-established prin-

* Foley Hoag LLP, Boston.
ciples suggests that, at least in the legal world, there is little difference between online and offline conduct.

II. COPYRIGHT: CAN I MARKET YOUR PICTURES IF SOMEONE ELSE POSTS THEM ON INSTAGRAM?

Social media can raise a host of questions regarding intellectual property, including copyright. One high-profile case bears watching. According to a complaint filed in the U.S. District Court for the Southern District of New York in December 2015, artist Richard Prince took photographs that had been posted on Instagram accounts without the copyright owner’s permission, enlarged and printed the photos together with the text that appeared above and below them on Instagram, displayed them at the Gagosian Gallery in New York, and sold them.¹ He was sued by Donald Graham, the author of one of the appropriated photographs, who claimed copyright infringement and requested injunctive relief (in the form of forcing Prince and the gallery to cease displaying the repurposed work) and damages. As of this writing, defendants have filed a motion to dismiss and briefing is pending.

The central question in the motion to dismiss is whether Prince’s use of the photos is protected use as “appropriation art.” Relying on the Second Circuit case *Cariou v. Prince*,² in which Richard Prince was also a defendant, Prince argued that “appropriation art can be considered ‘transformative’ as a matter of law and, therefore, make fair use of copyrighted material.”³ In response, Graham argued that, even where *Cariou* did not find fair use, Prince had “copied far less and added far more” of the appropriated art.⁴

The case bears watching for several reasons. First will be the court’s legal reasoning on the motion to dismiss: whether *Cariou* (and other cases) effectively foreclose a copyright infringement action on “appropriation art”—making the decision potentially generalizable and thus far-reaching—or whether, as Graham argues, more facts are needed before a disposition can be reached. Second, should the case go forward, the court will decide whether Prince’s method of using the appropriated art was sufficiently “transformative” to permit a finding of fair use. And third, regardless of the outcome in the district court, the Second Circuit will almost certainly weigh in on this question, further defining the use of publicly available content on social media sites and what constitutes fair use of such content.

². 714 F.3d 694, 705–06 (2d Cir. 2013) (“Transformative works . . . lie at the heart of the fair use doctrine . . . .”) (citation omitted).
III. FAIR COMPETITION: WHAT IS FAIR, AND WHAT IS DECEPTIVE, IN ONLINE ADVERTISING?

The Federal Trade Commission (“FTC”) has been actively involved in defining what constitutes fair advertising in social media spaces. In December 2015, the FTC issued a policy statement addressing certain types of advertising commonly appearing in social media spaces.\(^5\) Relying on its broad section 5 powers, which allow it to prevent “unfair or deceptive acts or practices in or affecting commerce,”\(^6\) the FTC took aim at so-called “native advertising” and “sponsored content,” which, in the FTC’s view, are “often indistinguishable from news, feature articles, product reviews, editorial, entertainment, and other regular content.”\(^7\)

The Policy Statement follows certain important cases, such as In re Machinima, Inc.,\(^8\) in which the FTC complained that Machinima was “paying influencers to post YouTube videos endorsing Microsoft’s Xbox One system and several games,” and that those paid “failed to adequately disclose that they were being paid for their seemingly objective opinions.”\(^9\) The FTC’s final consent order with Machinima (which neither admitted nor denied the FTC’s allegations) prohibits Machinima from “misrepresenting in any influencer campaign that the endorser is an independent user of the product or service being promoted.”\(^10\) The FTC cited this case in its Policy Statement, and it set forth various factors that it will use in determining whether online digital advertisement is misleading—that is, to determine “the net impression the advertisement conveys to reasonable consumers.”\(^11\) Among those factors are (1) an ad’s “overall appearance,” (2) “the similarity of its written, spoken, or visual style to non-advertising content offered on a publisher's site,” and (3) “the degree to which it is distinguishable from such other content.”\(^12\) The touchstone for the FTC is “how reasonable consumers would interpret the ad in a particular situation.”\(^13\) Reasonableness, in turn, means that “an interpretation or response of consumers to a particular ad need not be the only one nor be shared by a majority of consumers.”\(^14\) Assisting the FTC in communicating what kind of ads will be considered fair and deceptive is the FTC’s

---

10. Id.
12. Id.
13. Id.
14. Id.
Guide for Businesses, which contains seventeen specific examples of how content can be deceptive, and how deception can be prevented by use of appropriate disclosures. From a reading of the Policy Statement’s discussion of the factors it will use, as well as a review of the examples it provides in its Guide for Businesses, the FTC clearly will consider the nature of online advertisements on a fact-intensive, case-by-case basis.

IV. FIRST AMENDMENT

A. SELFIES AT THE BALLOT BOX

Social media has created rich new avenues for ordinary citizens, employers, institutions, and the government to speak. Whether this represents promise or peril for American democracy remains to be seen. As the cases below demonstrate, courts have used traditional ways of thinking about the First Amendment in social media spaces, suggesting that social media will also be a rich medium for development in First Amendment law.

In 2014, New Hampshire enacted an amendment to a voting law, specifying the illegality of voters posting pictures of their ballots in online media. The U.S. District Court for the District of New Hampshire struck down the law in Rideout v. Gardner, holding that the law was content-based and failed the strict-scrutiny test. The law is content-based because, according the court, “it requires regulators to examine the content of the speech to determine whether it includes impermissible subject matter.” The court held that the defendant had failed to show that the law addresses “an actual problem” and therefore failed to carry his burden of showing that it promotes a compelling state interest. The problem that the law purportedly addressed was that of vote-buying or voter coercion, but there was no evidence that photographic images of ballots were being used for that purpose. The court also found that the statute was not narrowly tailored because it was “vastly overinclusive,” applying almost exclusively to “those who wish to use images of their completed ballots to make a political point.”

B. CYBERBULLYING LAWS

In State v. Bishop, the Supreme Court of North Carolina held that the state’s cyberbullying statute violated the First Amendment. The case involved a high

18. Id. at 229.
19. Id. at 231.
20. Id. at 231–33.
21. Id. at 234.
school student who was being tormented by classmates in Facebook posts, often sexual in nature. The defendant was convicted under North Carolina’s cyberbullying statute. Disagreeing with the courts below, the North Carolina Supreme Court held that the statute prohibited not the non-expressive conduct of the “act” of posting online, but the speech itself. In making this determination, the court reasoned that there is no substantive distinction between posting online and other traditional forms of protected speech.23 “Such communication does not lose protection,” the court opined, “merely because it involves the ‘act’ of posting information online, for much speech requires an ‘act’ of some variety—whether putting ink to paper or paint to canvas, or hoisting a picket sign, or donning a message-bearing jacket.”24

Moreover, the court determined that the law was a content-based restriction on speech, and that it failed strict scrutiny. Although it was undisputed that the state had a compelling interest in protecting children from online bullying, the court determined that the statute was not the least restrictive means to achieve that end. The language of the statute, the court observed, did not specify that the target of the posting must suffer an injury, or even that the target must be aware of the posting, before criminal penalties could apply.25 Moreover, the statute was filled with such undefined, and thus potentially expansive, language (for example, the state offered that the word “torment” in the statute could be construed to include “annoy”) that the court concluded the statute was unnecessarily broad.26

C. Comments as Protected Speech

James Plowman is the Commonwealth’s Attorney in Loudoun County, Virginia, and was charged with overseeing a profile page about the Office of the Commonwealth’s Attorney on social networking sites, including Facebook. The plaintiff, Brian Davison, posted a comment on the office’s Facebook page, complaining about a dispute he had with members of Loudoun County Public Schools. Plowman deleted Davison’s comment and blocked him from posting any additional comments. After Davison filed a lawsuit, claiming that blocking the comments violated his First Amendment rights, the office restored Davison’s ability to comment and reinstated the deleted post. Plowman then moved to dismiss the complaint as moot. In Davison v. Plowman,27 the U.S. District Court for the Eastern District of Virginia denied the motion, on the ground that voluntary cessation of the challenged conduct did not moot the case because there is a reasonable expectation that the conduct will resume. If the case moves forward, the central issue will be whether Plowman violated Davison’s First Amendment right to free speech by deleting his Facebook comment and blocking further postings.

23. Id. at *3.
24. Id.
25. Id. at *6.
26. Id.
By contrast, in *White v. Ortiz*,\(^2^8\) the court denied a motion to dismiss claims of invasion of privacy and defamation where the defendant allegedly used fake Twitter handles and other online identifiers to post, putting it mildly, negatively (and often viciously) about the plaintiff. The defendant argued, among other things, that the postings were protected by the First Amendment. The court disagreed, noting that the First Amendment was not so expansive as to protect all of the defendant’s Twitter content. The court otherwise applied New Hampshire law on privacy and defamation and allowed the claims to proceed.\(^2^9\)

All of these cases suggest that conduct that employs social media—posting a photograph of a ballot, engaging in harassing speech online, and censoring online speech—will be evaluated under traditional legal standards.

V. EMPLOYMENT: ONLINE CONDUCT AS PROTECTED CONCERTED ACTIVITY

In *Three D, LLC v. NLRB*,\(^3^0\) the Second Circuit affirmed an NLRB determination that an employer committed an unfair labor practice in violation of the National Labor Relations Act (“NLRA”) when the employer, Triple Play, discharged employees for their Facebook conduct. The employee conduct at issue in the case was (1) an employee’s “like” of another employee’s Facebook post critical of Triple Play and (2) another employee’s comment expressing agreement with the criticism. All comments concerned the employer’s claimed errors in tax withholding, a subject that was also discussed by employees within the workplace. The court upheld the NLRB’s determinations that the Facebook activity was protected concerted activity and therefore within the scope of the NLRA, and that the employees’ actions were not “so disloyal or defamatory as to lose the protection of the Act.”\(^3^1\) The court also upheld the board’s determination that the company’s online communication policy, which prohibited employees from engaging in “inappropriate discussions,” could reasonably be construed by employees as prohibiting protected activity and, therefore, violated the NLRA.\(^3^2\)

This case is of a piece with other NLRB actions in the social media space, which are highly protective of workers’ rights to engage in concerted activity. The case demonstrates that the NLRB has adapted to the ubiquitous use of social media by employees, and that, while employers may create reasonable policies to protect a company’s products, services, brand, and reputation from harm and


\(^{29}\) Id. at *4–6. Also in the realm of tort law, the U.S. District Court for the Southern District of Florida allowed multiple tort claims to proceed in *Binion v. O’Neal*, No. 15-60869-CIV-COHN/SELTZER, 2016 WL 111344 (S.D. Fla. Jan. 11, 2016), arising from former NBA star Shaquille O’Neal posting pictures, in humiliating fashion, of the plaintiff on Twitter and Instagram.


\(^{31}\) *Three D, LLC*, 629 F. App’x at 36.

\(^{32}\) Id. at 38.
disparagement, a court will strike a balance in favor of employee’s rights to speak critically within certain limits.

VI. LITIGATION: ARE YOUR FACEBOOK POSTS DISCOVERABLE?

In general, there are no special rules for discoverable content within social media. Like e-discovery rules in general, whether social media content is discoverable depends on general standards of reasonableness, so long as the applicable civil rules otherwise permit such discovery.

In one case that has garnered attention, Forman v. Henkin,\(^3\) the New York State Appellate Division rejected a defendant’s request, in a personal injury case, to private photos of plaintiff and messages by plaintiff posted on Facebook—that is, to non-public social media information. Discovery of the social media photos was prompted, at least in part, by the plaintiff’s allegation that, prior to the injury, she had led an active life that was reflected in her Facebook postings, but that her activities were severely inhibited as a result of the injury. The majority held that the requests amounted to a fishing expedition because the broad requests for texts and photographs posted to friends and families were not tethered to anything other than speculation as to their relevance: that is, that the ordinary rules applied and there was nothing special in discovery about social media. But in dissent, one justice argued the opposite: that in fact there is a complex web of rules regarding discovery for social media content that simply does not exist for other kinds of documents, and that this complex web should be dismantled. As one example, New York case law provides that, at least in some circumstances, a request for private social media content must be predicated on the existence of public content, and then the private content must be examined in camera.\(^4\) As the dissent argued: “There is no reason why the traditional discovery process cannot be used equally well where a defendant wants disclosure of information in digital form and under the plaintiff’s control . . . . There is no particular difficulty in applying our traditional approach to discovery requests for information posted on social networking sites.”\(^5\)

VII. CONCLUSION

Social media presents a rich avenue for the development of law in numerous fields. So long as it maintains its ubiquity—where generating and being exposed to content is as simple as a swipe of a thumb on a wearable device—questions regarding its use will continue to wind their way through the courts. But as the above cases demonstrate, social media is not working a revolution in the law, but rather is part of the law’s slow, steady evolution.

---


\(^{5}\) Id. at 188 (Saxe, J., dissenting).
Online Contracting

By Nancy S. Kim*

I. INTRODUCTION

Cases addressing contract formation in the online environment have generally held that there was assent to contract if there was “reasonable notice” and a “manifestation of assent.”1 “Reasonable notice” could be actual notice or constructive notice, the latter meaning that the notice was conspicuous enough that a “reasonably prudent offeree”2 would have been alerted to it. A “manifestation of assent” means either that the user affirmatively agreed to the terms, such as by clicking to indicate agreement (typically referred to as a “clickwrap” or “click-through” agreement), or that the user continued to engage with the website after receiving notice that terms applied to website activity (typically referred to as a “browsewrap” agreement).

The recent cases do not change the standards for assent to online contracts. They do, however, provide more guidance as to how these standards are applied. Significantly, in these cases, the courts engaged in a more nuanced analysis of notice. Continuing the trend seen in Berkson v. Gogo LLC3 and Nguyen v. Barnes & Noble Inc.,4 these cases focused on how the terms were presented to the user. Generally, the courts are taking a more sophisticated approach to assess what conspicuous notice means in the online context.

This shift in wrap contracting doctrine should not be surprising. Unlike in the early days of the Internet, when the first online contract cases were decided, likely all of the judges deciding these most recent cases have had personal experience with online contracts and are familiar with the way users encounter and interact with online contracts. These courts are applying existing contract rules in a way that recognizes the burdens that wrap contracting formats place on consumers. Consequently, they are paying attention to website design, presentation of terms, and the process by which consumers must manifest assent to determine whether a contract was formed.

* ProFlowers Distinguished Professor of Internet Studies and Professor of Law, California Western School of Law.
1. See Specht v. Netscape Commc’ns Corp., 306 F.3d 17, 35 (2d Cir. 2002) (“Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility.”).
2. Id. at 30.
4. 763 F.3d 1171 (9th Cir. 2014).
Consistent with a more sophisticated understanding of online contracts, several courts seem to be acknowledging the folly of blanket assent to online terms and rejecting the view that notice that contract terms apply to the transaction means notice of (and assent to) all of the terms. Concordant with the notion that notice of a contract does not equal notice of specific terms, courts seem to be paying more attention to the potential for altering digital terms. For example, even if a business proves that a user clicked to proceed on a website, the court may require the business to prove that the user clicked to a particular version of the terms of use, which may require that it provide evidence that there were safeguards to prevent fraudulent alterations to agreements. Accordingly, courts may start to move away from the notion that a click on an icon is the same as a signature on a page.

II. ANALYSIS OF CASES

A. IMPORTANCE OF RECORDKEEPING AND PROPER PROCEDURES

The court, in Dillon v. BMO Harris Bank, N.A., focused on both issues of proof and the potential for fraud. The plaintiff in that case, James Dillon, applied online for loans from USFastCash and VIN Capital, two payday lenders. He clicked through various terms and conditions which, other than the loan amount, he did not read. The two lenders accepted his online applications and provided him with the money. The defendant, Bay Cities Bank, facilitated the transaction by providing access to the Automated Clearing House Network. Dillon alleged that the lenders charged usurious interest rates, and he sued Bay Cities, asserting violations of the Racketeer Influenced and Corrupt Organizations Act. Bay Cities moved to compel arbitration based on the agreements between Dillon and the payday loan lenders. Although there was “no dispute” that Dillon entered into contracts with the lenders, this was not enough to establish that “the lenders presented and Mr. Dillon accepted an arbitration provision as part of the loan agreement.” The court stated that the relevant questions were “whether the lenders presented the arbitration provisions in the proffered documents to Mr. Dillon during the online loan process” and “whether the proffered documents accurately reflect the terms to which Dillon and the lenders mutually agreed.”

Applying North Carolina law, the court first analyzed the contract between Dillon and USFastCash. In support of its argument that there was an agreement to arbitrate, Bay Cities offered a declaration from Christopher Muir, an employee of an entity that provided various services to USFastCash. Muir stated that he...
had personal knowledge of USFastCash’s online loan application process and that applicants agreed to an arbitration provision in their application and in their loan note and disclosure. He also affirmed that he reviewed Dillon’s records, which contained the loan application and loan agreement.11

The court expressed skepticism, given USFastCash’s “history of dishonesty in court proceedings,”12 and found Muir’s declaration insufficient to establish that an arbitration provision was presented to Dillon in the loan application process. The court noted that Muir’s declaration did not explain how the electronic document that purportedly memorialized the loan agreement was created, nor did he affirm that the document which was presented to the court was presented to Dillon in the same format.13 In addition, his declaration did not explain how USFastCash maintained its electronic records or preserved its documents so they could not be altered. Furthermore, the court stated that the screenshots of the USFastCash homepage, which were attached to Muir’s declaration, did not bear Dillon’s name or personal information, or the relevant dates.14

Bay Cities also offered as evidence what it claimed to be the loan agreement, but the court found this too failed to prove that Dillon agreed to an arbitration clause. The court explained that “[c]lick-wrap contracts like the one at issue here pose special risks of fraud and error.”15 With online transactions, one of the parties has exclusive control of the electronic record, which means that it could fraudulently alter the document.16 Even absent fraud, the court noted that there was a risk of error in the production of the document that could include agreements where the click-through process varied over time.17 Finally, the court noted that the risk of error was even higher when, as here, the party maintaining the record was not the party who produced the records.18 For similar reasons, including the witness’s lack of familiarity with the lender’s online record creation and retention practices, the court found that there was no agreement to arbitrate between Dillon and VIN Capital.

The court indicated that a click did not have the same evidentiary weight as a signature on a page, noting that there was no evidence that the document was created accurately or maintained without alteration, “[i]nor does the document contain a physical signature, which often is circumstantial evidence of agreement.”19

This case indicates that courts will not necessarily accept, without adequate proof, a vendor’s claim that an electronic document it submits as evidence is the document to which the consumer assented during an online contracting

11. Id. at *3.
12. Id.
13. Id.
14. Id. at *4.
15. Id.
16. For example, the court explained, “an unscrupulous lender could add an arbitration provision if it was sued by the borrower, but delete the arbitration provision if the lender filed suit claiming a default.” Id. at *4 n.5.
17. Id. at *4.
18. Id.
19. Id. at *9.
session. Dillon v. BMO Harris Bank, N.A. highlights the importance of good recordkeeping practices on the part of companies who seek to enforce online contract terms. It also conforms to a trend seen in several recent cases of distinguishing notice and assent to a contract from notice and assent to particular terms.

B. NOTICE OF CONTRACT VS. NOTICE OF TERMS

Handy v. LogMeIn, Inc. does not involve a dispute about contract formation, but is illustrative of this trend of distinguishing types of notice. The plaintiff, Darren Handy, obtained LogMeIn Free, a product that the defendant provided free of charge, which allowed access to a remote desktop computer from another computer. The plaintiff subsequently purchased a companion product from the defendant, called Ignition, for $29.99. Four years later, the defendant discontinued LogMeIn Free and began offering a subscription-based premium product, LogMeIn Pro. Handy sued under California’s False Advertising Law and Unfair Competition Law, claiming that he would not have purchased Ignition if he had known that LogMeIn Free would be discontinued. Accordingly, Handy had to show that the defendant fraudulently omitted informing its users that LogMeIn Free could be discontinued.

The defendant introduced the “Terms and Conditions of Use” (the “Terms”) that applied when the plaintiff purchased Ignition and which users had to click to accept when they signed up for LogMeIn Free. The Terms stated that the defendant could “modify or discontinue any Product for any reason or no reason with or without notice to You or the Contracting Party. [LogMeIn] shall not be liable to You or the Contracting Party or any third party should [LogMeIn] exercise its right to revise these Terms or modify or discontinue a Product.”

Handy argued that the Terms were not binding as a browsewrap. The court stated that whether the Terms constituted an enforceable contract was “irrelevant” to whether they provided notice to prospective purchasers that LogMeIn Free could be discontinued. By posting the information to its website, the defendant published the fact that it reserved the right to terminate LogMeIn Free.

In a footnote, the court noted that there was no effort by the defendant to bind
plaintiff to the Terms, but that they were used to “demonstrate merely that it posted notice of their policies.”

Handy v. LogMeIn is another case recognizing that notice serves different purposes and that a higher standard of “notice” is required for purposes of establishing assent. Although the availability of terms on LogMeIn’s website was sufficient to show that LogMeIn did not violate California’s False Advertising and Unfair Competition statutes (because it showed that the company was not intentionally concealing that it could discontinue its products), the court’s language indicates that the notice in this case would have been insufficient to constitute contractual assent.

C. Website Design and Contract Presentation

1. Resorb Networks, Inc. v. YouNow.com

A New York trial court recently looked to Berkson v. Gogo LLC to determine the enforceability of online agreements. In Resorb Networks, Inc. v. YouNow.com, the plaintiff, Robert Ianuale, was a user and a partner broadcaster of YouNow, a live video platform, until the defendants deactivated his account. He sued, claiming defamation, commercial disparagement, trade libel, and breach of contract. The defendants, maintaining that he entered into an online agreement to arbitrate his claims, moved to compel arbitration.

The YouNow sign-in page gave users the option to sign in using their social media account. Underneath the sign-in options, the screen states: “By signing in you agree to our terms of use.” Adi Sideman, the CEO of the YouNow companies, stated in an affidavit that the bolded words were a hyperlink, but the affidavit was ambiguous as to whether the hyperlink led to the YouNow Terms of Use, which contained an arbitration provision, or to the License Agreement, which did not.

A button at the bottom of the partner page included a hyperlink labeled “Apply Now” which took the user to the partner broadcast application form. The user would then click “Submit” to submit its application form. YouNow sent acceptance notifications to eligible users that requested that the application be completed by clicking “Continue.” Clicking on the “Continue” button took the user to a page with the heading “Partner Agreement.” At the bottom of that page was a white box next to the words “I also agree to the Partner Agreement & Terms and Conditions.” Sideman said that the words “Terms and Conditions” were a hyperlink to YouNow’s Terms of Use, which contained an arbitration clause. (The Partner Agreement did not contain an arbitration clause.) Underneath the white box, which the user had to check, was a blue box that stated “Yes, I agree,” which the user also had to click in order to proceed.

27. Id. at *9 n.4.
29. Id. at 507–08.
30. Id. at 508 (quoting YouNow website).
After the user checked the white checkbox and clicked the blue “Yes, I agree” button, the next screen stated, “You’re In!” Each time a user signed in, the user was presented with a statement that, by signing in, the user agreed to the Terms of Use.31

The court stated that where “the supposed assent to terms is mostly passive, as it usually is online, courts seek to know ‘whether a reasonably prudent offeree would be on notice of the term at issue’ and whether the terms of the agreement were ‘reasonably communicated’ to the user.”32 To determine whether this standard was met, the court looked to the three general principles set forth in Berkson v. Gogo LLC:

First, the website must be designed such that a “reasonably prudent user” will be placed on “inquiry notice” of the terms of using the website. Second, the design and content of the website must encourage the user to examine the terms “clearly available through hyperlinkage.” Third, agreements will not be enforced where the link to the agreement is “buried at the bottom of a webpage or tucked away in obscure corners of the website.”33

The court concluded that the defendants’ presentation of the arbitration clause did not adhere to these requirements.34 Sideman’s affidavit failed to state unambiguously that the hyperlink labeled “terms of use” actually led to the Terms of Use, which contained the arbitration clause.35 Furthermore, defendants’ statement that the Terms of Use were accessible somewhere on the website did not establish that a “reasonably prudent offeree” would have noticed the terms, because they did not state where on the website the terms appeared.36

The defendants argued that their tracking system showed that the plaintiff had spent 1,162 minutes on its website in a category called “Policy,” which included the Terms of Use. The plaintiff argued that there were alternative explanations, including that there was no evidence that he was the one viewing the relevant pages. The court agreed, finding that there was insufficient foundation for finding that it reflected activity by the plaintiff.37

Finally, the defendants argued that they sent an e-mail to all partners that stated that partners should adhere to the company’s Terms of Service. The court found that it was not clear that the Terms of Service referenced the same document as the Terms of Use or that it was a hyperlink to the Terms of Use page.38

31. Id.
33. Id. (citations omitted) (quoting Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 401–02 (E.D.N.Y. 2015)).
34. Id.
35. Id.
36. Id.
37. Id. at 512.
38. Id.
2. Long v. Provide Commerce, Inc.

In Long v. Provide Commerce, Inc., the California Court of Appeal likewise carefully examined website design and contract presentation and concluded that there was no conspicuous notice of terms on a website and in an order confirmation e-mail. The plaintiff, Brett Long, purchased a flower arrangement via Provide’s website, ProFlowers.com. Long alleged that the goods were not as described, and he brought claims against Provide under the state’s Unfair Competition Law and the Consumer Legal Remedies Act. The defendant moved to compel arbitration, arguing that the plaintiff was bound by its website Terms of Use.

When Long placed his order, the Terms of Use were accessible through a capitalized and underlined hyperlink, TERMS OF USE, located at the bottom of each webpage. The hyperlink was in light green typeface on the website’s lime green background along with fourteen other capitalized and underlined hyperlinks of the same color, font, and size.

To complete his order, Long was required to enter information and click through a multi-page “checkout flow.” The information fields and the click-through buttons were in a bright white box set against the website’s lime green background. At the bottom of the white box were the words “Your order is safe and secure.” Below the white box was a dark green bar with a hyperlink “SITE FEEDBACK” in light green typeface. Below the dark green bar at the bottom of each page of the checkout flow were two hyperlinks, “PRIVACY POLICY” and “TERMS OF USE.” These two hyperlinks were in the same light green typeface displayed against the website’s lime green background.

After Long placed his order, Provide sent him an e-mail confirmation. The e-mail message included multiple lines of information, including: the ProFlowers logo alongside the words “order confirmation”; a dark green bar with several hyperlinks to other product offerings for different occasions, such as “Birthday”; a light green bar thanking the customer for the order; a summary of the order; two banner advertisements; a notification regarding online account management services; yet another dark green bar with the words “Our Family of Brands” and six different brand logos; and a paragraph listing customer service information in small grey type. There followed, in the same small grey type, two hyperlinks labeled “Privacy Policy” and “Terms,” and finally the company’s corporate address in the same small grey type.

The arbitration clause on which the defendant relied appeared in the website’s Terms of Use. Provide argued that the plaintiff was on “inquiry notice” of the clause because the Terms of Use hyperlink was immediately visible on the checkout flow, was viewable without scrolling, and was located next to fields that the user had to complete.
The trial court disagreed and ruled that the hyperlinks on the website and in the e-mail were too inconspicuous to put a reasonably prudent Internet consumer on inquiry notice, and the appellate court affirmed. The court noted that the fact that the Terms of Use hyperlinks were visible without scrolling was insufficient to establish an enforceable browsewrap. It quoted with approval the “bright line rule” set forth in Nguyen v. Barnes & Noble Inc.:

[W]here a website makes its terms of use available via a conspicuous hyperlink on every page of the website but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent, even close proximity of the hyperlink to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice.

The court found that, in view of the “placement, color, size and other qualities” of the hyperlinks “relative to the . . . website’s overall design,” the presentation of the terms failed to meet the standard of conspicuous notice. In making its determination, the court discussed the screenshots in detail and noted that it was difficult to find the Terms of Use hyperlinks in the checkout flow “even when one is looking for them . . . [,] to say nothing of how observant an Internet consumer must be to discover the hyperlinks in the usual circumstance of using Pro-Flowers.com to purchase flowers.”

The court further stated that, while the lack of conspicuous notice resolved the matter, it agreed with the Ninth Circuit in Nguyen v. Barnes & Noble that “to establish the enforceability of a browsewrap agreement, a textual notice should be required” to alert the user that continued use of the website constitutes assent to the terms. In other words, a conspicuous hyperlink alone “may not be enough to alert a reasonably prudent Internet consumer to click the hyperlink.”

3. Sgouros v. TransUnion Corp.

The last case for discussion, Sgouros v. TransUnion Corp., comes out of the Seventh Circuit, the circuit that decided the landmark case in this area, ProCD, Inc. v. Zeidenberg. Gary Sgouros purchased a credit score report from TransUnion's website. He discovered, however, that the score was useless to him, because the lender he approached with it used a different score calculated using a different formula. Sgouros sued TransUnion alleging violations of credit and consumer protection statutes.
To purchase the credit score, the plaintiff had to click on a large orange “Click Here” button on the homepage underneath the heading “Get Your Credit Score & Report.” This took him to a page with the message “Your FREE credit score & $1 credit report are only moments away.” Underneath that were boxes indicating that the user was on Step 1 of 3 required to complete the application process. Step 1 required the user to input various personal information in different fields. The user then had to click on another orange button that contained the words “Submit & Continue to Step 2” and a green arrow. The court included a color copy of a screenshot of the Step 1 page.55

The court also included a color copy of a screenshot of the Step 2 page. On this page, the customer created an account user name and password and filled in credit card information. The question “Is your home address the same as your billing address?” requires the customer to fill in either the “Yes” or “No” bubble. Underneath these bubbles was a rectangular scroll window. Appearing at the top of the scroll window were the words “Service Agreement.” Underneath that line were two fully visible lines and a third that was still legible but partially obscured. The visible text read: “Welcome to the TransUnion interactive website, membership.tui.transunion.com (the ‘Site’). This Service Agreement (‘Agreement’) contains the terms and conditions upon which you (‘you’ or ‘the member’) may access and use.”56 Underneath the scroll window, in small hyperlinked text, were the words, “Printable Version.” Below that was the following paragraph in bold text:

You understand that by clicking on the “I Accept & Continue to Step 3” button below, you are providing “written instructions” to TransUnion Interactive, Inc. authorizing TransUnion Interactive, Inc. to obtain information from your personal credit profile from Experian, Equifax and/or TransUnion. You authorize TransUnion Interactive, Inc. to obtain such information solely to confirm your identity and display your credit data to you.57

Underneath that paragraph was a button that contained the words “I Accept & Continue to Step 3” followed by a small green arrow. The user was not required to click on or scroll down the scroll window. Furthermore, the court noted that the website did not “in any other way call his attention to any arbitration agreement.”58 The first page of the printable version of the agreement contained a brief statement indicating that it included an arbitration clause and a class action waiver. The arbitration provision itself was on page eight of the ten-page printable version of the agreement.59

TransUnion argued that the plaintiff’s act of clicking on the “I Accept & Continue to Step 3” button indicated his acceptance of the agreement. The court applied the “reasonable communicativeness” test to determine “whether the web

55. *Id.* at 1031.
56. *Id.* at 1032 (quoting TransUnion’s website).
57. *Id.* at 1033 (quoting TransUnion’s website).
58. *Id.*
59. *Id.*
pages presented to the consumer adequately communicate all the terms and conditions of the agreement, and whether the circumstances support the assumption that the purchaser receives reasonable notice of those terms.”

The court held that this criterion was not met. It noted that the web pages that Sgouros viewed contained “no clear statement that his purchase was subject to any terms and conditions of sale.” The scroll window contained the words “Service Agreement” but did not indicate what terms it governed. The hyperlink that led to the terms was labeled with the wholly uninformative words “Printable Version,” rather than with a phrase, like “Terms of Use” or “Service Agreement,” that would have alerted a purchaser to the nature of the document to which it linked.

Most significant, according to the court, was the fact that the website “actively misleads the customer.” The bold text immediately underneath the scroll box stated that clicking on the “I Accept & Continue to Step 3” button authorized TransUnion to obtain the customer’s personal information, but did not say that it indicated acceptance to contractual terms. The court stated that “[n]o reasonable person would think that hidden within that disclosure was also the message that the same click constituted acceptance of the Service Agreement.”

Thus, TransUnion “undid whatever notice” might have been furnished by the bold text when it stated in that text that clicking on the button merely constituted assent for TransUnion to obtain personal information.

The court helpfully included in its opinion examples that would likely bind users to an agreement, such as “placing the agreement, or a scroll box containing the agreement, or a clearly labeled hyperlink to the agreement, next to an ‘I Accept’ button that unambiguously pertains to that agreement.”

III. CONCLUDING OBSERVATIONS

These recent cases indicate that, following the recent trend established by Berkson v. Gogo and Nguyen v. Barnes & Noble, courts are more carefully analyzing the presentation of contract terms in the online environment. As these cases demonstrate, courts are willing to engage in a detailed factual analysis that more accurately reflects the user’s experience with online contracts to determine whether terms were reasonably communicated to the user. Accordingly, text font size, website design and color, presentation, hyperlink labeling, and the user experience (including a clear prompt to the terms) will all be relevant in determining whether there was conspicuous notice.

These courts seem to be acknowledging the differences in consumer perception of online and paper contracts. As the court in Dillon v. BMO Harris Bank,
N.A. stated: “While it is black letter law that consumers are bound by the fine print whether they read it or not, it is equally obvious that online sellers cannot insert terms and conditions the consumer did not have an opportunity to review.”67 The Seventh Circuit noted in Sgouros v. TransUnion Corp. that the online contracting environment is not the same as the offline one:

[W]e cannot presume that a person who clicks on a box that appears on a computer screen has notice of all contents not only of that page but of other content that requires further action (scrolling, following a link, etc.). Indeed, a person using the Internet may not realize that she is agreeing to a contract at all, whereas a reasonable person signing a physical contract will rarely be unaware of that fact.68

Accordingly, businesses should do more than provide notice of the existence of a contract if they want to increase the likelihood that specific terms will be enforced. These cases reveal a subtle shift away from the notion of blanket assent and indicate that conspicuous notice may require notice of specific terms.

68. Sgouros, 817 F.3d at 1035.
Developments in the Law Affecting Electronic Payments and Financial Services

By Stephen T. Middlebrook,* Tom Kierner,** and Sarah Jane Hughes***

I. INTRODUCTION

Developments affecting e-payments and financial services were as varied as ever during the past year. The subjects we chose for this survey focus on emerging issues in e-payments and federal and state regulation of e-payments and e-payment providers.

II. PREPAID CARDS—FDIC GUIDANCE ON BROKERED DEPOSITS, INTER-AGENCY CIP GUIDANCE, AND MORE

Since last year’s survey, there have been several developments in the prepaid area. Multiple agencies have provided guidance and issued frequently asked questions (“FAQs”) that have provided answers and, in some instances, more uncertainty.

A. FDIC ISSUES FAQS ON BROKERED DEPOSITS

The Federal Deposit Insurance Corporation (“FDIC”) issued guidance that brings prepaid debit cards within the scope of rules governing brokered deposits, placing new restrictions and requirements on issuers of the popular financial product.

---

* General Counsel of UniRush, LLC, a prepaid card provider. Prior to joining UniRush, he was General Counsel of FSV Payment Systems, Inc. and Senior Counsel at the U.S. Department of the Treasury, Financial Management Service. He is the ABA’s Advisor to the Uniform Law Commission’s Drafting Committee on the Regulation of Virtual Currency Businesses Act. He is co-chair of the Electronic Payments and Financial Services Subcommittee of the ABA Business Law Section’s Cyberspace Law Committee. He can be reached at stm@aol.com.

** Assistant Counsel at UniRush, LLC. He can be reached at tom.kierner@rushcard.com.

*** University Scholar and Fellow in Commercial Law at the Maurer School of Law, Indiana University-Bloomington. She currently serves as the Reporter for the Uniform Law Commission’s Regulation of Virtual Currency Businesses Act Drafting Committee. She can be reached at sjhughes@indiana.edu, and her SSRN number is 408848.

The views expressed in this survey are our own, as are all remaining errors.

The authors thank Michelle Marie Botek Trumbo and Ralph Gaebler of the Jerome H. Hall Law Library, Maurer School of Law, Indiana University, and Robert R. Britt of the Marion Gould Gallagher Law Library, School of Law, University of Washington, for their assistance with this survey.
In November 2015, the FDIC issued a set of FAQs that updates prior FAQs issued in January 2015 and responds to questions that continue to arise throughout the financial industry. In what may be seen as broadening the definition of a brokered deposit, the FDIC explicated many common scenarios that have caused confusion within the financial industry. Embracing a fact-intensive approach in determining whether a deposit is brokered, the FDIC clarified that when a third party informally refers a depositor to a financial institution, that deposit is generally not considered brokered. However, deposits that are referred through a more formal, programmatic arrangement would generally be considered brokered.

The FDIC also clarified certain exceptions to the definition of a deposit broker. Notably, companies that sell or distribute general purpose prepaid cards do not qualify for the primary purpose exception and, therefore, are deposit brokers because of the inseparable nature of the funds in the underlying deposit account and the prepaid card.

Classifying prepaid cards as brokered deposits may be problematic for some issuers because section 29 of the Federal Deposit Insurance Act restricts depository institutions that are not well capitalized from accepting brokered deposits. If a prepaid issuer ceases to be well capitalized, it must establish an FDIC-approved supervisory plan for section 29 compliance.

B. AGENCIES PROVIDE GUIDANCE ON CIP REQUIREMENTS FOR BANKS THAT ISSUE PREPAID CARDS

In March 2016, several agencies published guidance to banks that issue prepaid cards on the banks’ customer identification program (“CIP”) obligations as set forth in section 326 of the USA PATRIOT Act. This guidance clarified that issuing banks should determine whether the issuance of the prepaid card results in the creation of an account; if so, the bank must ascertain the identity of its customers.

If a cardholder has “(1) the ability to reload funds or (2) access to credit or overdraft features,” the card should be treated as an account. If the prepaid

---

4. Brokered Deposit FAQ, supra note 1, at 11–12.
6. Brokered Deposit FAQ, supra note 1, at 15.
7. The federal agencies include the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Financial Crimes Enforcement Network (FinCEN).
10. CIP Guidance, supra note 8, at 4.
card cannot be reloaded by the cardholder and does not provide access to credit or overdraft features, the card should not be treated as an account.\textsuperscript{11} For cards issued with these features not yet enabled but which are capable of being activated later by the cardholder, an account is only created once one of those features is activated.\textsuperscript{12}

The agencies provide further guidance on a bank’s CIP requirement in several contexts, including payroll cards, government benefit cards, and health benefit cards. Generally, they apply the proposition that whoever has access to the features that trigger an account classification is the customer for CIP purposes. For example, in the context of payroll cards, if the employer is the only party able to deposit funds to the card account, the employer should be considered the bank’s customer.\textsuperscript{13}

Finally, the agencies advise issuing banks that their contracts with third-party program managers should, at a minimum, (1) include an outline of CIP obligations, (2) preserve the issuing bank’s right to access all CIP information, (3) provide for the bank’s right to audit and monitor the program manager’s performance, and (4) indicate that relevant regulatory bodies have the right to examine the third-party manager.\textsuperscript{14}

\section*{C. FinCEN Issues FAQs for Sellers of Prepaid Cards}

The Financial Crimes Enforcement Network (“FinCEN”) issued supplemental guidance\textsuperscript{15} on regulatory expectations for nonbank sellers of prepaid cards by addressing some FAQs. The new FinCEN guidance focused primarily on five issues. First, it addressed an open issue related to state laws that require the refunding of de minimis card balances in cash to an individual holding a closed-loop card. For ease of administration, FinCEN clarified that a retailer operating in several states may set as its standard the highest level as required among the various states in which it does business without losing the benefit of the closed-loop prepaid access exclusion.\textsuperscript{16}

Second, FinCEN addressed industry concerns by confirming that prepaid credit accessed by quick response codes or a similar technology at multiple merchants would qualify for certain closed-loop exceptions to the Prepaid Access Rule.\textsuperscript{17}

Third, FinCEN clarified that “defined merchant” is not limited to a single merchant. So long as “the universe of merchants is identifiable and articulated to the purchasing public, and the partner merchants are joined for the limited purpose

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Id. at 4–5.
\item Id. at 6.
\item Id. at 7.
\item Id. at 1.
\item Id. at 2–3.
\end{enumerate}
\end{footnotesize}
of providing a closed-loop prepaid access program, such an arrangement falls within the term ‘defined merchant.”18

Fourth, under the existing FinCEN regulations, a person may avoid being classified as a “seller of prepaid access” by implementing policies and procedures reasonably adapted to prevent a sale of more than $10,000 to any person during a given day.19 FinCEN clarified that retailers that wish to take advantage of this exception must “(1) develop an internal policy regarding sales of prepaid access in excess of $10,000 to a single individual in a day; (2) articulate this policy to the appropriate personnel within the organization; and (3) monitor activity, through mechanisms appropriate to the retailer’s size and type of operating structure . . . .”20

Finally, FinCEN clarified that a provider of prepaid access is required to list a seller of its products on its MSB agent list only if the seller meets the definition of a “seller of prepaid access.”21

III. LOCAL PRESSURES ON PAYMENT PROCESSORS: BACKPAGE Fought THE LAW AND BACKPAGE (SORT OF) WOn

In 2015, several years after losing22 a legal battle with craigslist,23 Thomas Dart, the sheriff of Cook County, Illinois, sought to disrupt another online forum—Backpage.24 Backpage hosts classified advertising from third-party users and includes a popular adult section that is subdivided into categories, including “escorts, body rubs, strippers and strip clubs, dom[ination] and fetish, ts (transsexual escorts), male escorts,”25 and so on.

After his suit against craigslist failed in 2009, Dart adopted a new strategy. Instead of litigating against Backpage, he coerced Visa and MasterCard to cease processing payments made by purchasers of Backpage advertisements, thereby cutting off the company’s principal revenue stream. Backpage filed an action and moved for a preliminary injunction against Dart, arguing that Dart’s actions constituted unconstitutional prior restraint on speech. The district court denied the preliminary injunction, and Backpage appealed to the Seventh Circuit. In a colorful opinion penned by Judge Posner, the Seventh Circuit reversed the district court opinion and ordered the district court to issue an injunction protecting Backpage.26

---

18. Id. at 3–4 (quoting 31 C.F.R. § 1010.100(kkk)).
21. Id. at 5 (citing 31 C.F.R. § 1010.100(ff)(7)).
26. Id. at 239.
The Seventh Circuit explained that had Dart been acting as a private citizen, he would have been within his rights, but it found that Dart had in fact acted as a government official. Judge Posner highlighted several factors supporting his conclusion, including the fact that Dart’s letter to Visa and MasterCard “is on stationery captioned ‘Office of the Sheriff,’ and begins: ‘As the Sheriff of Cook County.’” Further, Dart’s use of legal terminology and citations of specific legal obligations made Dart’s contention that he was acting as a private individual easy to dismiss.

Dart filed a Petition for Writ of Certiorari, arguing that his actions constituted permissible advocacy and are protected by the First Amendment. In October 2016, the U.S. Supreme Court denied the petition.

IV. DEVELOPMENTS RELATING TO VIRTUAL CURRENCIES

A. JAPAN’S GOVERNMENT DECIDES TO REGULATE VIRTUAL CURRENCIES

In May 2016, Japan’s Ministry of Internal Affairs and Communications issued a cabinet order that will result in an amendment to the Business Telecommunications Law requiring virtual currency exchanges to register with the Financial Supervisory Agency.

B. MORE CRIMINAL PROSECUTIONS OF BITCOIN USERS UNDER 18 U.S.C. § 1960

In last year’s survey, we discussed the prosecutions of bitcoin users Faiella, Shrem, Powell, Reid, and Espinoza for operating as unlicensed money transmitters in violation of 18 U.S.C. § 1960. Based on the number of such prosecutions, we suggested that “criminal enforcement under this statute will play a significant role in the government’s response to bitcoin.” Our prediction has been validated by the initiation of several new section 1960 prosecutions in the last year.

In July 2015, federal officials filed a criminal complaint against Anthony Murgio for operating an unlicensed money transmitting business in violation of section 1960, as well as for conspiracy, money laundering, and failure to file a suspicious activity report (“SAR”). The complaint alleges Murgio and his co-conspirators operated the coin.mx online virtual currency exchange in violation of federal law and knowingly facilitated “ransomware” attacks, in which a
person is blocked from using a computer system until a sum of money, typically in bitcoin, is paid.35 Victims of ransomware approached coin.mx to obtain bitcoin to pay these ransoms. The exchange provided the virtual currency but failed to file a SAR as required by law.36 In addition, Murgio is accused of acquiring beneficial ownership of a small credit union in New Jersey and using the institution to facilitate access to electronic payment networks in order to further his other illegal activities.37

In September 2015, Pascal Reid pled guilty to a single count of operating an unlicensed money transmitter and will serve ninety days in jail and five years of probation.38 In addition, he is required to conduct twenty trainings on virtual currency and cybercrime for law enforcement.39

In November 2015, federal officials charged Randall Bryan Lord and his son, Michael Aaron Lord, with several crimes, including operating an unlicensed money transmitting business in violation of section 1960.40 The two men allegedly took dollars in exchange for bitcoin, connecting with many of their customers on the localbitcoins.com website.41 The defendants pled guilty.42 In another case, Richard Petix was also indicted for violating section 1960.43 Petix is alleged to have made thirty-seven bitcoin transfers worth approximately $13,000 to an undercover officer.44 The fact that section 1960 continues to be law enforcement’s default tool is problematic because the statute is being interpreted so broadly that it imperils virtual currency activity that does not involve criminal activity.45

C. BANKRUPTCY COURT AVOIDS DECIDING WHETHER BITCOIN IS PROPERTY OR CURRENCY

A bankruptcy proceeding in California garnered significant attention in the virtual currency world when commentators thought the court was going to
rule on the question of whether bitcoin is property or currency.\textsuperscript{46} HashFast Technologies LLC, which was a manufacturer of specialized computers used to mine bitcoin, pre-sold equipment that it failed to deliver, resulting in allegations of fraud and attendant litigation.\textsuperscript{47} The company filed a Chapter 11 bankruptcy proceeding, and in early 2016, the trustee asked the court to avoid and recover 3,000 bitcoin that had been paid to an individual doing marketing for HashFast.\textsuperscript{48} At the time the bitcoin were paid out, they were worth $363,861, but because the value of bitcoin had increased, they were worth $1.3 million at the time of the motion’s filing. The trustee asked the court to treat the bitcoin as property, which would mean that the estate could recover the bitcoin at the higher current value.\textsuperscript{49} In the end, the judge concluded that he did not have to decide whether, for purposes of the bankruptcy rules on avoiding transactions, bitcoin is a currency or a commodity, putting that question off until the trustee prevails in setting aside the transactions at issue.\textsuperscript{50} We are confident that this question will be addressed by this and other courts in the future.

V. FEDERAL AND STATE LAWS AFFECTING PAYMENTS PROCESSORS—A WILD YEAR FOR “DAILY FANTASY SPORTS” OPERATORS AND PAYMENTS ProcessORS

Beginning in October 2015, there were reports that the U.S. Department of Justice and Federal Bureau of Investigation had launched investigations of daily fantasy sports (“DFS”) operators\textsuperscript{51} over possible violations of the Unlawful Internet Gambling Enforcement Act of 2006 (“ UIGEA”).\textsuperscript{52} These reports trig-


\textsuperscript{48} Memorandum of Points and Authorities in Support of Motion for Partial Summary Judgment at 1, Kasolas v. Lowe (In re HashFast Techs. LLC), No. 14-bk-30725-DM (Bankr. N.D. Cal. Jan. 22, 2016) (on file with The Business Lawyer). HashFast Technologies LLC is affiliated with HashFast LLC and their bankruptcy proceedings were consolidated. See id.

\textsuperscript{49} Id.


\textsuperscript{51} See Matthew Futterman & Sharon Terlap, The Deals that Made Daily Fantasy Sports Take Off, WALL ST. J. (Oct. 17, 2015, 8:55 PM EST), http://www.wsj.com/articles/the-deals-that-made-daily-fantasy-take-off-1445043328 (reporting on large investments made in both major DFS websites, DOJ and FBI investigations, and the order from the State of Nevada for both operators to halt gambling for Nevada residents).

\textsuperscript{52} 31 U.S.C. §§ 5361–5367 (2012); see Kenneth N. Caldwell, The Shifting Tide in Internet Gambling—Survey of Recent Developments, 69 BUS. L AW. 291, 292–93 (2013) (discussing the U.S. Department of Justice’s 2011 opinion on uses of interstate processors to sell lottery tickets to in-state adults and the federal Wire Act). UIGEA is implemented by Regulation GG, which was jointly promulgated by the Federal Reserve Board and the Department of Treasury. 12 C.F.R. §§ 233.1–233.7 (2016) (identifying payment systems and financial transaction providers that are required to identify and block or otherwise prevent payments transactions that UIGEA governs); see Compliance Guide to Small Entities—Regulation GG: Prohibition
gered a long spell of focus on the legality of DFS payments processing under the UIGEA. The UIGEA prohibits persons in the business of betting or wagering from knowingly accepting payments in connection with persons participating in “unlawful Internet gambling.” Under the UIGEA, the term “unlawful Internet gambling” includes bets or wagers that (a) involve “the use, at least in part, of the Internet” and (b) are “unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made.” The UIGEA provides an exemption from the definition of the terms “bet or wager” for games of “knowledge and skill,” as opposed to games of chance, so long as other conditions are met.

Pressure on DFS operators and their payments processors intensified first when Nevada’s Gaming Control Board issued cease-and-desist orders against two large operators, DraftKings, Inc. and FanDuel, Inc., and then when New York’s Attorney General issued cease-and-desist orders against both operators, commencing actions for injunctions and other relief in November 2015. If bets are not lawful where initiated, as regulators in Nevada and New York concluded, then the UIGEA prohibits operators from taking the associated payments. What transpired from then to mid-June 2016 could be described as a whirlwind of developments affecting DFS operators and, consequently, banks and other payment processors that handle the funds flowing to and from DFS operators. They ranged from attorney general opinions that declare DFS to be illegal gambling in some states to efforts to legalize DFS through

---


32. Id. § 5362(10)(A).
33. Id. § 5362(1)(E)(ix)(II).
state legislation.59 Among the states to legalize DFS are Indiana60 and Virginia.61 Two additional state legislatures legalized DFS gaming in June 2016. On June 10, 2016, the governor of the State of Colorado signed legislation that legalized and provided for the regulation of DFS.62 And in August 2016, the governor of New York signed legislation to regulate “interactive fantasy sports” and require operators to obtain licenses from the state.63 Each licensee will pay a share of its gross revenues in New York, which could total as much as 15.5 percent.64 This legislation effectively will resolve the unlawful gambling charges against DraftKings and FanDuel65 that prompted the original cease-and-desist orders issued in late 2015.66 The attorney general’s charges against both operators for making false advertising claims were not resolved in the agreements or legislation.67

The legislation and prior settlements mean that DFS can restart in New York and payments processors can handle these operators so long as they are licensed entities without fear of violating the UIGEA.

VI. POTENTIAL PERSONAL LIABILITY FOR CHIEF COMPLIANCE OFFICERS (AND POTENTIALLY OTHER EMPLOYEES) FOR COMPANY COMPLIANCE FAILURES

In January 2016, the federal district court in Minnesota held that compliance officers and other individuals can be held personally liable for their employer’s


64. Id. § 1407 (imposing a base tax of 15 percent of gross revenues generated in the state and an additional tax equal to 1/2 of 1 percent, not to exceed $50,000 annually).


failure to properly implement anti-money laundering ("AML") safeguards. The case comes out of the Treasury Department's enforcement actions against MoneyGram International Inc., which separately admitted that it had willfully violated the Bank Secrecy Act by not implementing an effective AML program and subsequently forfeited $100 million. The government also assessed a $1 million civil penalty against MoneyGram's chief compliance officer, alleging he had failed to implement and maintain an effective AML program and also failed to ensure that SARs were filed appropriately. The court upheld the action against the chief compliance officer under the Treasury Department's broad enforcement authority found in 31 U.S.C. § 5321(a)(1), which extends to "a partner, director, officer, or employee of a domestic financial institution." Although, in this case, prosecution of an individual was tied to a specific statutory authorization, the general focus on individual responsibility is in keeping with the U.S. Department of Justice's so-called "Yates memo," which detailed the government's intent to step up the investigation and prosecution of individuals for corporate wrongdoing. Given the additional scrutiny being placed on individual employees, it is likely that the parameters of corporate compliance programs, as well as the compensation and protections for compliance officers who manage them, will be subject to significant review and revision over the next year.

VII. Conclusion

In last year's survey, we identified numerous aspects of electronic payments and financial services that we urged readers to follow. For the coming year, we urge readers to pay attention to pending rulemakings and new enforcement actions at the Consumer Financial Protection Bureau as well as to reactions in the financial services world to the U.S. Supreme Court's denial of certiorari in Madden v. Midland Funding, LLC; probable additional developments related to the UIGEA, DFS gaming, and other Internet gambling and online gaming payment providers; and likely developments in the regulation of virtual currencies.

70. Id.
71. Id. at 2 (quoting 31 U.S.C. § 5321(a)(1)).
73. Hughes & Middlebrook, supra note 32, at 372.
74. 136 S. Ct. 2505 (2016) (mem.).
Copyrights in Cyberspace: Fair Use, Takedown Notices, and the Sixth Triennial Section 1201 Rulemaking

By Jonathan T. Rubens*

I. INTRODUCTION

In last year’s survey, we considered the resolution of some novel copyright claims in Garcia v. Google, Inc., looked at the resolution of certain fair use defenses involving one of Google’s digitization projects in Authors Guild, Inc. v. HathiTrust, and considered several cases involving the Digital Millennium Copyright Act (“DMCA”) safe harbors, addressing whether a defendant is truly a “service provider” in Gardner v. CafePress Inc. and whether the defendant exerted sufficient “right and ability to control” the users of a service it provides in that case and in Mavrix Photographs LLC v. LiveJournal, Inc.

In this year’s survey, we continue to explore the copyright doctrine of fair use in disputes involving digital media and software development. First, we revisit the complaints against the Google Books project, with a look at the Second Circuit’s decision affirming Google’s fair use defense in Authors Guild v. Google, Inc. This latest Google Books opinion is instructive for its further analysis of fair use factors, with particular focus on what makes a use “transformative” and whether full-scale copying by a commercial enterprise can still be fair use.

Meanwhile, an opinion from the Eleventh Circuit, Katz v. Google, Inc., focuses more on the second fair use factor and reminds us that republication of copyrighted material that has already been published online for a critical or satirical purpose can weigh heavily in favor of fair use. We also consider an order of the U.S. District Court for the Northern District of California denying motions for

* Jonathan Rubens is a former chair of the Cyberspace Law Committee and is cofounder of Javid | Rubens LLP in San Francisco. He began his career litigating copyright infringement cases for media companies and writers, and his practice now includes commercial transactions, emerging companies, business acquisitions, and intellectual property.

2. 766 F.3d 929 (9th Cir. 2014), rev’d en banc, 786 F.3d 733 (9th Cir. 2015).
3. 755 F.3d 87 (2d Cir. 2014).
6. 804 F.3d 202 (2d Cir. 2015).
7. 802 F.3d 1178 (11th Cir. 2015).
judgment notwithstanding a jury verdict in favor of Google,⁸ the latest installment in the long saga of Oracle’s copyright infringement claims against Google over development of the Android platform based on the Java programming language, and the finding that Google’s use of the Java APIs was fair use.

Rounding out our assortment of fair use cases, we look at the famous, now almost ten years old, “dancing baby” lawsuit against YouTube, Lenz v. Universal Music Corp.⁹ dealing with a video of a toddler dancing while a Prince song played in the background and how Universal Music was required to consider whether the use was a fair use before sending a takedown notice under the DMCA.

Finally, we conclude with a look at the sixth triennial Section 1201 rulemaking,¹⁰ under which the Library of Congress, on recommendations from the Register of Copyrights, issued its list of works that are exempt from the DMCA’s prohibition on circumvention of measures designed to restrict access to copyrighted works. This latest iteration of the exemptions addresses uses of copyrighted software embedded in the rapidly expanding world of consumer products, but the exemptions are notable as much for items that were not included in the list as for an ever-larger set of exempt categories.

II. GOOGLE’S SCANNING OF ENTIRE BOOKS, AGAIN

In the last year, Google was successful in several high-profile cases confirming that its wide-ranging technology development and digitization efforts are shielded from copyright infringement claims. The Google Books project saga finally seems to have reached a stopping place with the decision of the Second Circuit in Authors Guild v. Google, Inc.¹¹

This decision comes after a long and complicated series of cases. In 2005, the plaintiffs, authors of published books, brought a class action against Google, alleging that Google’s unauthorized scanning of their books to make digital copies infringed on their copyrights. After several years of litigation, the parties negotiated a settlement, but the district court rejected it as not fair, adequate, and reasonable.¹² The plaintiffs then filed a new class action complaint, and after hearing disputes regarding class certification, the district court granted Google’s motion for summary judgment on the grounds of fair use.¹³

The Second Circuit’s opinion affirms that the fair use doctrine does indeed protect the massive Google Books project, in which, to recap, Google made digital copies of tens of millions of books that were submitted to it for that purpose by libraries. Google scanned the books and made the resulting digital texts pub-

---

⁹. 815 F.3d 1145 (9th Cir. 2016).
¹¹. 804 F.3d 202 (2d Cir. 2015).
licly searchable without fees for users to determine whether the books contain specified searched-for terms. The search function tells a user the number of times a searched-for term appears in a particular book, and it also displays for the user three “snippets” of text from the book (i.e., short segments of the book’s actual text), which usually constitute about one-eighth of a book page.

Google makes unavailable for its so-called “snippet view” one snippet from each page and one entire page out of every ten, which is called “blacklisting.” The participating libraries are allowed to download and retain digital copies of books they submit. The plaintiffs alleged copyright infringement, but the lower court found that Google’s actions constituted fair use.

In determining whether an allegedly infringing use of copyrighted material will constitute fair use under the Copyright Act, a court must consider the four fair use factors laid out in section 107 of the Copyright Act, namely,

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

The court examined each fair use factor in turn. Most instructive may be the court’s discussion of whether Google’s uses of authors’ works were “transformative,” a term that is used extensively in fair use opinions and considered part of the first fair use factor. Looking repeatedly to the Supreme Court’s decision in Campbell v. Acuff-Rose Music, Inc., the court explained that “transformative” for purposes of a fair use finding means a use that comments on or provides information about the original work rather than a use that “transforms” an original work into a different format, as in the case of a “derivative work.” In other words, a would-be fair use must have “justification for the taking,” such as that the fair user intends to comment on, or publish a parody of, the underlying work.

14. Authors Guild, 804 F.3d at 208–09.
15. Id. at 209.
16. Id. at 210.
17. Id.
18. The plaintiffs in this appeal included several individual authors. The Authors Guild had been found to lack standing to sue for copyright infringement on its members’ behalf in a separate case, see Authors Guild, Inc. v. HathiTrust, 755 F.3d 87, 94 (2d Cir. 2014), but the appeal in this case proceeded because the individual plaintiffs did have standing to assert infringement of their own copyrights. Authors Guild, 804 F.3d at 208 n.1.
19. Authors Guild, 804 F.3d at 211.
22. Authors Guild, 804 F.3d at 215–16 (citing Campbell, 510 U.S. at 580–81).
23. Id.
The court found that both the search function and the “snippet” view function easily constitute “transformative” uses of the original works and weigh toward fair use on the first factor, considering the purpose and character of the use.24 That Google is without doubt a commercial for-profit enterprise does not weigh against the fair use finding, and the court emphasized the Supreme Court’s rejection of the notion that commercial use cannot be fair use.25

In an analysis of the third fair use factor,26 “the amount and substantiality of the portion used in relation to the copyrighted work as a whole,” others might still find problematic that Google’s digitization projects involve scanning entire books and making entire copies available for searching. However, the court found that entire-text copying did not negate fair use because full-text copying was required in order to enable a search, which was transformative under Campbell,27 and because Google does not make the entire text available for viewing. Instead, Google makes available only a limited amount of text (through its “snippet” views and its “blacklisting” functions), which does not “offer[] the marketplace a significantly competing substitute for the copyrighted work.”28

The fourth factor, “the effect of the use upon the potential market for or value of the copyrighted work,” seems to be more difficult for the court. The analysis is not only whether copying (the full scanning of the books) creates a likely substitute for the original work but also whether it “results in widespread revelation of sufficiently significant portions of the original as to make available a significantly competing substitute.”29 The court found that, as currently configured, Google’s snippet view does not create enough of a potential substitute to erode the value of the copyright owners’ works by diminishing sales.30 The court also conjectured that a snippet view is more likely to direct viewers to uncopyrightable segments of texts, such as historical facts that a researcher may be seeking, than to expression protected by copyright.31 For those reasons, the fourth factor was found satisfied, allowing the court to rule in favor of fair use and appearing to put the fair use question to bed once and for all, unless Google makes substantial changes to the scanning, searching, and view functions of these systems.
III. Online Satire Using Reproduction of “Factual” Rather than “Creative” Works

In an example of the ways courts sometimes seem to strain to fit the context of an alleged infringing use into fair use factors, the Eleventh Circuit affirmed an order granting summary judgment for the defense on the grounds of fair use, in Katz v. Google, Inc. The defendant’s multiple republication of photos of the plaintiff in blog posts seems familiar as critique or parody. The blog posts in question lambasted the actions of the defendant, a wealthy real estate developer and part owner of an NBA franchise, in connection with his business practices in managing real estate properties in which the blogger was a tenant. The photo in question was taken by a professional photographer and depicted the plaintiff in an unflattering pose, courtside, while cheering for a basketball team he was interested in acquiring. The blogger posted the picture in several blog posts, some accompanied by critical text and others in which the picture was pasted into mocking cartoons. Annoyed and allegedly embarrassed, the plaintiff purchased the rights to the photo from the photographer and then sued the blogger for copyright infringement.

Many readers know that angry litigants who seek to use legal means to stop bloggers and other Internet commentators from disseminating statements about them almost never achieve their aims. Here, the plaintiff may have been no more sympathetic a figure to the court than he would be to most readers, and the court seems to have made short shrift of the fair use factors, finding all of them to weigh in favor of fair use. The court noted first that the defendant’s use was noncommercial and was transformative because she used the photos of the plaintiff on her blog posts “to ridicule and satirize [the plaintiff’s] character.” The court reminds us that satire and critical commentary will very often be found to be fair use.

Interesting for our review of fair use analysis, and unlike the court in the Google Books opinion, this court found the second fair use factor, the nature of the copyrighted work, to be significant in the analysis. Noting that courts consider two sub-factors when assessing the nature of the work: “(1) whether the work was previously published and (2) whether the work is primarily creative or factual,” the court found it significant that the defendant republished a photo that was previously published online. And the nonliterary or noncreative nature of the original work, the photograph, is important to the court in finding fair use. The court noted that the photograph was a candid shot taken in a crowded basketball arena and that there was “no evidence in the record that [the photographer] attempted to convey ideas, emotions, or in any way influence Katz’s pose, ex-

---

32. 802 F.3d 1178 (11th Cir. 2015).
33. See, e.g., Guttenberg v. Emery, 26 F. Supp. 3d 88, 95 (D.D.C. 2014) (citing Bill Mordan, The Streisand Effect, which described how efforts to remove, hide, censor, or suppress certain information online, such as the location of a home, often backfire and have the unintended consequence of making that information more widely available).
34. Katz, 802 F.3d at 1183.
35. Id.
36. Id.
pression, or clothing.” This may raise questions for some, however, as to whether it truly will be evident whether the nature of any photograph will be primarily “creative or factual.” Surely many editorial photographs have elements that make them equally “creative” and “factual.”

The court briefly noted that the third factor, the amount of the original work used, will not usually be important in the case of a photograph (because the entire photograph is almost always used), and this factor did not weigh on either side of the fair use analysis. The fourth factor, the effect of the use on the potential market for the original work, weighed in favor of fair use because there was not any potential market for the original photograph—as the litigant bought rights in it solely for the purpose of bringing this lawsuit. In the end, the online satirical critique wins, and an unsympathetic aggressive plaintiff loses.

**IV. SOFTWARE DEVELOPMENT: THE JAVA APIs, AGAIN**

In one of the most-watched cases dealing with software development and a defense based on fair use, a second trial concluded in the long-running dispute between Oracle Corporation and Google over Google’s development of the Android system based on the Java software that Oracle had long ago acquired from Sun Microsystems. The jury found in favor of Google on its theory of fair use. As it did following the first trial, Oracle moved for judgment as a matter of law, despite the jury verdict against it, on the theory that no reasonable jury could have found fair use. The court denied the Rule 50 motion and issued an order holding that under the jury instructions, the jury “could reasonably have found for either side on the fair use issue.”

The court then provided a lengthy analysis of the fair use instructions, including some detailed discussion of what portions of the Java APIs were copied and how the APIs were used to create the Android platform. Among the most significant points from this decision may be the judge’s comments regarding an issue that remains unresolved: whether the “propriety” of a defendant’s conduct (i.e., the extent to which the defendant acted in bad faith in using the plaintiff’s copyrighted work) should be a determining factor in fair use analysis. The court pointed out that, following the Supreme Court decision in *Campbell*, it is not clear whether “propriety” should remain a part of fair use analysis. Oracle argued that Google’s alleged bad faith in proceeding to develop Android after its negotiations with Oracle had broken down is an important factor that should be considered in finding that its use was not fair use. We may need to wait for the appeal of this second jury verdict to the Ninth Circuit, or a subsequent case, to find out more about good faith as a fair use factor.

---

37. *Id.* (emphasis added).
38. *Id.* at 1184.
39. *Id.*
41. *Id.* at 3.
V. DMCA TAKEDOWNS AND GOOD FAITH: THE OBLIGATION TO CONSIDER FAIR USE

Fair use analysis may not always be clear, but are copyright holders required to undertake some degree of fair use analysis before seeking removal of allegedly infringing content from a website? The DMCA takedown rules do not specifically mention or require any fair use review, but in the closely watched case of the dancing baby video, Lenz v. Universal Music Corp., the Ninth Circuit held that the DMCA “requires copyright holders to consider fair use before sending a takedown notification” and that in this case there was a triable issue as to whether the copyright holder formed a subjective good faith belief that the use was not authorized by law.43

The dispute involved a video that Lenz posted to YouTube featuring her two young children dancing in the family kitchen while the song “Let’s Go Crazy” by the artist Prince played in the background. Universal Music, the entity responsible for enforcing Prince’s copyrights, assigned staff to regularly scan YouTube for postings that made use of Prince songs and to determine whether those videos made “significant use of . . . the composition, specifically if the song was recognizable, was in a significant portion of the video or was the focus of the video.”44 After its staffer identified the video in question as containing a recognizable excerpt of the Prince song, Universal sent a takedown notice to YouTube that identified more than 200 videos, including this one, that Universal believed made unauthorized use of Prince songs. The notice included the statement required by section 512(c)(3): “We have a good faith belief that the above-described activity is not authorized by the copyright owner, its agent, or the law.”46 YouTube removed the video and notified Lenz by e-mail, and then Lenz sent a counter notification under section 512(g)(3).47 Universal protested to YouTube that Lenz had not obtained a license to use the song and that the counter notification was not explicitly made under penalty of perjury, as required under the DMCA. Lenz sent a second counter notification, and YouTube reinstated the video.48

Lenz filed suit, and the lower court dismissed some of her initial claims, leaving a single claim, under section 512(f), that Universal knowingly and materially misrepresented that the video infringed its copyrights.49 The district court denied cross motions for summary judgment of the section 512(f) claim, and the Ninth Circuit accepted an interlocutory appeal.50

42. 815 F.3d 1145 (9th Cir. 2016).
43. Id. at 1148.
44. Id. at 1149.
46. Lenz, 815 F.3d at 1149.
47. Id. at 1150.
48. Id.
49. Id. Section 512(f) grants a copyright holder recourse for abuse of the DMCA takedown procedures by providing: “Any person who knowingly materially misrepresents under this section—(1) that material or activity is infringing . . . shall be liable for any damages . . . .” 17 U.S.C. § 512(f) (2012).
50. Lenz, 815 F.3d at 1150.
The central question was whether Universal was required, before sending its takedown notice, to consider whether the use of the Prince song in the video was a fair use. The language of the takedown rules in section 512(c) does not explicitly require a copyright holder to consider whether the use is a fair use. It requires that a takedown notice include a “statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.”51 The dispute centered on whether the term “authorized by . . . the law” would include fair use, which the court said was an issue of first impression.52

In what may become a frequently cited portion of the opinion, the court held that a fair use is “authorized by . . . the law” and is not merely an infringing use that is excused by the law.53 Accordingly, the court held that “a copyright holder must consider the existence of fair use before sending a takedown notification under § 512(c).”54 A copyright holder will satisfy its statutory obligation if, based on this consideration, it forms “a subjective good faith belief” that the use is unauthorized; it need not meet an objective standard of reasonable belief.55 At the same time, a user could in theory assert willful blindness by the copyright holder, thereby negating a showing of subjective good faith belief, but the plaintiff, Lenz, was unable to do that in this case.56 The court also rejected the defendant’s assertion that the plaintiff could not recover money damages under section 512(f) without a showing of actual monetary loss.57 Based on these rulings, the court affirmed the lower court’s order denying cross motions for summary judgment, remanding the case for a jury determination of whether Universal’s actions “were sufficient to form a subjective good faith belief about the video’s fair use or lack thereof.”58

In the end, this case will likely be cited for its strong assertion of fair use as authorized use and its statement that fair use must be considered before takedown notices are sent, even if the court adopted a low standard for demonstrating a subjective good faith belief that the use is not fair use.

VI. THE SIXTH TRIENNIAL SECTION 1201 RULEMAKING—EXEMPTIONS FROM THE ANTICIRCUMVENTION RULE

Section 1201(a)(1)(A) of the DMCA59 makes it illegal to circumvent a technological protection measure employed to restrict access to copyrighted material. But the law also instructs the Librarian of Congress to determine in a rulemaking

52. Lenz, 815 F.3d at 1151.
53. Id. ("Fair use is not just excused by the law, it is wholly authorized by the law.").
54. Id. at 1153.
55. Id. at 1153–54.
56. Id. at 1155–56.
57. Lenz could seek to recover “nominal” damages, but the court did not decide whether she could recover expenses or pro bono costs and attorney’s fees. Id. at 1156–57.
58. Id. at 1154.
procedure conducted every three years whether to adopt exemptions from this prohibition for certain categories of uses in order to prevent the prohibition from impinging on noninfringing uses of the material protected by the technological measure. The U.S. Copyright Office conducts the rulemaking proceeding, which consists of public hearings and submission of written comments from interested parties, and makes a recommendation to the Librarian of Congress. The first such rulemaking was held in 2000 and the sixth and most recent rulemaking was completed in 2015.

This sixth rulemaking stands out for the extensive reach of the proposed exemptions and, in the words of the National Telecommunications and Information Administration, for its “extensive discussion of matters with no or at best a very tenuous nexus to copyright protection.”

This time around the list of exemptions includes twenty-two categories of items. Several of the exemptions are, as in previous rulemakings, intended to allow users to circumvent the technological protection measures used on DVDs, Blu-ray discs, and streaming entertainment services to limit copying so that users can engage in certain noninfringing uses such as remixes, criticisms, educational uses, noncommercial videos, documentary films, and e-books offering film analysis. An exemption was also continued for creating versions of texts for assisting handicapped users. Several of the exemptions continued previous exemptions for “unlocking” and “jailbreaking” smartphones, but to increase access, the exemptions were expanded from only smartphones to cover other portable mobile computing devices, including tablets, mobile hotspots, and smartwatches.

60. Id. § 1201(a)(1)(B) (calling for exemption from the prohibition for persons who are likely to be “adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works”).
63. See the summary of the first eight exempt uses, 2015 Final Rule, supra note 10, at 65946–50.
64. See the summary of the ninth exempt class, allowing circumvention of access controls to enable read-aloud functions or similar functionality to make literary and dramatic works accessible to blind and other disabled users, renewing a prior exemption, 2015 Final Rule, supra note 10, at 65950.
65. “Unlocking” a smartphone is the process of modifying the software controlling the device so that it is no longer tied exclusively to the mobile network of a specific mobile carrier but will work with other carriers’ networks.
66. “Jailbreaking” refers to the process of removing certain software restrictions a manufacturer or retailer includes in a mobile device, so that a user may have unrestricted access to all the software built into the device.
67. See the discussion of the exemptions for unlocking cell phones, tablets, “[p]ortable mobile connectivity devices, such as mobile hotspots, removable wireless broadband modems, and similar devices,” and wearable devices, 2015 Final Rule, supra note 10, at 65950–52 (continuing prior exemptions under earlier rulemakings as extended by the Unlocking Consumer Choice and Wireless Competition Act of 2014, Pub. L. No. 113-144, 128 Stat. 1751 (2014), and expanding the exemptions to include the categories of devices in addition to cell phones); and the discussion of the exemption for jailbreaking “smartphones and portable all-purpose mobile computing devices,” 2015 Final Rule, supra
It was also recognized that broader exemptions were needed to allow access to the copyrighted computer code that can now be found embedded in many consumer devices. A new exemption was issued to allow users to circumvent software restricting access to certain systems embedded in cars and other land vehicles in order to allow repair and modification of the vehicle.68 A new broad exemption was allowed for circumventing software on consumer devices, including land vehicles and medical devices, for purposes of security research,69 and another allows access to a person’s personal data that is generated by a medical device.70 The Librarian of Congress also allowed an exemption for circumventing access to certain kinds of video games in which access might be necessary to preserve or archive an old game for which there is no longer marketplace support.71

However, the exemptions were not extended to allow similar “jailbreaking” of video game consoles for other purposes or jailbreaking computer software that operates dedicated e-book readers such as the Amazon Kindle or hacking into audiovisual works (motion pictures, television programs) for purposes of “space shifting” or “format shifting,” because none of these uses, according to the Librarian of Congress, had been sufficiently established to be noninfringing uses.72

As might be expected, the exemptions that the librarian continued or adopted for the first time were not universally supported. There was substantial objection, among not only industry groups but also different government entities, to expanding the exemptions in several categories.73 With the increasingly long process in each of the triennial rulemakings, the substantial debate among different agencies about the merit of creating certain exemptions, and the increased debate over preserving the anticircumvention rule for certain uses and exempting it for others, an even more contentious rulemaking process is likely in the next triennial rulemaking as copyright protection covers more and more of the things we encounter in our daily lives.

note 10, at 65952–53. The exemption for unlocking applies only to a “used” device, meaning one that has been lawfully acquired and used on the network of a wireless carrier. Id. at 65952.

68. 37 C.F.R. § 201.40(b)(6) (2016).
69. Id. § 201.40(b)(7).
70. Id. § 201.40(b)(10).
71. Id. § 201.40(b)(8).
72. The Librarian of Congress accepted the Register of Copyrights’ recommendations and declined to grant these exemption. 2015 Final Rule, supra note 10, at 65960–61.
73. For example, the Copyright Office noted that the National Telecommunications and Information Administration favored broadening the exemptions to allow circumvention in order to promote security research or to enable modifications of motor vehicles, or to promote security testing on medical devices, but broadening exemptions for such purposes was opposed or questioned by the Environmental Protection Agency, the Department of Transportation, and the Food and Drug Administration. See 2015 Final Rule, supra note 10, at 65946; see also Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention; Recommendation of the Register of Copyrights 22–23 (Oct. 8, 2015), www.copyright.gov/1201/2015/registers-recommendation.pdf.
Online Intermediary Immunity Under Section 230

By Venkat Balasubramani*

I. INTRODUCTION

This survey discusses recent cases applying the intermediary liability provision of the Communications Decency Act ("CDA"), 47 U.S.C. § 230 ("Section 230"), which gives providers and users of "an interactive computer service" broad protection against liability for claims based on information “provided by another information content provider.”¹ In Zeran v. America Online, Inc., an early and influential interpretation of Section 230, the Fourth Circuit gave the provision an expansive scope,² and since Zeran, immunity for online service providers has largely remained broad.³ During the survey period, many courts have relied on Section 230 to dismiss cases seeking to hold intermediaries liable based on third-party content, the intermediaries’ editorial decisions, or interactions between the putative victim and the perpetrator that took place through the intermediaries’ website or network.⁴ However, some courts have taken a lenient view of plaintiffs’ burden for overcoming Section 230 immunity where the intermediary did not create the content in question, taking a narrow view of Section 230 protection. Plaintiffs have overcome Section 230 immunity by alleging that intermediaries had a role in developing third-party content,⁵ engaged in selective editing of the challenged material,⁶ or did not act as a neutral conduit.⁷ In other cases, plaintiffs have successfully advanced theories other than content-creation by the intermediary in order to circumvent Section 230 immunity, demonstrating that the provision’s protection is not airtight.⁸ Finally, the survey also discusses the

---

² Zeran v. Am. Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997) (“Congress enacted . . . broad immunity . . . .”)
⁴ See infra Part II.
⁵ See infra Part III.
⁶ See infra Part IV.
⁷ See infra Part V.
⁸ See infra Part VI.
efforts of intermediaries (often relying on a combination of Section 230 and the First Amendment) to push back against the investigative efforts of regulators. 9

II. MANY CASES HAVE CONTINUED TO APPLY SECTION 230 BROADLY

Recent cases have included a number of clear defense wins for online service providers. In these cases, courts have adhered to long-standing precedent and held that Section 230 continues to bar a wide range of claims against intermediaries for hosting harmful information.

In GiveForward, Inc. v. Hodges, the court granted summary judgment to the defendant—fundraising website GiveForward—on the issue of Section 230 immunity. 10 GiveForward allows individual parties to post and fundraise for “family members or friends in need.” 11 A third-party defendant, Kimani Johnson, allegedly posted a fraudulent fundraiser on GiveForward, asserting that his minor son KDH, an eight year old, had a possibly terminal heart condition and needed money for surgery. 12 GiveForward had an alert system in place for possible fraudulent fundraisers, which was triggered three times during the fundraiser, and it had also been alerted by KDH’s mother, Kena Hodges, that the fundraiser was a fraud. 13 Hodges brought suit against GiveForward, arguing that GiveForward was liable for the fraudulent fundraiser as it had created additional “content” through “a tweet, widgets, and thank you emails sent to donors.” 14

A finding of Section 230 immunity involves a three-prong test, requiring that “1) the party seeking immunity is an interactive computer service, 2) the claim is based on information provided by another information content provider, and 3) the claim treats the party as the publisher or speaker of that information.” 15 Hodges attempted to circumvent this immunity by claiming that GiveForward could still be held liable for “independent actions it took distinct from the fraudulent text,” 16 i.e., based on the tweet, widgets, and thank you emails sent by GiveForward. 17 The court rejected this argument, stating that “the tweet would not have existed but for the content posted by [the] third-party information content providers” and noting that the tweet “simply thanked a twitter user for sharing the story of KDH,” which “did not add additional information, or make any unique or independent statements.” 18

A similarly straightforward case is Sikhs for Justice “SFJ,” Inc. v. Facebook, Inc., 19 holding that the plaintiff’s civil rights claim against Facebook for removal of

9. See infra Part VII.
11. Id. at *1.
12. Id.
13. Id.
14. Id. at *9.
15. Id. at *3 (internal quotations omitted).
16. Id. at *7.
17. Id. at *9.
18. Id.
19. 144 F. Supp. 3d 1088 (N.D. Cal. 2015).
plaintiff’s Facebook page was barred by Section 230. The plaintiff sought to hold Facebook liable for deciding not to publish its content, but the court found that “removing content is something publishers do, and to impose liability . . . necessarily involves treating the liable party as a publisher,” therefore necessitating immunity against liability under Section 230 as a publisher of third-party content.20

Jane Doe No. 1 v. Backpage.com, LLC,21 involving advertisements posted by sex traffickers on the defendant’s website for the purposes of trafficking the victimized plaintiffs, also took a robust view of Section 230. Despite the tragic facts, the First Circuit held that Section 230 barred the victims’ claims under federal and state anti-sex trafficking statutes.22 The court reached this conclusion even though the plaintiffs alleged Backpage “deliberately structured its website to facilitate sex trafficking”23 and also made changes to the advertisements through actions, such as “stripping . . . metadata from photographs uploaded to the website.”24 The plaintiffs argued that Backpage’s actions in operating its website went beyond “traditional publishing or editorial functions” for purposes of Section 230 because Backpage established posting standards for advertisements, such as deciding what are permissible terms in a posting, offering anonymization of e-mail addresses, and accepting anonymous payments.25 However, the court rejected this argument, looking to Universal Communication Systems, Inc. v. Lycos, Inc., in which the court held that, if “the cause of action is one that would treat the service provider as the publisher of a particular posting, immunity applies not only for the service provider’s decisions with respect to that posting, but also for its inherent decisions about how to treat postings generally.”26 Thus, seeking to hold Backpage liable for furthering illegal activity through its posting policies requires “treat[ing] the website as a publisher . . . of content provided by third parties” and is forbidden by Section 230.27

In Roca Labs, Inc. v. Consumer Opinion Corp.,28 plaintiffs brought multiple claims against the operator of a website that allows consumers to post complaints against companies with which they had dealt. The court rejected the argument that Consumer Opinion could be held liable as an information content provider “because companies can pay to have testimonials placed on [the defendant’s website].”29 The court also held that trimming the length of a third-party posting so that it fits within a tweet, adding handles and links, and then tweeting the resulting message does not turn the website operator into an “information content provider” and therefore does not result in the loss of Section 230 protec-
tion. However, notably, despite granting Consumer Opinion’s motion for summary judgment, the court denied its request for fees. The court found that, although Consumer Opinion was entitled to immunity under Section 230, Roca Labs’ maintenance of the lawsuit did not constitute bad faith and was not unreasonable. The court also noted that a finding of bad faith, for purposes of awarding fees, “requires something more than lack of merit.”

Courts have repeatedly held that the egregiousness of the alleged harm does not undermine Section 230 protection. The First Circuit’s Backpage ruling, discussed above, is one example. Witkoff v. Topix, LLC is another. In that case, the plaintiff’s son used the defendant’s website, which hosted a forum for discussion of Oxycodone, a controlled substance, to contact a third-party user for purposes of illegally obtaining the drug, and he subsequently died of an Oxycodone overdose. The plaintiff argued that Topix, by creating a public Oxycodone forum, was an information content provider and thus subject to liability. The California Court of Appeal disagreed, finding that Topix did not provide “the content of any thread, other than having provided a forum,” and that “the criminal conduct was the result of user-input.”

Caraccioli v. Facebook, Inc. was another straightforward dismissal on Section 230 grounds. In Caraccioli, the plaintiff sought to hold Facebook liable for a Facebook account that featured sexual photos and videos of the plaintiff. The plaintiff attempted to distinguish his case from the precedent in Facebook’s favor by arguing that Facebook could have easily deleted the offensive content. However, the plaintiff did not allege that Facebook “actually created, developed or posted the content on the suspect account,” allowing the court to easily dismiss the claim on Section 230 grounds.

In Roe v. Amazon.com, an erotic book published through Amazon’s Kindle digital publishing system used the plaintiffs’ engagement photo on the cover without their consent. The court found that Amazon was not a publisher, and that its digital publishing system instead would be treated as if it were [the] next logical step after the photocopier. Just as Xerox would not be considered a publisher and held responsible for an invasion of privacy tort carried out with a photocopier, [Amazon and the other defendants] will not be liable as publishers for the tort allegedly committed using their technology.
The court accordingly granted summary judgment for Amazon, without addressing the applicability of Section 230.

III. OTHER COURTS HAVE DECLINED TO DISMISS ON SECTION 230 GROUNDS, CREDITING PLAINTIFFS’ ALLEGATIONS REGARDING THE INTERMEDIARY’S CREATION OR DEVELOPMENT OF CONTENT

Some courts have adopted a lenient pleading standard to allow plaintiffs to overcome an intermediary's Section 230 immunity, despite the absence of specific allegations that the intermediary created or developed the content in question.

For example, AdvanFort Co. v. Maritime Executive, LLC involved an article published by the defendant on its website and in its newsletter that was alleged to contain defamatory comments. The court granted leave to allow the plaintiffs to amend to include allegations that the defendant materially contributed to the creation of the article after finding “a newly discovered copy of the Article . . . which” was published under the “BY MAREX” byline. Furthermore, the court showed additional leniency by contemplating the possibility that the newsletter was also distributed in print format, thus placing it outside the scope of Section 230 immunity. These two possibilities gave the court reason to believe that a combination of this new information would “support a reasonable inference that [the defendant] was at least partly responsible for the creation or development of the Article, rendering the CDA inapplicable.” While the court dismissed the claims, it nevertheless allowed plaintiff a second opportunity to make allegations that could overcome Section 230 immunity.

Similarly, the court in Congoo, LLC v. Revcontent LLC denied the defendant’s motion to dismiss on Section 230 grounds. In Congoo, the plaintiff merely alleged that the defendant published “false and misleading native advertising”; it nowhere alleged that the defendant had any part in creating that advertising, and explicitly characterized the defendant as an “intermediary,” suggesting that the defendant did not create the advertising in question and, thus, should be protected by Section 230. However, the court, construing the plaintiff's allegations in the light most favorable to the plaintiff, concluded that the plaintiff had pled sufficiently that the defendant was “responsible in part for the development of

43. No. 1:15-cv-220, 2015 WL 4603090, at *1–2 (E.D. Va. July 28, 2015). “Although not alleged in the Amended Complaint, it also seems plausible that [the] newsletter appears in print format. . . . [If] the Article . . . appears in print, the[n] it falls] outside the scope of CDA immunity under the plain language of the statute.” Id. at *11.
44. Id. at *11.
45. Id.
46. Id.
47. Id. at *12.
49. Id. at *1.
the subject advertisements.” Accordingly, the court declined to dismiss on the basis of Section 230 immunity.

IV. Plaintiffs May Avoid Section 230 by Alleging that Defendants Developed Content Through Selective Editing

Several cases demonstrate that courts may deny immunity under Section 230 to defendants who host third-party content where plaintiffs allege that the defendants developed the content in question by selectively editing it.

For example, the court in General Steel Domestic Sales, LLC v. Chumley declined to find immunity for the defendants and focused on the question of the meaning of “development of information” for purposes of finding liability. The plaintiff alleged that the defendants ran advertisements appearing on search engine results pages that “contain[ed] derogatory information about General Steel and contain[ed] links to a portion of the Armstrong Steel Corporation website [that] also contain[ed] derogatory information” consisting of references to legal actions that had been brought against General Steel. The court concluded that the defendants could not receive immunity, as they had developed information by selecting “certain summaries and quotations describing the referenced court proceedings, fail[ing] to accurately describe the proceedings as a whole, and post[ing] those quotations and summaries” on search engine results pages that contained links to the Armstrong Steel website, further described as “editorial choices” that could be viewed “as a choice to emphasize unflattering allegations made against General Steel.”

The court in Consumer Cellular, Inc. v. ConsumerAffairs.com denied the defendants’ special motion to strike on a defamation claim. Plaintiff Consumer Cellular, Inc. ("CCI") alleged that the defendants, which operated a consumer-complaint website, engaged in a scheme to extort payments from CCI in exchange for manipulating the treatment of consumer postings on the site so that CCI would receive a more favorable rating. The court denied the motion to strike because CCI alleged that the defendants “knowingly failed to include positive reviews in their calculation of [CCI’s] rating.” Thus, CCI adequately alleged a defamation claim based on the defendants’ “statements regarding the aggregate ‘overall satisfaction rating,’” which did not constitute statements of opinion that would normally not be actionable as defamation. Furthermore, because the plaintiff’s allegations were not focused on third-party statements hosted by the defendants,

53. Id. at *1.
54. Id. at *8.
56. Id. at *4.
57. Id. at *12.
58. Id. (quoting defendants’ website).
but instead on “the defendants’ own factual representation(s) regarding those third-party expressions of opinion,” Section 230 did not bar these claims.59

V. SOME COURTS RELY ON THE STRUCTURE OF A WEBSITE OR THE ALLEGATION THAT IT WAS NOT A NEUTRAL CONDUIT IN DENYING SECTION 230 IMMUNITY

Courts have declined to apply Section 230 immunity when they have observed that the structure of the website results in the intermediary’s development of the content or where the intermediaries did not act as neutral conduits.

The Washington Supreme Court allowed claims against Backpage to proceed in *J.S. v. Village Voice Media Holdings, L.L.C.*, where the plaintiffs alleged that the defendant had helped develop advertisements for buying and selling children for sexual services on its website.60 The court found that allegations—including that Backpage had “intentionally developed its website to require information that allows and encourages . . . illegal trade to occur through its website,” “developed content requirements that it knows will allow pimps and prostitutes to evade law enforcement,” and knew “that the foregoing content requirements are a fraud and a ruse that is aimed at helping pimps”—were enough to survive a motion to dismiss under Section 230.61 Thus, while Backpage did not create any particular item of offending content, the court found that it could nevertheless be held legally responsible. Justice McCloud issued a strong dissent, noting that the existence of posting requirements and guidelines should not transform a website into an “information content provider,” and, in any event, the complaint alleged that a third party, and not Backpage, had provided the content at issue.62

The court in *Vision Security, LLC v. Xcentric Ventures, LLC* allowed the case to proceed with discovery despite the defendant’s claim of immunity under Section 230.63 Xcentric Ventures operates the “Ripoff Report,” a consumer-complaint website that has been involved in numerous Section 230 cases. The court looked to Tenth Circuit precedent in *FTC v. Accusearch Inc.*, in which the court held that a service provider could be held liable, despite Section 230, if it functioned as “more than a neutral conduit for that content” and “specifically encourages development of what is offensive about the content.”64 The plaintiff maintained that the defendant operated as something other than a neutral publisher by alleging that its website allowed competitors and not just consumers to post comments, despite the website’s “By Consumers, for consumers” tag line.65 Furthermore, defendant’s webmaster stated that “under no circumstances will the Ripoff Report remove postings,” yet the defendant offered a corporate advocacy program on “How to make your search engine listings positive . . .

59. *Id.* at *13.
60. 359 P.3d 714, 715–16 (Wash. 2015) (en banc).
61. *Id.* at 717–18 (quoting the “Clerk’s Papers”).
62. *Id.* at 724 (McCloud, J., dissenting).
64. *Id.* at *2 (quoting FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009)).
65. *Id.* at *2–3 (quoting defendant’s website).
make your reports look like they should: positive” for a fee for companies with negative postings.66 Based on the above allegations, the court found that it was reasonable to infer that the defendant was not a neutral publisher and that the website’s objective was “to commercialize on its ability to sell its program to counter the offensive content the Ripoff Report encouraged.”67 Therefore, the court denied the defendant’s motion to reconsider the court’s order denying its motion to dismiss for failure to state a claim.

Diamond Ranch Academy, Inc. v. Filer68 shows that websites that host third-party comments will not necessarily receive Section 230 immunity. The defendant created a website called “DRASurvivors.com” that published critical statements about a residential youth treatment facility, Diamond Ranch Academy (“DRA”), and DRA sued for defamation.69 The defendant argued that she was entitled to Section 230 immunity because she merely posted third-party statements, but the court disagreed.70 The court found that the defendant “did more than simply post whatever information the third parties provided. She elicited statements through two surveys that contained specific questions to gather information about specific issues.”71 Additionally, the defendant added “her own comments to the website, post[ed] her own articles, and summarize[d] the statements of others,” therefore precluding her from obtaining immunity under Section 230.72

VI. PLAINTIFFS HAVE CONTINUED TO ASSERT THEORIES OTHER THAN CONTENT-CREATION AIMED AT OVERCOMING SECTION 230 IMMUNITY, WITH SOME SUCCESS

As in prior years, there has been a trend this year of plaintiffs advancing theories other than the intermediary’s development of the content in question as a means to circumvent Section 230 immunity.

In Song fi Inc. v. Google, Inc., the court held that the safe harbor of Section 230 did not protect defendant YouTube against claims based on its removal of the plaintiffs’ video from the YouTube website.73 YouTube explained that it removed the plaintiffs’ video because it determined that the video’s view count was artificially inflated through automated means, such as use of robots.74 YouTube argued that Section 230 conferred immunity for removing the video because the artificially inflated view count was “otherwise objectionable” as stated in Section 230(c)(2).75 However, the court found that interpretation of the catchall term “otherwise
objectionable” required looking at the list of terms preceding it—“obscene, lewd, lascivious, filthy, excessively violent, [and] harassing”—and was unpersuaded that “otherwise objectionable” included the alleged artificially inflated view count.76 The court further determined that the fact Section 230 is captioned “Protection for ‘Good Samaritan’ blocking and screening of offensive material” is another signal that Congress intended the provision to apply to “potentially offensive materials, not simply any materials undesirable to a content provider or user.”77 Because YouTube’s conduct did not fall within the scope of Section 230, the court denied immunity for YouTube from the plaintiffs’ contract and tortious interference claims.78

The plaintiff in Tanisha Systems, Inc. v. Chandra79 avoided Section 230 immunity by alleging that the defendant Chandra conspired with another party, Jayaprakash, to create a blog and make defamatory statements about Chandra’s former employer, plaintiff Tanisha Systems, Inc. (“Tanisha”). Because Tanisha did not allege that Chandra actually wrote the defamatory blog post, this deficiency normally would have allowed Chandra to invoke the protection of Section 230. However, the court found that Tanisha had “sufficiently pled that Chandra materially contributed to the development of the blog post” by allegedly creating a “hit list’ of employees” to solicit for confidential information to use for their “widely disseminated misrepresentations,” and he also “use[d] social media and blog postings to infect any search results concerning Tanisha . . . with false, malicious, and defamatory’ statements.”80 The court reasoned that “it would make little sense to allow an individual to work in concert with another to defame someone, but allow him to disclaim liability because he worked behind the scenes, did not initially publish the defamatory statement he helped create, and only ‘passed along’ the defamatory statement once it was out in the air.”81

A noteworthy decision is Jane Doe No. 14 v. Internet Brands, Inc., in which the Ninth Circuit held that Section 230 did not bar a plaintiff’s claim that the website modelmayhem.com (“Model Mayhem”), which is owned by Internet Brands, was liable for not warning her or other users about rapists who had used the website, through which she was invited to a fraudulent modeling audition in order to drug, rape, and record her for a pornographic video.82 The plaintiff alleged that Internet Brands knew that the rapists had been contacting other members of Model Mayhem using false identities in order to lure them to fraudulent modeling auditions and perform similar acts.83 Although the trial court dismissed the claim as barred

76. Id. at 882–83 (quoting 47 U.S.C. § 230(c)(2)(A)).
77. Id. at 883 (emphasis added by court) (quoting, in the first instance, the caption to 47 U.S.C. § 230(c)).
78. Id. at 884.
80. Id. at *9 (alteration added by court) (footnote omitted) (quoting the complaint).
81. Id.; see id. at *8 (“The CDA only provides a defense to those who pass along information provided by ‘another’ content provider. 47 U.S.C. § 230(c)(1).”).
82. 824 F.3d 846, 848–49 (9th Cir. 2016). The court granted an earlier petition for rehearing and withdrew a previously issued opinion. Id. at 848.
83. Id. at 849.
by Section 230, the Ninth Circuit held that dismissal was improper as the plaintiff was not seeking to hold the defendant liable as a publisher of content on the website, or for failure to remove content.\textsuperscript{84} Instead, the Ninth Circuit found that the plaintiff was asserting liability for “failing to warn her about information it obtained from an outside source about how third parties targeted and lured victims through Model Mayhem.”\textsuperscript{85} The court held that the “duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes or monitors such content.”\textsuperscript{86} Instead, the Ninth Circuit suggested that Internet Brands could have warned users by posting a notice or sending an e-mail about its knowledge of the rapists’ activities.\textsuperscript{87} This suggestion may create future implications that service providers are expected to warn users of dangers. The court further supported its conclusion by stating that the plaintiff’s failure to warn claim was not related to defendant’s “efforts, or lack thereof, to edit, monitor, or remove user generated content.”\textsuperscript{88} Instead, the plaintiff was alleging that the defendant “should be held liable, based on its knowledge of the rape scheme and its ‘special relationship’ with users like Jane Doe, for failing to generate its own warning.”\textsuperscript{89} The Ninth Circuit voted to deny a rehearing en banc,\textsuperscript{90} leaving further questions open about the interplay between failure to warn and Section 230 in the Ninth Circuit.

VII. INTERMEDIARIES FIGHT REGULATORY EFFORTS RELYING ON A COMBINATION OF THE FIRST AMENDMENT AND SECTION 230

A final category of cases involved disputes between intermediaries and regulators that sought information or otherwise exerted pressure.

In \textit{Xcentric Ventures, L.L.C. v. Smith}, the plaintiffs, which own and operate the Ripoff Report website, sought an injunction prohibiting the County Attorney of Sac County, Iowa, from engaging in investigatory efforts targeting Ripoff Report and one of its principals.\textsuperscript{91} The plaintiffs alleged that others posted to Ripoff Report defamatory statements about witnesses who had testified against a woman previously convicted of murder.\textsuperscript{92} The plaintiffs also stated that Ripoff Report used search engine optimization techniques to cause these defamatory posts to appear first in Google searches for the witnesses’ names.\textsuperscript{93} The court did not take a favorable view of Ripoff Report’s Section 230 defense, instead considering it likely that both Xcentric Ventures and its principal would be found at trial to be “more than a neutral conduit” for the allegedly unlawful content and that they

\begin{itemize}
  \item \textsuperscript{84} Id. at 849–51.
  \item \textsuperscript{85} Id. at 851.
  \item \textsuperscript{86} Id.
  \item \textsuperscript{87} Id.
  \item \textsuperscript{88} Id. at 852.
  \item \textsuperscript{89} Id. (quoting Tarasoff v. Regents of Univ. of Cal., 551 P.2d 334, 343 (Cal. 1976)).
  \item \textsuperscript{90} Jane Doe No. 14 v. Internet Brands, Inc., 824 F.3d 846 (9th Cir. 2016) (order denying petition for rehearing en banc of defendant-appellee Internet Brands, Inc.).
  \item \textsuperscript{91} No. C15-4008-MWB, 2015 WL 4940812, at *2 (N.D. Iowa Aug. 19, 2015).
  \item \textsuperscript{92} Id. at *6–7.
  \item \textsuperscript{93} Id. at *6.
\end{itemize}
would be found “to have materially contributed to the alleged illegality of the statements at issue.” The court nevertheless issued a broad injunction on First Amendment grounds, after finding that the County Attorney’s investigatory efforts had a retaliatory motive.

Backpage.com, LLC v. Dart was a somewhat similar case. There, the Cook County, Illinois, sheriff sent letters to Visa and MasterCard pressuring them to cease providing payment services to Backpage, which operated a site that was the subject of numerous Section 230 rulings, including two discussed above. Backpage sought an injunction against Sheriff Dart prohibiting him from engaging in his letter-writing campaign. The district court declined to issue the injunction, but the Seventh Circuit reversed, finding that Sheriff Dart’s threats infringed Backpage’s First Amendment rights. In the course of the ruling, the appellate court noted that Backpage was immune from the conduct Sheriff Dart sought to quash, and neither it nor the credit card companies he tried to coerce could likely be held liable for state law violations, consistent with Section 230.

The last case in this genre is Google, Inc. v. Hood. There, the attorney general of Mississippi issued a broad administrative subpoena to Google, seeking information regarding Google’s alleged efforts to facilitate the publication of “unlawful activity.” Google sought an injunction in federal court. The district court granted the injunction, noting among other things that “federal law [i.e., Section 230] significantly restricts [Attorney General Hood’s] ability to take action of the sort in question here.” The Fifth Circuit reversed on procedural grounds, holding that the subpoena was not ripe for review. But in so doing, it noted the important Section 230 interests at stake: “This lawsuit, like others of late, reminds us of the importance of preserving free speech on the internet, even though that medium serves as a conduit for much that is distasteful or unlawful.”

VIII. CONCLUSION

These developments reflect a healthy number of Section 230 rulings that are typical defense wins, i.e., unremarkable applications of Section 230 to plaintiffs’ claims. On the other hand, many courts took a broad view of the quality of al-
legations necessary to allege that an intermediary played a role in creating or developing the content, in the process taking a narrow view of Section 230. Plaintiffs also continued to advance a variety of theories other than content-creation to circumvent Section 230 immunity, with some success, including a big win in the Ninth Circuit. Finally, this year saw a number of legal skirmishes between intermediaries and regulators, where intermediaries tried to push back and preempt regulatory efforts.
Navigating the Perils of Ransomware

By Edward A. Morse* and Ian Ramsey**

I. INTRODUCTION

Extortion is a longstanding business model for criminal enterprises. Kidnapping still presents a significant business risk in some areas.1 Vessels and their cargoes are also vulnerable to acts of piracy that entail ransom demands.2 Although well-developed legal and security systems can reduce these physical threats to persons and property, technology presents new avenues for extortion. Criminal enterprises are adapting their business models by using so-called “ransomware” to gain control over computer networks and then demand payment in exchange for restoration. This emerging threat presents new challenges for businesses, law enforcement agencies, and policymakers.

II. OVERVIEW OF RANSOMWARE

Ransomware is malware that encrypts data in a host computer or mobile device with the intent to exchange a ransom payment for the decryption key.3 The concept is not new, but it has recently metastasized into a sophisticated and lucrative criminal enterprise.4 Through exploiting macro functions in common business applications like Microsoft Word or Microsoft Excel, macro malware can infect a user’s computer system with code that can affect operational control or encrypt stored data, thus preventing access. Microsoft responded to earlier versions of this threat by requiring users to affirmatively approve the operation of macros, but malware authors have continued to operate through carefully targeted social engineering campaigns. An e-mail attachment from what appears to

---

* Professor of Law, Creighton University School of Law, Omaha, Nebraska.

** Stites & Harbison PLLC, Louisville, Kentucky.


2. See Tom Patterson, Maritime Risk Outlook, in RISKMAP REPORT, supra note 1, at 116, 116–18.


be a trusted source may thus contain a malevolent payload, which is opened by an unsuspecting user who sees a familiar subject line that triggers curiosity, such as a résumé or an invoice.\footnote{Id. at 35–37.} Data collected by McAfee indicate that the vast majority of victims of these attacks reside in North America (44 percent) and Europe (29 percent).\footnote{Id. at 36.} Growth continues because, as McAfee notes, “ransomware campaigns are financially lucrative with little chance of arrest, so they have become quite popular.”\footnote{McAfee Labs, Threats Report 39 (Mar. 2016), http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf.}

Such attacks can be prevented. According to McAfee, “[g]enerally, there is no need to enable macros to view the contents of a document. If you receive such a document, beware. These tricks can be easily defeated just by staying aware of the threat.”\footnote{McAfee Labs, supra note 4, at 46.} Nevertheless, human error presents a formidable obstacle to overcome, and in some cases, merely clicking on a link or visiting a website can trigger an infection.

Microsoft also provides extensive information on the latest ransomware infections. Topping the list are two related versions, Crowti and CrowtiA, which use JavaScript embedded in spam e-mails to encrypt files on a computer and direct the owner to a webpage requesting payment in bitcoin in order to unlock those files.\footnote{Ransom: HTML/Crowti.A, Microsoft: Malware Protection Ctr., https://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Ransom:HTML/Crowti.A (last updated July 6, 2016).} Numerous variations exist as cyber-criminals continue to modify their threats in response to a constantly evolving security environment.\footnote{See Alert (TA16-091A), supra note 3.}

Bitcoin has emerged as a preferred ransom payment medium because of its comparative advantage of effective anonymity and transferability outside of regulated financial networks.\footnote{Routing through the financial system may not provide traceability in all cases, particularly when international channels are involved. See Katy Burne, Swift Finds Evidence of Second Malware Attack, WALL ST. J. (May 12, 2016, 10:50 PM), http://www.wsj.com/articles/swift-finds-evidence-of-second-malware-attack-1463102215 (noting that thieves stole $81 million from a Bangladesh bank using the Swift platform, and the funds have not yet been traced).} Bitcoin owners face a potential “choke point” if they convert bitcoin to cash, thus reentering a regulated financial network. However, that conversion may occur in a jurisdiction where regulation is weak, or after bitcoin has been effectively “laundered” through the purchase of goods and services. As the emergence of bitcoin permits a ransom payment to circumvent detection and tracking otherwise possible through traditional financial networks, it has become apparent that technology favors the hacker.

Not all extortion incidents involving personal data involve ransomware. For example, hackers targeted clients of Ashley Madison, a website devoted to “casual encounters, married dating, discreet encounters and extramarital affairs.”\footnote{Ashley Madison, www.ashleymadison.com (last visited May 12, 2016) (quoting from the description metatag). Mrs. Morse and Mrs. Ramsey, please note this was a professional visit only.}
The hackers advised Ashley Madison account holders: “If you would like to pre-
vent me from finding and sharing this information with your significant other 
send [\$450 dollars in bitcoin] to the following address . . . .”13 In this case, it 
was likely that hackers had control of the data from Ashely Madison accounts 
and that they chose to monetize that access through extortion.14 However, in 
ransomware cases, it is often not clear that the hacker has control of data.15 In-
stead, the owner or custodian has simply lost control of that data until the hacker 
provides a key to restore that control.

III. LEGAL ISSUES FOR RANSOM PAYMENTS

Ransomware attacks often present a clear business case for payment. For ex-
ample, hackers have targeted hospitals, effectively shutting down their opera-
tions by cutting off access to electronic patient records. In one case, system con-
trol was restored for the modest payment of \$17,000 worth of bitcoin—likely far 
less than the potential losses incurred.16 Even if access could be restored through 
a backup system, transaction costs and delays associated with restoration may 
nevertheless counsel payment, if the price is right. Law enforcement officials 
have recognized the practical efficacy of paying off the hacker if access to data 
is important, as they lack the practical ability to restore the data or to capture 
the perpetrator. As an official of the Federal Bureau of Investigation (“FBI”) 
noted: “[T]o be honest, we often advise people just to pay the ransom.”17 
Legal sanctions are unlikely to preclude solving a ransomware problem in this 
manner, but some laws may deserve further consideration.

2015/ashley-madison-hack-sparks-lawsuit.

14. In fact, following the hack, numerous websites displayed putative account information in 
searchable databases, some of which may present other risks. See, e.g., Elizabeth Weise, Why You 
Shouldn’t Download the Ashley Madison Database, USA TODAY (Aug. 22, 2016, 2:18 PM), http:// 
www.usatoday.com/story/tech/2015/08/21/ashley-madison-database-cheaters-dangerous-download-
stolen-property/32118963/.

15. Each incident will require careful analysis of the applicable data security breach notification 
laws, which is beyond the scope of this survey. The U.S. Department of Health and Human Services 
is reportedly developing guidance for hospitals affected by ransomware to comply with breach noti-
fications. See Alex Ruoff, Privacy Enforcers to Weigh In on Ransomware, BLOOMBERG BNA HEALTH CARE 

16. See Brian Mastroianni, Dangerous Escalation in Ransomware Attacks, CBS NEWS (Feb. 20, 2016, 
for-ransom/. This payment also appears to be far less than the likely value of patient data on the 
black market, which may reach \$50 to \$60 per record. See Crime Leading HIPAA Breach Cause 
Says Ponemon Data Security Study, HIPAA J. (May 8, 2015), http://www.hipaajournal.com/crime-
leading-hipaa-breaches-cause-says-ponemon-data-security-study-4432/. This suggests that the hack-
ers likely did not possess that data, but instead had merely prevented access to it.

17. See Devlin Barrett, Paying Ransoms to Hackers Stirs Debate, WALL ST. J. (Nov. 9, 2015, 4:59 PM), 
54 and accompanying text (indicating that payment of ransom is not the FBI’s current policy).
A. SANCTIONS BARRIERS

The Treasury Department’s Office of Foreign Assets Control (“OFAC”) supervises the implementation of economic sanctions designed to prevent trade or financial transactions with designated payees, entities, or countries. Economic sanctions are rooted in laws that implement political policies by regulating private commercial actors in order to support foreign policy and national security goals.18

OFAC maintains a searchable database of designated parties and relevant sanction restrictions.19 Thus, payments made to designated parties or countries covered by sanctions are clearly illegal, potentially resulting in civil or criminal penalties not only for those making the payments, but also for those facilitating them.20 Although banks are accustomed to consulting the OFAC database when making payment abroad to a designated payee, a firm making a bitcoin payment via e-mail will likely not have the name or location of the designated payee. Thus, the sanctions regime is unlikely to affect a ransom payment, except in cases when the criminal self-identifies in a manner triggering the sanctions regime.

Executive Order No. 13,694 seeks to expand the sanctions regime to block the property of persons engaging in “Significant Malicious Cyber-Enabled Activities.”21 The order declares a “national emergency to deal with this threat” from cyber-enabled activities.22 It extends to the assets of those who “have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity [proscribed by the order] or any person whose property and interests in property are blocked pursuant to this order.”23 The Secretary of the Treasury consults with the Attorney General and the Secretary of State in determining whether to block one’s assets.24 Firms like Coinbase25 that facilitate bitcoin transactions could possibly fall under this executive authority on account of bitcoin payments being made to cybercriminals through its wallet services.

B. TAX LAWS

Tax laws that impose limits on deductibility, require information reporting, and impose withholding obligations on certain payments may also affect firms

---

18. For an historical discussion of post-World War II sanctions and these laws, see Joseph W. Bishop, Jr., Judicial Construction of the Trading with the Enemy Act, 62 Harv. L. Rev. 721 (1949).
22. Id.
23. Id. § 1(a)(ii)(B).
24. Id. § 1(a)(ii).
that choose to pay ransom. Section 162 of the Internal Revenue Code provides authority for deducting “ordinary and necessary” expenses in carrying on a trade or business,\(^2\) but it restricts deductions for payments that constitute “an illegal bribe, illegal kickback, or other illegal payment under any law of the United States [or any generally enforced State law] which subjects the payor to a criminal penalty or the loss of license or privilege to engage in a trade or business.”\(^2\) Significantly, the government bears the burden of proof regarding disallowance of a deduction under this provision.\(^2\) Thus, any uncertainty about the applicability of the sanctions regime (potentially presenting a case for a criminal penalty) would tend to favor the taxpayer’s claim for a deduction.

Information-reporting requirements may also present complexities. Payors are required to provide an information return for an aggregate payment of $600 or more to certain service providers.\(^2\) The payee is required to furnish his name, address, and identification number,\(^2\) but cyber-criminals are unlikely to comply. Penalties may apply for failing to furnish statements,\(^2\) furnishing incomplete or incorrect statements,\(^2\) or failing to file correct information returns with the government.\(^2\) However, penalties may be excused where failure is “due to reasonable cause and not to willful neglect.”\(^2\) Query whether a ransom payment to a cyber-criminal will qualify for such relief. Although federal income tax law apparently does not disallow deductions for such payments even if not properly reported,\(^2\) at least one state (California) claims authority to deny deductions for amounts not timely reported on Form 1099.\(^2\)

Withholding requirements imposed on payments to foreign payees if the payment constitutes gross income from sources within the United States could present another tax compliance issue.\(^2\) Again, the uncertain identity and location of the payee presents compliance concerns, including whether the malefactor’s activities provide a sufficient nexus to treat that income as U.S.-sourced. Improper failure to withhold could trigger liability for the tax\(^2\) —a potential additional cost associated with ransom.

---

27. Id. § 162(c)(2); see also id. § 162(c)(1) (targeting illegal payments to government officials).
28. Id. § 162(c)(2).
29. See id. § 6041A(a).
30. Id. § 6041A(f).
31. Id. § 6722(a)(2)(A).
32. Id. § 6722(a)(2)(B).
33. Id. § 6721.
34. Id. § 6724(a).
38. See id. § 1461.
C. OTHER CONCERNS

The above discussion is not exhaustive, as other provisions could affect a payor or even one advising a payor to facilitate a ransom payment. For example, the Foreign Corrupt Practices Act of 1977 (“FCPA”)\(^\text{39}\) could potentially apply in cases where the cyber-criminal has a known connection to a foreign government. Again, the muted identity of cyber-criminals involved in ransomware likely prevents a payor from having knowledge that a proscribed payment is being made. However, it should be noted that economic duress (which occurs in the typical ransomware context) has been viewed as insufficient to excuse conduct from sanctions under the FCPA,\(^\text{40}\) but no authorities have tested this theory in a ransomware scenario.

IV. GOVERNMENT ASSISTANCE

Government agencies are acutely interested in taking action against this growing problem. Local cybercrime units in larger U.S. cities may provide assistance, but the international scope of this activity generally requires involvement from federal agencies and cross-border cooperation.\(^\text{41}\) A plethora of federal agencies are active in this area, presenting challenges for information sharing and coordination. The FBI has a dedicated and effective Cyber Task Force, which utilizes an online cybercrimes reporting form via the Internet Crime Complaint Center, commonly known as “IC3.”\(^\text{42}\) Other affiliated agencies include the National Cyber Investigative Joint Task Force,\(^\text{43}\) which also operates in partnership with the Department of Defense Cyber Crime Center,\(^\text{44}\) iGuardian\(^\text{45}\) (relating to minors), Infra-Guard\(^\text{46}\) (a collaboration between the private sector and FBI to share information), and the National Cyber-Forensics & Training Alliance.\(^\text{47}\) The FBI also offers its Cyber Action Team\(^\text{48}\) to assist with cyber intrusions around the world.

Other agencies could also be involved. For example, the Department of Homeland Security (“DHS”) organized the National Cybersecurity and Communica-

---


V. POLICY DIRECTIONS

Despite government attention to threats from cyber-criminals, self-help is likely to appeal to ransomware victims. Nevertheless, current FBI policy discourages ransom payments in favor of prevention efforts and a strong business continuity plan to address malware infections.\footnote{See Incidents of Ransomware on the Rise: Protect Yourself and Your Organization, FED. BUREAU INVESTIGATION (Apr. 29, 2016), https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise.} The FBI is concerned that making ransom payments will incentivize further ransomware incidents and also fund other illegal activity.\footnote{See id.}

Investments in technology, training, data storage, and restoration protocols create a deterrent effect by imposing costs on cyber-criminals. Those who invest will drive cyber-criminals to move on to other markets, perhaps with softer targets that allow better payoffs. Some hackers may even market their technologies to the highest bidder, including those seeking to develop effective preventive measures.\footnote{See Thomas Fox-Brewster, Meet the Ex-Army Hackers Trying to Save America from Blackouts, FORBES (Mar. 23, 2016, 6:03 AM), http://www.forbes.com/sites/thomasbrewster/2016/03/23/saving-america-from-hacker-blackouts/#7b63d48a657e (noting gray market for software weaknesses in utility industry).}

Ransomware incidents have demonstrated a strong business case for enhanced cybersecurity investments in many environments. Successful attacks have effectively provided a diagnostic for failed practices and systems, and ransom pay-
ments may be viewed as a small price to pay for this diagnosis. When risks to human life and to firm reputations are at stake, future failures are not an option.

Government measures to encourage private investment in prevention and remediation technologies and to discourage payments that monetize crime may yet emerge. However, the shape and content of such measures remain uncertain. Information sharing among government agencies and within the private sector will be essential to develop an effective approach to managing risks from ransomware threats.  