

Cornell Law Review


Volume 102
Issue 6 September 2017

Article 6

What Would Grandma Say? How to Respond When Cyber Hackers Reveal Private Information to the Public

Jason P. Ottomano
Cornell Law School

Follow this and additional works at: <https://scholarship.law.cornell.edu/clr>

 Part of the [Computer Law Commons](#), and the [Intellectual Property Law Commons](#)

Recommended Citation

Jason P. Ottomano, *What Would Grandma Say? How to Respond When Cyber Hackers Reveal Private Information to the Public*, 102 Cornell L. Rev. 1743 (2017)
Available at: <https://scholarship.law.cornell.edu/clr/vol102/iss6/6>

This Note is brought to you for free and open access by the Journals at Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell Law Review by an authorized editor of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.

NOTE

WHAT WOULD GRANDMA SAY?: HOW TO RESPOND WHEN CYBER HACKERS REVEAL PRIVATE INFORMATION TO THE PUBLIC

Jason P. Ottomano†

INTRODUCTION	1743
I. BACKGROUND	1745
A. Privacy and the Internet	1745
B. The Rights of Privacy and Publicity	1747
C. The Communications Decency Act and its Good Samaritan Provision	1750
II. SPLIT OF AUTHORITY	1752
A. Ninth Circuit: <i>Perfect 10, Inc. v. CCBill LLC</i> ...	1752
B. New Hampshire District Court: <i>Doe v.</i> <i>Friendfinder Network, Inc.</i>	1754
C. New York District Court: <i>Atlantic Recording</i> <i>Corp. v. Project Playlist, Inc.</i>	1755
III. ANALYSIS	1756
A. Statutory Resolution	1756
B. Policy Proposals	1759
1. <i>Information Transfer</i>	1759
2. <i>Narrow the Intellectual Property</i> <i>Carve-Out</i>	1761
3. <i>Data-Breach Insurance</i>	1762
CONCLUSION	1763
A. Resolution of the § 230(e)(2) Intellectual Property Carve-Out.....	1763
B. Moving Forward	1764

INTRODUCTION

On August 18, 2015, a group of hackers named Impact Team released 37 million records—9.7 gigabytes of data—from the Toronto-based website Ashley Madison.¹ The hackers

† B.A., Colby College, 2014; J.D., Cornell Law School, 2017; Editor, *Cornell Law Review*. I would like to thank my parents, Peter and Kristine, for their endless love and support. Additionally, I would like to thank the members of the *Cornell Law Review* for their hard work.

¹ Bree Fowler, *Lawsuits Against Ashley Madison Over Hack Face Tough Road*, AP NEWS ARCHIVE (Aug. 20, 2015, 3:00 AM), <http://www.apnewsarchive>

claimed to be motivated by the alleged unscrupulous practices of Ashley Madison's parent company, Avid Life Media Inc., such as false advertising and failing to follow through on a data-purging procedure for which it charged members a nineteen-dollar fee.² The data dump has affected people from all walks of life, including 15,000 government employees,³ Vice President Joe Biden's son,⁴ and individuals who, because of this data breach, learned that strangers used their e-mail addresses to create Ashley Madison accounts.⁵ Former subscribers to the website have received demands to pay money in the form of bitcoins as a ransom on their personal information.⁶ The data breach is likely related to at least two suicides thus far.⁷ Lawsuits against Avid Life Media Inc. have commenced, and more are in the planning stages; some plaintiffs hope to coordinate class action litigation.⁸ Despite the understandable outrage that the website's members and former members feel, many lawyers are not optimistic about the chances of recovering damages from Ashley Madison or Avid Life Media Inc.⁹

.com/2015/Lawsuits_against_Ashley_Madison_over_hack_face_tough_road/id-2bb8646f7770441f804d8070696f0ade [https://perma.cc/UGD5-GFN6]; Nicole Perlroth, *Hackers Say They Have Released Ashley Madison Files*, N.Y. TIMES (Aug. 18, 2015, 7:37 PM), https://bits.blogs.nytimes.com/2015/08/18/hackers-say-they-have-released-ashley-madison-files/?_r=1 [https://perma.cc/J459-49DH]; Daniel Victor, *The Ashley Madison Data Dump, Explained*, N.Y. TIMES (Aug. 19, 2015), <http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html> [https://perma.cc/EN7D-7YFW].

² Perlroth, *supra* note 1.

³ Cory Bennett, *15,000 Government Emails Revealed in Ashley Madison Leak*, HILL (Aug. 19, 2015, 9:55 AM), <http://thehill.com/policy/cybersecurity/251431-ashley-madison-leak-appears-real-includes-thousands-of-government-emails> [https://perma.cc/Y5BU-FDWX]. *But see id.* ("[T]he site reportedly did not check the validity of email addresses, and it's likely that many of the government email accounts were faked.")

⁴ Tal Kopan, *Hunter Biden Denies Link to Ashley Madison*, CNN (Aug. 25, 2015, 5:40 PM), http://www.cnn.com/2015/08/25/politics/hunter-biden-ashley-madison-denial/?iid=ob_article_organicsidebar_expansion&iref=obinsite [https://perma.cc/L34U-UMD3].

⁵ See Victor, *supra* note 1 (reporting that an unmarried woman in New York City said that a man in South Africa had created an account using her e-mail address).

⁶ Katie Rogers, *After Ashley Madison Hack, Police in Toronto Detail a Global Fallout*, N.Y. TIMES (Aug. 24, 2015), <http://www.nytimes.com/2015/08/25/technology/after-ashley-madison-hack-police-in-toronto-detail-a-global-fallout.html> [https://perma.cc/5FUW-HYC8].

⁷ See *id.*; CNNMoney Staff, *The Ashley Madison Hack . . . in 2 Minutes*, CNN MONEY (Sept. 11, 2015, 11:34 AM), <http://money.cnn.com/2015/08/24/technology/ashley-madison-hack-in-2-minutes/> [https://perma.cc/5XSU-43ZT].

⁸ Fowler, *supra* note 1; see CNNMoney Staff, *supra* note 7.

⁹ Fowler, *supra* note 1.

This Note will explore the avenues for recovery available to individuals who lose control of their personal information when the security of an organization that collects or holds such information is compromised. This Note will begin by tracing the development of privacy jurisprudence as it specifically relates to the creation and eventual prominence of the Internet in the United States. Next, the piece will discuss the emerging split of authority surrounding a question of statutory interpretation presented by the Good Samaritan exception of the Telecommunications Act of 1996. Specifically, the issue is whether 47 U.S.C. § 230(e)(2)—a carve-out within the Good Samaritan exception that withholds immunity for civil liability for intellectual property claims—applies to federal intellectual property laws *only*, or to both federal *and* state intellectual property laws. The piece will then conclude that if the Supreme Court were to resolve this split of authority, it should, and likely would, hold that § 230(e)(2) withholds immunity from claims brought under both federal *and* state intellectual property laws. Finally, this Note will present new policy proposals that Congress and interactive computer service providers (ICSPs) could pursue in light of that conclusion.

I

BACKGROUND

A. Privacy and the Internet

“The Internet is ‘a unique and wholly new medium of worldwide human communication.’”¹⁰ The Internet grew out of a 1969 military program called “ARPANET,”¹¹ which was designed to allow communication between military units, defense contractors, and universities engaged in defense research.¹² ARPANET provided for redundant channels of communication in case parts of the network were destroyed in a war.¹³ While the ARPANET exists now only in the annals of history, it provided the model for the civilian networks that today enable “tens of millions of people to communicate with one another and to access vast amounts of information from around the world.”¹⁴

¹⁰ *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 850 (1997), (quoting *Am. Civil Liberties Union v. Reno*, 944 F. Supp. 824, 844 (E.D. Pa. 1996)).

¹¹ An acronym for the Advanced Research Project Agency Network. *Id.* at 850 n.3.

¹² *Id.* at 849–50.

¹³ *Id.* at 850.

¹⁴ *Id.*

The Internet has profoundly affected both consumers and publishers of information. For consumers, the Internet provides "both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services."¹⁵ For publishers,¹⁶ the Internet is "a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers."¹⁷

The Internet's emergence and rapid rise in both popularity and use¹⁸ has presented novel questions of individual privacy rights.¹⁹ The Internet is forcing American privacy jurisprudence to evolve with it—a phenomenon that history has rarely seen occur with such alacrity.²⁰ As one court has noted:

The near instantaneous possibilities for the dissemination of information by millions of different information providers around the world to those with access to computers and thus to the Internet have created ever-increasing opportunities for the exchange of information and ideas in "cyberspace."²¹ This information revolution has also presented unprecedented challenges relating to rights of privacy and reputational rights of individuals, to the control of . . . rumors and other information that is communicated so quickly that it is too often unchecked and unverified. Needless to say, the

¹⁵ *Id.* at 853.

¹⁶ "Any person or organization with a computer connected to the Internet can 'publish' information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals." *Id.* "The Internet allows anyone connected to it to disseminate information, statements, gossip, and so on, to millions of people with a few strokes on a computer keyboard. Thus millions of people now have their own electronic printing presses . . ." R. Timothy Muth, *Old Doctrines on a New Frontier: Defamation and Jurisdiction in Cyberspace*, WIS. LAW., Sept. 1995, at 10, 11–12.

¹⁷ *Reno*, 521 U.S. at 853.

¹⁸ *Id.* at 850 ("The Internet has experienced extraordinary growth." (internal quotations omitted)).

¹⁹ See, e.g., *Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998) (discussing how the Internet has given rise to unprecedented legal debates about privacy and identity protection); Muth, *supra* note 16, at 13, 56 (discussing how the virtual sphere of cyberspace affects traditional concepts of jurisdiction).

²⁰ See, e.g., *It's in the Cards, Inc. v. Fuschetto*, 535 N.W.2d 11, 14–15 (Wis. Ct. App. 1995) ("The rate at which technological developments are growing coupled with the complexity of technology is beyond many laypersons' ken. A uniform system of managing information technology and computer networks is needed to cope with the impact of the information age. It is the responsibility of the legislature to manage this technology and to change or amend the statutes as needed.").

²¹ "Cyberspace refers to the interaction of people and businesses over computer networks, electronic bulletin boards and commercial online services. The largest and most visible manifestation of cyberspace is the Internet . . ." Muth, *supra* note 16, at 11.

legal rules that will govern this new medium are just beginning to take shape.²²

As both the use and sophistication of the Internet have increased, so too have the potential risks that Internet users face with respect to their personal information.²³ Citizens in the United States are aware of these risks—according to a 2016 Pew Research Center Poll, about half of Americans are concerned about the possible misappropriation of their personal information through the Internet.²⁴ Scholars agree that this concern is indeed well-founded.²⁵

B. The Rights of Privacy and Publicity

The historical development of the rights of privacy and publicity long predate the Internet. Indeed, these legal concepts had a head start of about eighty years when, in 1890, Samuel Warren and Louis Brandeis argued in a law review article that the common law should recognize a right to privacy.²⁶ This right to privacy, they said, should protect citizens against intrusive and embarrassing stories by the press.²⁷

In 1902, the New York Court of Appeals rejected both the Warren and Brandeis article and a common law right to privacy

²² *Blumenthal*, 992 F. Supp. at 49; see also Muth, *supra* note 16, at 13 (“Analogies to existing legal doctrines can take the courts only so far as they begin to develop the law of cyberspace.”).

²³ 1 RONALD N. WEIKERS, DATA SECURITY AND PRIVACY LAW: SECURITY AND PRIVACY IN THE NETWORKED WORLD § 2:4 (2016).

²⁴ Kenneth Olmstead & Aaron Smith, *Americans and Cybersecurity*, PEW RES. CTR. (Jan. 26, 2017), <http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/> [<https://perma.cc/3ZKP-3M74>] (“This survey finds that a majority of Americans have directly experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse.”).

²⁵ See, e.g., Muth, *supra* note 16 at 12 (“To say that libel and slander are rampant on the Internet would be an understatement.”).

²⁶ Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); see also 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:10 (2d ed. 2015); Leah Burrows, *To Be Let Alone: Brandeis Foresaw Privacy Problems*, BRANDEISNOW (July 24, 2013), <http://www.brandeis.edu/now/2013/july/privacy.html> [<https://perma.cc/R5ET-EYSF>] (“Brandeis and his law partner Samuel Warren published ‘The Right to Privacy’ in the Harvard Law Review in 1890, where it became the first major article to advocate for a legal right to privacy.”).

²⁷ Warren & Brandeis, *supra* note 26, at 196; see also 1 MCCARTHY, *supra* note 26, § 1:10; Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 2 (1979) (“In simplest terms, for Warren and Brandeis the right to privacy was the right of each individual to protect his or her psychological integrity by exercising control over information which both reflected and affected that individual’s personality.”).

in *Roberson v. Rochester Folding Box Co.*²⁸ The *Roberson* court held that Abigail Roberson could not recover from the defendant flour company after the flour company used her portrait in an advertisement without her consent.²⁹ Writing for the majority, Chief Judge Alton B. Parker invoked the floodgates rationale:

If [the right to privacy] be incorporated into the body of the law through the instrumentality of a court of equity, the attempts to logically apply the principle will necessarily result, not only in a vast amount of litigation, but in litigation bordering upon the absurd, for the right to privacy, once established as a legal doctrine, cannot be confined to the restraint of the publication of a likeness but must necessarily embrace as well the publication of a word-picture, a comment upon one's looks, conduct, domestic relations or habits.³⁰

In 1905, the Georgia Supreme Court recognized a right to privacy in *Pavesich v. New England Life Insurance Co.*³¹ The plaintiff, Paolo Pavesich, sued the New England Mutual Life Insurance Company for publishing an advertisement that was comprised of Pavesich's picture and a testimonial of Pavesich's satisfaction with his life insurance policy.³² Pavesich had neither purchased a New England Mutual Life Insurance policy nor given permission for the company to use his picture.³³ The *Pavesich* court implicitly rejected Chief Justice Parker's floodgates argument:

It may be said that to establish a liberty of privacy would involve in numerous cases the perplexing question to determine where this liberty ended This affords no reason for not recognizing the liberty of privacy, and giving to the person aggrieved legal redress against the wrongdoer³⁴

Justice Cobb, writing for the Georgia Supreme Court, reconciled potential conflicts between a right to privacy and the constitutional rights of free speech and press by admitting that in certain instances personal privacy would need to yield to the public need for information.³⁵ Justice Cobb expressed his confidence in the judiciary to properly balance these two competing interests and noted that in the case at bar, New England

²⁸ See *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 544-45 (1902).

²⁹ *Id.* at 557-58.

³⁰ *Id.* at 544-45.

³¹ *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68, 70-71 (1905).

³² *Id.* at 68-69.

³³ *Id.* at 69.

³⁴ *Id.* at 72.

³⁵ *Id.* at 72-73; 1 MCCARTHY, *supra* note 26, § 1:17 .

Mutual Life Insurance's advertisement was not "an expression of an idea, a thought, or an opinion, within the meaning of the constitutional provision which guaranties to a person the right to publish his sentiments on any subject."³⁶

Almost fifty years later, in 1953, Judge Jerome Frank of the Second Circuit Court of Appeals coined the phrase "right of publicity."³⁷ In *Haelan Laboratories v. Topps Chewing Gum*, a dispute arose when rival chewing gum companies competed over contracts with professional baseball players to use the players' pictures on chewing gum cards.³⁸ The plaintiff contended that the defendant knowingly induced players—who had already signed a contract with the plaintiff—to sign a contract with the defendant. Although the plaintiff brought the case under a theory of tortious interference with a contract, Judge Frank nevertheless turned to the narrower issue of the players' pictures themselves.³⁹ Judge Frank conceived of the right of publicity when he said, "We think that . . . a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture This right might be called a 'right of publicity.'⁴⁰

One year later, in 1954, Professor Melville Nimmer wrote an article outlining the fundamental elements necessary to a right of publicity.⁴¹ Nimmer first defined *publicity values* as the pecuniary value in a person's name, photograph, or likeness.⁴² He then explained that the right of publicity is "the right of each person to control and profit from the publicity values which he has created or purchased."⁴³ It is important to note that Professor Nimmer argued that the right of publicity should not be limited to those who have achieved celebrity status; rather, *every individual has a right of publicity*, with the caveat that the value, with respect to damages, may vary depending on the societal status of the wronged individual.⁴⁴

Claire Gorman notes, for example, that the biggest obstacle that private citizens face in asserting right of publicity claims is demonstrating a pecuniary interest in their identity and eco-

³⁶ *Pavesich*, 50 S.E. at 80.

³⁷ 1 MCCARTHY, *supra* note 26, § 1:26.

³⁸ 202 F.2d 866 (2d Cir. 1953).

³⁹ *Id.* at 867–69.

⁴⁰ *Id.* at 868.

⁴¹ See Melville B. Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954).

⁴² *Id.* at 204.

⁴³ *Id.* at 216.

⁴⁴ *Id.* at 217.

conomic harm from its misappropriation.⁴⁵ Although the simple fact that a defendant misappropriated a person's identity triggers a presumption of commercial value, this presumption is limited to situations in which the defendant uses the person's identity for commercial benefit.

The Nimmer and Gorman propositions, taken together, would seem to bar most private citizens from successfully bringing right of publicity claims in cases where the details of their identity have been compromised but not used for commercial gain, as in the case of the Ashley Madison victims. Nevertheless, private citizens may prevail even if the commercial link is tenuous—such as if the misappropriating party uses the victim's identity or likeness in a commercial forum even without expressly identifying the victim.⁴⁶

Currently, the courts of twenty-one states have recognized the right of publicity under state common law.⁴⁷ Additionally, eleven states have statutes on the books which, despite explicitly mentioning only the right of privacy, are worded so as to embody the principles of the right of publicity. In sum, then, thirty-two states recognize the right of publicity, either by statute or under common law.

C. The Communications Decency Act and its Good Samaritan Provision

Congress enacted the Communications Decency Act (CDA)⁴⁸ as part of the Telecommunications Act of 1996 in large part to “protect minors from exposure to obscene and indecent material on the Internet.”⁴⁹ Indeed, the CDA was meant to modernize protections against “an increasing number of published reports of inappropriate uses of telecommunications technologies to transmit pornography, engage children in inappropriate adult contact, terrorize computer network users

⁴⁵ See Claire E. Gorman, *Publicity and Privacy Rights: Evening Out the Playing Field for Celebrities and Private Citizens in the Modern Game of Mass Media*, 53 DEPAUL L. REV. 1247, 1274 (2004) (acknowledging that the lodestar of the right of publicity cause of action is the monetary value that society places on the image and likeness of celebrity figures).

⁴⁶ *Id.* at 1256–57; see, e.g., *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 292 (D.N.H. 2008) (involving a claim in which a plaintiff alleged biographical information and a photo reasonably identified her to members of the community despite not expressly using her name).

⁴⁷ 1 MCCARTHY, *supra* note 26, § 6:3.

⁴⁸ Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified as amended in scattered sections of 47 U.S.C.).

⁴⁹ *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 699 (S.D.N.Y. 2009) (discussing legislative history of the CDA).

through ‘electronic stalking,’ and seize personal information.”⁵⁰ Although certain portions of the CDA have been struck down as “unconstitutional limitations on free speech,” § 230 remains good law.⁵¹

Section 230(c)(1) of the CDA states, “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”⁵² This Good Samaritan exception was enacted to combat congressional concern that subjecting interactive service providers to the same standards of liability as entities that actually published online content would create a chilling effect on the development of the Internet based on the specter of massive tort liability.⁵³ After all, millions of people use the Internet and interactive service providers could not screen every posting for potential problems.⁵⁴ The Good Samaritan exception “sought to prevent lawsuits from shutting down websites and other services on the Internet.”⁵⁵ Congress prioritized free speech interests and sought to combat any chilling effect by immunizing service providers for content published by other entities.⁵⁶

In the CDA, Congress attempted to walk a fine line between “preserv[ing] the vibrant and competitive free market that presently exists for the Internet . . . , unfettered by Federal or State regulation”⁵⁷ on the one hand, and “ensur[ing] vigorous enforcement of . . . criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer”⁵⁸ on the other. In walking this line, Congress chose to distinguish providers of interactive computer services from other types of information providers.⁵⁹ Indeed, “[w]hether

⁵⁰ S. REP. NO. 104-23, at 9 (1996).

⁵¹ *Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003).

⁵² 47 U.S.C. § 230(c)(1) (2012).

⁵³ *See Atl. Recording Corp.*, 603 F. Supp. 2d at 699.

⁵⁴ *Zeran v. American Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997) (“Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted.”).

⁵⁵ *Batzel*, 333 F.3d at 1028.

⁵⁶ *Zeran*, 129 F.3d at 331.

⁵⁷ 47 U.S.C. § 230(b)(2) (2012).

⁵⁸ 47 U.S.C. § 230(b)(5) (2012).

⁵⁹ *See Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998) (“Congress decided not to treat providers of interactive computer services like other information providers such as newspapers, magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared by others.”); *see also Zeran*, 129 F.3d at 330–31 (“Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. . . . Section 230 was enacted,

wisely or not, [Congress] made the legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others.”⁶⁰ Without the Good Samaritan exception, ICSPs could be liable for speech published or distributed on its website, even though a third party was actually the author of that speech.⁶¹

Accordingly, website owners may be exempt from liability from common law and state statutory privacy claims pursuant to the Good Samaritan exception. There is presently a split of authority as to whether the CDA preempts state law right of publicity claims asserted against providers of ICSPs.⁶² The Ninth Circuit has held that state law claims against owners and operators of blogs, websites, and other Internet sites or services are preempted.⁶³ The Ninth Circuit’s analysis has been criticized as inconsistent with the plain terms of the CDA in two district court opinions in the First and Second Circuits.⁶⁴ While these cases are not binding precedent, they are likely to provide persuasive authority in courts outside of the Ninth Circuit.

II

SPLIT OF AUTHORITY

A. Ninth Circuit: *Perfect 10, Inc. v. CCBill LLC*

Perfect 10 publishes an adult entertainment magazine and owns the website perfect10.com.⁶⁵ Customers pay Perfect10.com a membership fee in order to access the site’s content. Perfect 10 displays on its site approximately 5,000 images it has created of its models, many of whom have signed away to Perfect 10 their rights of publicity.⁶⁶ CWIE is an In-

in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. . . . Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties’ potentially injurious messages.”).

⁶⁰ *Blumenthal*, 992 F. Supp. at 49.

⁶¹ See *Batzel v. Smith*, 333 F.3d 1018, 1026 (9th Cir. 2003).

⁶² 4 E-COMMERCE AND INTERNET LAW § 37.05[5] (2016).

⁶³ *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007).

⁶⁴ *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 702 (S.D.N.Y. 2009); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 298 (D.N.H. 2008).

⁶⁵ *Perfect 10*, 488 F.3d at 1108.

⁶⁶ The right of publicity is “the right to prevent others from using one’s name or picture for commercial purposes without consent.” *Douglass v. Hustler Magazine, Inc.*, 769 F.2d 1128, 1138 (7th Cir. 1985). The right of publicity can include a person’s “name, likeness, and other identifying characteristics.” Michael

ternet service-provider to website-owners; CCBill enables credit card or check payment for online memberships or subscriptions to e-commerce venues.⁶⁷ CWIE and CCBill provided services to websites that posted images on the Internet from Perfect 10's magazine and website. In 2002, Perfect 10 sued CWIE and CCBill claiming, inter alia, a violation of right of publicity under state law as well as false and misleading advertising.

According to the Ninth Circuit, a majority of federal courts have read the Good Samaritan clause of the CDA to immunize service providers against claims originating from third-party usage of their service.⁶⁸ This immunity does not extend, however, to suits sounding in intellectual property.⁶⁹ The court noted that 47 U.S.C. § 230(e)(2), which exempts intellectual property claims from Good Samaritan immunity, does not expressly define "intellectual property."⁷⁰ The court reasoned that because state intellectual property laws differ across the country, and because information on the Internet can be accessed in multiple states at the same time, Congress must have intended to exempt only *federal* intellectual property claims from immunity.⁷¹ To hold otherwise would be to allow one state's intellectual property laws to "dictate the contours of this federal immunity."⁷² Accordingly, the court determined that CWIE and CCBill are eligible for immunity under the CDA against Perfect 10's state law false advertising and right of publicity claims.⁷³

Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CALIF. L. REV. 125, 130 (1993). "The majority of commentators and courts hold that everyone, celebrity and noncelebrity alike, has a right of publicity." 1 McCarthy, *supra* note 26, § 4:14.

⁶⁷ *Perfect 10*, 488 F.3d at 1108.

⁶⁸ *Id.* at 1118.

⁶⁹ The CDA also states that "[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2) (2012).

⁷⁰ *Perfect 10*, 488 F.3d at 1118.

⁷¹ *Id.* at 1118–19; see also Eric Goldman, *Ninth Circuit Opinion in Perfect 10 v. CCBill*, TECH. & MARKETING L. BLOG (Mar. 29, 2007), http://blog.ericgoldman.org/archives/2007/03/ninth_circuit_o.htm [<https://perma.cc/3Q8Q-NAAE>] ("In one brief yet bold stroke, the 9th Circuit . . . say[s] simply that where Congress said '[intellectual property],' they meant 'federal [intellectual property].'").

⁷² *Perfect 10*, 488 F.3d at 1118.

⁷³ *Id.* at 1121.

B. New Hampshire District Court: *Doe v. Friendfinder Network, Inc.*

In *Doe v. Friendfinder Network, Inc.*, the plaintiff sued the adult social network and dating service, Adult FriendFinder, for, among other things, violation of the plaintiff's right of publicity under New Hampshire law.⁷⁴ The plaintiff alleged that a fake profile was created on the site, and that the biographical data and nude photo associated with the profile could reasonably identify the plaintiff to members in her community.⁷⁵ The plaintiff further alleged that when she requested that the profile be removed from the site, Adult FriendFinder agreed, but that for several more months the profile continued to exist on other similar websites that the defendant owned.

The defendant contended that the CDA shielded it from the plaintiff's state law claim.⁷⁶ The plaintiff asserted that the CDA does not bar her state law claim of violation of her right of publicity, "which she characterize[d] as an infringement of her intellectual property rights."⁷⁷ The defendant countered that the CDA does not apply to state-created property rights.

The District Court noted that both the First and Eleventh Circuits have construed § 230(e)(2) as applying to both federal and state intellectual property laws.⁷⁸ The court went on to address the Ninth Circuit's contrary statutory interpretation in *Perfect 10*, stating, "this court does not find the Ninth Circuit's resolution of the statutory interpretation question to be persuasive."⁷⁹ The District Court reasoned that Congress's use of the modifier "any" in § 230(e)(2) suggests that Congress did not intend to place a limiting construction on intellectual property law, especially in light of the fact that Congress distinguished between federal and state law in other provisions of the CDA.⁸⁰

⁷⁴ *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 302 (D.N.H. 2008).

⁷⁵ *Id.* at 292.

⁷⁶ *Id.* at 294.

⁷⁷ *Id.* at 298.

⁷⁸ *Id.* at 299; see also Martin Samson, *Jane Doe v. Friendfinder Network Inc. and Various, Inc.*, INTERNET LIBR. L. & CT. DECISIONS, http://www.internetlibrary.com/cases/lib_case600.cfm [<https://perma.cc/PXD8-3PHV>] ("In reaching this result, the Court found more persuasive dicta from the First Circuit in *Universal Comm'n Sys., Inc. v. Lycos, Inc.*, 478 F.3d 413, 422-23 (1st Cir. 2007) than a contrary holding of the Ninth Circuit in *Perfect 10, Inc. v. CC Bill, LLC*, 488 F.3d 1102 (9th Cir.) cert denied 128 S.Ct. 709 (2007), where the Ninth Circuit 'construe[d] the term "intellectual property" to mean "federal intellectual property."').

⁷⁹ *Friendfinder Network, Inc.*, 540 F. Supp. 2d at 299; see also Goldman, *supra* note 71 ("[T]he Ninth Circuit is out-of-bounds here. Just based on straight statutory interpretation, I don't see how the Ninth Circuit can conclude that the word 'federal' is imported into the words 'intellectual property.'").

⁸⁰ *Friendfinder Network, Inc.*, 540 F. Supp. 2d at 300.

The court “disagree[d] with the Ninth Circuit’s decision in *Perfect 10* that § 230(e)(2) exempts only federal intellectual property laws” and held that “§ 230(e)(2) applies simply to ‘any law pertaining to intellectual property,’ not just federal law.”⁸¹ Accordingly, the CDA did not shield Adult FriendFinder from the plaintiff’s state-law right of publicity claim.⁸²

C. New York District Court: *Atlantic Recording Corp. v. Project Playlist, Inc.*

In *Atlantic Recording Corp. v. Project Playlist, Inc.*, the plaintiffs were six of the largest record companies and the defendant (“Playlist”) operated a website on which users could compile playlists of songs available through third-party websites.⁸³ Playlist used a computer program called a “spider” to locate recordings of songs across the world wide web.⁸⁴ After finding a song, users could listen to it, save it to a playlist on Playlist’s website, or download it.⁸⁵ In addition, users could also upload their playlists to social networking sites such as Facebook and MySpace.

The plaintiffs owned copyrights to the majority of the songs that users could access through Playlist and contended that many of the songs on third-party websites to which Playlist provided links were posted without plaintiffs’ permission.⁸⁶ Accordingly, the plaintiffs sued Playlist for copyright infringement and unfair competition. The plaintiffs argued that their state law claims could proceed against Playlist because they fell within the carve-out to immunity under § 230(e)(2) of the CDA.⁸⁷ Playlist countered that § 230(e)(2) withholds immunity from only federal claims and thus protects Playlist from plaintiffs’ New York state-law claims.

⁸¹ *Id.* at 302 (quoting *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001)); see also Samson, *supra* note 78 (“The Court held that the Communications Decency Act did not, however, immunize defendants from intellectual property claims plaintiff advanced, both under applicable federal and state laws, including right of publicity claims advanced under New Hampshire state law. Plaintiff was accordingly allowed to proceed with claims that defendants, by including identifiable aspects of plaintiff’s persona in advertisements and ‘teasers’ in an effort to increase the profitability of their websites, violated her right to publicity.”).

⁸² *Friendfinder Network, Inc.*, 540 F. Supp. 2d at 302.

⁸³ *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 692–93 (S.D.N.Y. 2009).

⁸⁴ *Id.* at 693.

⁸⁵ *Id.* at 694.

⁸⁶ *Id.* at 693.

⁸⁷ *Id.* at 702.

United States District Judge Denny Chin held that the Good Samaritan exception does not provide immunity for either federal or state law intellectual property claims.⁸⁸ In reaching this conclusion, Judge Chin dealt specifically with the Ninth Circuit's decision in *Perfect 10*.⁸⁹ First, Judge Chin stated that the Ninth Circuit's analysis of the intellectual property carve-out was grounded in policy considerations rather than textual interpretation.⁹⁰ Second, he noted that Congress explicitly specified in four different instances that a particular subsection of 230(e) was to apply to local, state, or federal law.⁹¹ Accordingly, if Congress had intended to limit the carve-out to *federal* law, it knew how to do so.⁹² Finally, the modifier "any" in the phrase, "any law pertaining to intellectual property" indicates that Congress had no desire to limit the carve-out in any way.⁹³

III ANALYSIS

A. Statutory Resolution

The Good Samaritan Provision of the Communications Decency Act states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."⁹⁴ This sentence provides immunity to entities such as Project Playlist, Adult FriendFinder, and Ashley Madison. Section 230(e)(2) of the CDA, however, is a carve-out from the Good Samaritan Provision that withholds immunity for intellectual property claims.⁹⁵ The question that has divided courts, and the question that the Supreme Court should resolve, is

⁸⁸ *Id.* at 704; see also Eric Goldman, *230 Doesn't Preempt State IP Claims—Atlantic Records v. Project Playlist*, TECH. & MARKETING L. BLOG (Apr. 17, 2009), http://blog.ericgoldman.org/archives/2009/04/230_doesnt_pree.htm [https://perma.cc/EW36-RK5E] ("The court conducts a very sensible textual analysis of 47 USC 230 to conclude that it preempts neither state nor federal [intellectual property]. Thus, the net result is that this court, like the N[ew] H[ampshire] *Friendfinder* court, votes against the Ninth Circuit's [*Perfect 10*] ruling. . . . [T]he Ninth Circuit's reading is untenable, in which case either the Ninth Circuit will have to revise its reading . . . or the circuit split may potentially bubble up to the Supreme Court.")

⁸⁹ The defendants relied heavily on the Ninth Circuit's holding. *Atl. Recording Corp.*, 603 F. Supp. 2d at 703.

⁹⁰ *Id.* at 703 & n.11.

⁹¹ *Id.* at 703.

⁹² *Id.* ("[Congress] knew how to make that clear, but chose not to.")

⁹³ *Id.* at 703–04.

⁹⁴ 47 U.S.C. § 230(c)(1) (2012).

⁹⁵ 47 U.S.C. § 230(e)(2) (2012).

whether the § 230(e)(2) carve-out applies to (1) all laws pertaining to intellectual property or (2) only federal laws pertaining to intellectual property. In the case of the former, the Good Samaritan Provision would not provide immunity for any federal or state-law intellectual property claims. According to the latter, ICSPs would retain immunity against state-law, but not federal, intellectual property claims.

The current split of authority has placed the Ninth Circuit Court of Appeals at odds with the District Courts of New Hampshire and New York.⁹⁶ In *Perfect 10*, the Ninth Circuit held that the immunity carve-out applies to only federal laws, thereby bestowing ICSPs with immunity against state-law intellectual property claims.⁹⁷ The court's analysis, however, was grounded in policy considerations rather than statutory language.⁹⁸ The court employed the following line of reasoning: First, each state may have a different statutory scheme regarding intellectual property claims. Second, the same website on the Internet can be accessed simultaneously in multiple states. Third, it follows that to exempt federal *and* state intellectual property claims from immunity would be to allow different *state* laws to define the contours of this *federal* immunity. Finally, given the preceding proposition, it must be true that Congress intended to exempt *only federal* intellectual property claims from immunity, while leaving ICSPs immune from state-law claims.

The New Hampshire District Court took the opposite view in *Doe v. Friendfinder*.⁹⁹ Unlike the Ninth Circuit, the New Hampshire District Court analyzed the language of the CDA and concluded that the immunity carve-out applies to both federal *and* state intellectual property claims.¹⁰⁰ The court

⁹⁶ See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1119 (9th Cir. 2007); *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 692 (S.D.N.Y. 2009); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 302 (D.N.H. 2008); see also Goldman, *supra* note 88 ("In the surprising 2007 [*Perfect 10*] opinion, the 9th Circuit read [47 U.S.C. § 230(e)(2)] to mean that [§] 230 does not preempt [federal intellectual property] claims, but all state [intellectual property] claims were preempted. Then, in the 2008 *Friendfinder* case, a New Hampshire district court expressly declined to follow the [*Perfect 10*] opinion, concluding that state publicity rights claims weren't preempted by [§] 230.").

⁹⁷ See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1119 (9th Cir. 2007).

⁹⁸ See *id.* at 1118–19.

⁹⁹ See *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 302 (D.N.H. 2008).

¹⁰⁰ *Id.* at 299–302; see also Goldman, *supra* note 88 ("[T]he Ninth Circuit's statutory analysis in [*Perfect 10*] was daft, so I am not surprised to find another court expressly rejecting it. (In fact, I doubt any court outside the Ninth Circuit will follow the [*Perfect 10*] case).").

noted that the modifier “any” in § 230(e)(2)’s phrase “[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property” does not place a limiting instruction on intellectual property law.¹⁰¹

The court argued that this is especially true given that Congress distinguished between federal and state law elsewhere in the CDA.¹⁰² Therefore, the court held that the immunity carve-out withholds immunity from both federal and state law intellectual property claims.¹⁰³

In *Project Playlist*, the District Court for the Southern District of New York arrived at the same conclusion as the New Hampshire District Court.¹⁰⁴ Judge Chin focused on the same statutory construction issues as the *Friendfinder* court, noting the significance of the modifier “any” in § 230(e)(2) and also stating that Congress knew how to limit the immunity carve-out to federal law if it so desired.¹⁰⁵

If the Supreme Court resolves this split of authority, it should hold that the immunity carve-out applies to claims under both federal *and* state laws pertaining to intellectual property. The New Hampshire and New York District Court opinions are more persuasive than the Ninth Circuit’s because the District Courts build their conclusion on the foundation of the actual statutory language.

The Ninth Circuit’s reasoning is not illogical; indeed, it comports with Congress’s “legislative judgment to effectively immunize providers of interactive computer services from civil liability in tort with respect to material disseminated by them but created by others”¹⁰⁶ by extending that immunity to state-law intellectual property claims. Nevertheless, it is not a court’s place to carry out what it perceives to be Congress’s will. Legislators are sophisticated actors who are both able and expected to promulgate laws that accurately represent the legislative branch’s intentions.

Accordingly, the plain text of the statutory provision in question should govern any type of interpretive analysis aimed at discerning Congress’s legislative intent. That the *Friendfinder* and *Project Playlist* courts grounded their analyses in the language of § 230(e)(2) is the reason that their reasoning

101 See *Friendfinder Network, Inc.*, 540 F. Supp. 2d at 299.

102 *Id.* at 301.

103 *Id.* at 302.

104 See *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009).

105 *Id.* at 703.

106 *Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998).

and conclusions are more persuasive than those of the *Perfect 10* court. The Supreme Court, therefore, should decide that ICSPs are not immune from federal or state-law intellectual property claims because § 230(e)(2) carves those claims out of the Good Samaritan Provision of the CDA.

A holding that § 230(e)(2) applies to both federal and state intellectual property laws will not create a chilling effect on Internet activity or allow state laws to determine the contours of the Good Samaritan immunity as the Ninth Circuit fears because the intellectual property exception is one small carve-out of an otherwise far-reaching immunity for ICSPs. Intellectual property abuses are just one of the many kinds of harmful activities that the millions of Internet users may engage in, including harassment and distributing obscene or defamatory material. Allowing ICSPs to be liable for intellectual property abuses will not contradict Congress's policy decision "not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages."¹⁰⁷

B. Policy Proposals

Assuming that ICSPs do not have immunity from claims brought under state and federal intellectual property laws, what does that mean for victims of intellectual property based abuses? Because right of publicity claims fall under intellectual property—as noted in *Doe v. Friendfinder*—victims can sue the ICSP for the violation of the right of publicity by third parties. This, in turn, shifts the incentive to the ICSPs to determine how to best police against and combat intellectual property abuses on their websites.

1. *Information Transfer*

One way that ICSPs can protect themselves against lawsuits is to present the injured party with the identity of the actual wrongdoer, i.e., the third party that wrongly disseminated information. If Congress's justification for the broad immunity of the CDA is that it is too difficult to hold companies liable for their members' posts and that such an imposition of liability will chill speech, then companies should at least be obliged to provide the victim of the data breach with details about the individual who posted the information. In doing so, ICSPs could deflect the injured party's claim back against the

¹⁰⁷ Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997).

actual wrongdoer. To effect this change, Congress could pass an amendment to the CDA requiring breached companies to relinquish any information that they discover about the identity of the hacker to the victims of the data breach. Accordingly, the victims would most likely direct the resulting lawsuit against the culpable party rather than against the ICSP.

Unfortunately, this proposed solution has a two-pronged defect. First, due to the fact that many security breaches of this kind are criminal activities performed by cyber hackers, it will be difficult for the breached company or entity to discover any meaningful information relating to the identity of the perpetrators. For example, when the Office of Personnel Management was hacked in 2015, hackers stole the Social Security numbers of approximately 21.5 million government workers.¹⁰⁸ However, even after this massive security breach, then Director of National Intelligence, James Clapper, stated only that China was the “leading suspect” in the cyber attack.¹⁰⁹ As another example, the most that is known about the Ashley Madison hackers is that the name of the group that orchestrated the cyber attack is Impact Team—investigators do not know anything more than this mysterious Internet calling card.¹¹⁰

Second, even if the breached company or law enforcement officers do discover the identity of the person or persons responsible for illegally disseminating victims’ personal information, it may prove impossible to prosecute due to international law or relations. For example, if the Chinese government orchestrated the breach of the Office of Personnel Management in 2015, then even if the United States discovered the identities of the hackers responsible, we would almost certainly not be able to arrange for their transportation to America to stand trial.

Take, as another example, Edward Snowden. Snowden was a contractor at the National Security Agency who, in June of 2013, leaked troves of information regarding American internet and phone surveillance techniques to the media.¹¹¹ Af-

¹⁰⁸ *Cybersecurity Resource Center: Frequently Asked Questions*, U.S. OFF. PERSONNEL MGMT., <https://www.opm.gov/cybersecurity/faqs/> [<https://perma.cc/W3DT-S52P>].

¹⁰⁹ Jim Sciotto, *OPM Government Data Breach Impacted 21.5 Million*, CNN (July 10, 2015, 1:15 PM), <http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/> [<https://perma.cc/4RHL-V87M>].

¹¹⁰ Perlroth, *supra* note 1.

¹¹¹ See *Edward Snowden: Leaks That Exposed US Spy Programme*, BBC (Jan. 17, 2014), <http://www.bbc.com/news/world-us-canada-23123964> [<https://perma.cc/F3LN-8JCP>].

ter he divulged the information, Snowden fled the United States and has since been granted asylum in Russia, out of the reach of the U.S. justice system.¹¹² The recent vote by the European parliament—composed of members from all twenty-eight European Union states—that called on member states to drop any criminal charges against Snowden and prevent his extradition to the United States means that he will likely be able to continue to evade prosecution for his crimes. Despite these examples, it is nonetheless possible—however unlikely—that victims of the Ashley Madison breach could sue the perpetrators. Ashley Madison is a Toronto-based company, and if it is discovered that the hackers are also Canadian, the United States would be able to rely on its extradition treaty with Canada to bring the hackers back to the United States to stand trial.¹¹³ That path is far from certain, however, considering that the hackers' identities are currently unknown.

2. *Narrow the Intellectual Property Carve-Out*

A different approach that Congress could take in response to the proposition that ICSPs are not immune from either federal or state right of publicity claims is to amend the CDA to narrow the § 230(e)(2) intellectual property carve-out. In other words, Congress could legislate that claims advanced under the right of publicity do not fall under the umbrella of intellectual property claims. This solution would be beneficial because it would save time and judicial resources. Given the difficulty that private citizens face in recovering under the right of publicity,¹¹⁴ there might be a net benefit from immunizing ICSPs from such claims and removing them from the judicial process. After all, the fact that private citizens may sue ICSPs does not seem to be serving as an incentive for ICSPs to undertake greater security measures—at least in the case of Ashley Madison.¹¹⁵

¹¹² See Tom McCarthy, *Edward Snowden Praises EU Parliament Vote Against US Extradition*, GUARDIAN (Oct. 29, 2015), <http://www.theguardian.com/us-news/2015/oct/29/edward-snowden-eu-parliament-vote-extradition> [https://perma.cc/QXQ9-QKW6].

¹¹³ See Treaty on Extradition Between Canada and the United States of America, Can.-U.S., Dec. 3, 1971, 27 U.S.T. 983, https://www.oas.org/juridico/MLA/en/traites/en_traites_can-usa-ext1991.pdf [https://perma.cc/3Z4F-KTSM].

¹¹⁴ See Nimmer, *supra* note 41, at 204; Gorman, *supra* note 45, at 1274.

¹¹⁵ Ashley Madison failed to perform the data-scrub that it offered members for a nineteen-dollar fee as a way to completely eliminate any records of the member's registration with the site. See Perlroth, *supra* note 1.

Accordingly, granting this immunity would be a method for Congress to further refine its process of balancing vibrant free speech interests with the need to protect minors from obscene material on the internet.¹¹⁶ Indeed, this policy proposal would further Congress's intention "not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages."¹¹⁷ Finally, this would only affect the subset of claims advanced under the right of publicity, while leaving untouched § 230(e)(2)'s allowance of liability for other types intellectual property claims. Because rights of publicity claims are purely personal, immunizing ICSPs from them would not have the same effect as immunizing ICSPs from, say, claims relating to research and development, new product designs, or other proprietary information. These commercial intellectual property claims should continue to be allowed as a way of ensuring good business practices. Right of publicity claims arising out of cybersecurity breaches play no such functional role in society.

However, immunizing ICSPs from right of publicity causes of action, despite uncluttering the judicial system, may nevertheless prove to be unsatisfactory. Even if this potential liability is not currently creating a significant incentive for ICSPs to engage in protective measures concerning consumer information, and even if claimants face substantial barriers to recovery, to eliminate the right of publicity cause of action would be to begin down a slippery slope. Although improving judicial efficiency is certainly a worthy endeavor, it should not be the basis for casting aside an otherwise legitimate cause of action. Similarly, the fact that private citizens may rarely recover does not mean that Congress should deprive them of the opportunity to vindicate their rights when an ICSP's security is breached.

3. *Data-Breach Insurance*

A final policy proposal is that insurance companies could create a new type of insurance policy specifically designed for ICSPs in the event that a cybersecurity attack occurs. This would be helpful because—were the Supreme Court to resolve the § 230(e)(2) split of authority by determining that ICSPs are not immune from state or federal law right of publicity claims—the price that ICSPs charge for their services might increase

¹¹⁶ 47 U.S.C. §§ 230(b)(2), (5) (2012).

¹¹⁷ *Zeran v. America Online, Inc.*, 129 F.3d 327, 330–31 (4th Cir. 1997).

dramatically. A price increase passed on to consumers would have precisely the chilling effect that Congress attempted to avoid in passing the CDA¹¹⁸ and would also have the potential to decrease demand for services to the point that some ICSPs might go out of business—another result that Congress sought to avoid.¹¹⁹

“Third-Party Data Breach” insurance would be similar to director and officer insurance in the corporate context in that it would transform a potentially massive source of liability into a manageable risk that would be assimilated into the everyday costs of doing business. If a cyber attack breached an ICSP’s security and accessed important consumer information, then the Third-Party Data Breach insurance would allow the victims to be compensated for the violation of their right of publicity. Additionally, ICSPs could avoid lawsuits and thereby save the legal fees of defending against right of publicity claims.

It is unclear whether a Supreme Court decision withholding immunity for state and federal intellectual property claims would indeed cause a large price increase for ICSP services. ICSPs might not consider right of publicity claims especially threatening given the difficulties private citizens have faced in succeeding on such claims mentioned above. Nevertheless, it is entirely possible that at least some ICSPs would raise their prices as a way to insulate their business against potential lawsuits. That, coupled with the fact that there is no downside to the creation of Third-Party Data Breach insurance policies, leads to the conclusion that this policy proposal is the best and most efficient way to respond if the Supreme Court resolves the split of authority in favor of the New York and New Hampshire District Courts.

CONCLUSION

A. Resolution of the § 230(e)(2) Intellectual Property Carve-Out

The Supreme Court should resolve this split of authority in order to settle the matter of whether ICSPs are immune from state and federal right of publicity claims. The analysis of the New York and New Hampshire District Courts was grounded in the plain language of § 230¹²⁰ and is thus more persuasive

¹¹⁸ See *Atl. Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 700 (S.D.N.Y. 2009).

¹¹⁹ See *Batzel v. Smith*, 333 F.3d 1018, 1028 (9th Cir. 2003).

¹²⁰ See *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 299, 301 (D.N.H. 2008) (noting first that Congress used the modifier “any” when referring to

than the Ninth Circuit's decision which relied exclusively on policy considerations.¹²¹ Accordingly, the Supreme Court should follow the District Court opinions in *Doe v. Friendfinder*¹²² and *Atlantic Records v. Project Playlist*.¹²³

B. Moving Forward

Assuming that the Supreme Court holds that § 230(e)(2) applies to both federal and state intellectual property laws, then the victims of the Impact Team's hack of Ashley Madison could, theoretically, sue Ashley Madison. However, because the hackers have yet to use the victims' information for any type of commercial purpose—the hackers merely made the information available to the public—the victims would likely be unable to show any recoverable monetary value. Therefore, a favorable ruling on the split of authority would help the Ashley Madison victims in theory, but not in practice. Those former members of Ashley Madison that paid the nineteen-dollar fee to have their profiles permanently deleted could very likely still succeed under contract principles, though again, harm and damages would likely be nominal.

The best societal response to the Supreme Court holding that ICSPs are immune from claims advanced under both state and federal intellectual property laws is the creation of Third-Party Data Breach insurance policies. Requiring breached companies to transfer information about the hackers to victims of the breach will likely yield little benefit; even in the unlikely case that an investigation uncovers the identity of the hackers, prosecution will still be difficult and costly. Additionally, narrowing the intellectual property carve-out to exclude claims based on the right of publicity would forsake a legitimate cause of action in the interests of judicial efficiency—an unbalanced tradeoff that society should avoid in this instance (and generally). Third-Party Data Breach insurance provides the greatest benefit—allowing companies to compensate victims of cybersecurity attacks for an affordable cost—with no significant drawback. Therefore, the best policy response to potential liability for right of publicity claims does not lie in Congress's

intellectual property laws, which signaled that the statute included both federal and state intellectual property law; and, second, that Congress knew how to distinguish between federal and state laws if it chose to do so); *Atl. Recording Corp.*, 603 F. Supp. 2d at 703 (reaching the same conclusion).

¹²¹ See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir. 2007).

¹²² *Friendfinder Network*, 540 F. Supp. 2d at 299.

¹²³ *Atl. Recording Corp.*, 603 F. Supp. 2d at 703.

hands, but in the hands of the private sector insurance industry.