WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 12, ISSUE 1 FALL 2016

EQUITABLE RECOVERY FOR ASHLEY MADISON HACK VICTIMS: THE FEDERAL TRADE COMMISSION AS EXECUTOR OF A NARROW RIGHT TO BE FORGOTTEN IN THE UNITED STATES

Mackenzie Olson[*]

Cite as: 12 Wash. J.L. Tech. & Arts 61 (2016)
http://digital.lib.washington.edu/dspace-law/handle/ 1773.1/1649

ABSTRACT

Events following the Ashley Madison data breach exposed the personal information of millions of users. Victims filed class action suits in multiple courts in the United States, seeking various forms of monetary and equitable relief. However, these plaintiffs have been unable to compel the removal of personal information from third-party Internet sites hosting the information previously circulated by hackers. Citizens of the European Union, by contrast, could likely compel the removal of such personal information. Unlike the United States, the European Union recognizes a "right to be forgotten", which authorizes individuals to demand the removal of their personal information from third-party sites.

This Article examines how such a right to be forgotten could function in the United States, and particularly how this right could allow victims of the Ashley Madison hack, as well as those of other data breaches, to see their personal information eventually removed from third-party sites. This Article suggests that such a right, if narrowly

---

[*] Mackenzie Olson, JD Candidate, University of Washington School of Law, Class of 2017. Thank you to my advisors, Professor Robert Gomulkiewicz, UW Law Foundation Professor of Law and Director for the IP LL.M, and Tim Lee of Olive Hill Group. Also thank you to the editorial staff of this Journal for your feedback and direction throughout the revising and editing process.

applied in limited circumstances by the Federal Trade Commission, could better serve the needs of consumers and still preserve First Amendment rights thereby implicated.

TABLE OF CONTENTS

INTRODUCTION

The dating website Ashley Madison tells its users "Life is short. Have an affair."[1] Accordingly, the site generates matches between its users who want to act on this suggestion.[2] As a result of this mission, Ashley Madison recently fell victim to data

[1] Ashley Madison, (last visited Nov. 8, 2015), *available at* https://www.ashleymadison.com.

[2] *See* Molly Mulshine, *I created an Ashley Madison account and it was worse than I imagined*, TECH INSIDER (Sep. 29, 2015, 4:07 PM), http://www.techinsider.io/what-its-like-on-ashley-madison-2015-9/#to-start-all-i-had-to-do-was-go-to-ashleymadisoncom-select-single-female-seeking-males-and-then-create-my-account-the-site-is-free-for-women-male-users-have-to-pay-at-least-49-per-month-for-100-credits-which-enable-them-to-use-the-site-1 (last visited Sep. 23, 2016).

hackers.[3] When companies suffer data breaches, such incidents compromise their customers' personal information, including their names, social security numbers, credit card numbers, and medical information.[4] Given the nature of Ashley Madison's services, the release of its customers' personal information could unravel the very fabric of many individuals' private lives.

Ashley Madison has used the Digital Millennium Copyright Act ("DMCA") as a means of damage control.[5] So far, the company has issued successful copyright takedown notices to multiple websites, including Twitter.[6] However, Ashley Madison's stolen customer data may not be entitled to copyright protection because a court would likely not consider it an original work of authorship.[7] Thus, Ashley Madison's reliance on the DMCA may ultimately prove ineffective.[8] Moreover, critics argue that these requests abuse the DMCA and that material copyright misrepresentations could simply land Ashley Madison in further legal trouble: other companies that previously suffered data hacks and subsequently issued misleading DMCA takedown requests to websites hosting the stolen material have lost countersuits challenging those requests.[9] From a practical standpoint, Ashley

---

[3] Many companies have fallen victim to data breaches, including: Target, Premara Blue Cross, Anthem, Chick-fil-A, Sony, the U.S. Postal Service, MCX, Staples, Kmart, Dairy Queen, Supervalu, Viator.com, Jimmy John's, Home Depot, Community Health Systems/Tenova, P.F. Chang's, and J.P. Morgan. *See Data Breach Tracker: All the Major Companies that Have Been Hacked*, TIME (Mar. 18, 2015), *available at* http://time.com/money/3528487/data-breach-identity-theft-jp-morgan-kmart-staples.

[4] *Id.*

[5] Hope King, *Ashley Madison tries to stop the spread of its leaked data*, CNNMoney (Aug. 21, 2015), available at http://money.cnn.com/2015/08/21/technology/ashley-madison-dmca-requests/index.html?iid=hp-stack-dom.

[6] *Id.*

[7] A work is copyrightable when it is an original work of authorship, fixed in a tangible form of expression. *See* Kelley v. Chicago Park Dist., 635 F.3d 290, 299 (7th Cir. 2011).

[8] King, *supra* note 5.

[9] Kashmir Hill, Hello, *DMCA A 1990s anti-piracy law is why you haven't seen the hacked list of Ashley Madison customers*, FUSION (Jul. 20, 2015, 2:44

Madison ultimately cannot use the DMCA to compel removal of every copy of its stolen information from all Internet sites.[10]

Unlike the DMCA, the European Union's 1995 Data Protection Directive ("Directive") and its right to be forgotten[11] provide a private cause of action that empowers individual European Union citizens to compel the removal of certain personal information from Internet sites. Under the Directive, Ashley Madison and its customers could theoretically issue takedown notices, regardless of whether the information is copyrightable. While such a right is not currently recognized in the United States, this Article explains how such a right could operate in the United States. First, this Article examines current data security issues in the United States and how the federal government prosecutes those companies with deficient cybersecurity measures. It goes on to compare privacy rights in the United States with those in the European Union. In so doing, it explores how a right to be forgotten, narrowly administered by the federal government, could function in the United States.

I. DATA SECURITY IN THE UNITED STATES

A. Ashley Madison Hack Victims Seek Monetary and Equitable Relief

Avid Life Media, a Canadian corporation, owns Avid Dating Life, which does business as Ashley Madison.[12] Prior to its data breach, the company charged users a $19 fee to remove

---

PM), http://fusion.net/story/169981/where-is-the-ashley-madison-hack/ (last visited Feb. 14, 2016).

[10] *Id.*

[11] *Factsheet on the "Right to be Forgotten" Ruling (c-131/12)*, European Commission, (last visited November 8, 2015), available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

[12] Robert Hackett, *What to know about the Ashley Madison hack*, Fortune (Aug. 26, 2015), available at http://fortune.com/2015/08/26/ashley-madison-hack.

information from its database, though it did not always remove this information after payment.[13] Hackers disagreed with Ashley Madison's mission to arrange marital affairs and broke into the Ashley Madison website in July 2015, releasing the personal information of 32 million users.[14]

Victims of the hack took legal action. Individuals sued Internet service providers Amazon Web Services and GoDaddy, as well as actual site operators, for hosting sites that contained the stolen data.[15] They alleged that these companies intentionally inflicted emotional distress on Ashley Madison users.[16]

Victims also filed class action suits against Avid Life Media and Ashley Madison in multiple federal district courts, including Texas, Missouri, Alabama, and California.[17] In December 2015, these cases were consolidated in the Eastern District of Missouri.[18] A judge in Missouri also recently barred plaintiffs from suing as John Does, ordering that they must instead use their own names.[19]

Plaintiffs asserted numerous theories of liability against Ashley Madison, including violation of the Stored

---

[13] *Id.*

[14] *Id.*; *see also* Kim Zetter, *Answers to Your Burning Questions on the Ashley Madison Hack*, Wired (Aug. 21, 2015), available at https://www.wired.com/2015/08/ashley-madison-hack-everything-you-need-to-know-your-questions-explained/.

[15] James Kosur, *Amazon and GoDaddy are being sued over the Ashley Madison data leak*, Business Insider (Sep. 7, 2015), available at http://www.businessinsider.com/amazon-and-godaddy-sued-over-ashley-madison-data-leak-2015-9.

[16] *Id.*

[17] *See* Compl., Doe v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a/ Ashley Madison, No. 6:15-cv-01464-LSC (N.D. Ala. Aug. 25, 2015), 2015 WL 5023966; Compl., J. DOE 1 v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a Ashley Madison, No. 8:15-cv-01347 (C.D. Cal. Aug. 24, 2015), 2015 WL 5012608.

[18] In re Ashley Madison Customer Data Sec. Breach Litig., No. 2669, 2015 WL 8541658, at *2 (U.S. Jud. Pan. Mult. Lit. Dec. 9, 2015).

[19] Robert Hackett, *Ashley Madison Hacking Victims Face a Big Decision*, Fortune (Apr. 20, 2016), available at http://fortune.com/2016/04/20/ashley-madison-data-breach-lawsuit-names/.

Communications Act; violation of state deceptive trade practices acts; breach of implied contract; breach of contract; violation of state data breach notification statutes; violation of state consumer protection laws; violation of state customer records acts and unfair competition laws; and public disclosure of private facts.[20] In these complaints, plaintiffs requested various forms of monetary relief, as well as injunctive relief that would require Ashley Madison to implement and maintain adequate security measures in the future and to notify affected customers in the event of other data breaches.[21] While such relief may help prevent future hacks and mitigate some of the harm that victims currently suffer, this relief does not enable victims to compel the removal of their stolen personal information from third-party sites. Nor does any government entity appear to possess the authority to force the removal of this information.[22]

B. The United States Government Currently Prosecutes Companies with Deficient Cybersecurity Under the Federal Trade Commission Act, 15 U.S.C. § 45(a)

The United States government is empowered to prosecute companies with deficient cybersecurity. The Federal Trade Commission ("FTC") is specifically authorized to prevent corporations "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or

---

[20] *See* Compl. at 80-130, J. DOE 1 v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a Ashley Madison, No. 8:15-cv-01347 (C.D. Cal. Aug. 24, 2015), 2015 WL 5012608; *See* Compl. at 33-87, Doe v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a/ Ashley Madison, No. 6:15-cv-01464-LSC (N.D. Ala. Aug. 25, 2015), 2015 WL 5023966.

[21] *Id.*

[22] The Federal Communications Commission, for example, does not even believe that it has the authority to shut down gang leader and terrorist group-operated websites and social media accounts. *See* Mario Trujillo, *FCC says it can't shut down ISIS websites*, The Hill (Nov. 17, 2015), available at https://thehill.com/policy/technology/260438-fcc-says-it-cant-shutdown-online-terrorist-activity.

affecting commerce."[23] In *FTC v. Wyndham Worldwide Corp.*, the Third Circuit granted interlocutory appeal to consider the FTC's ability to regulate cybersecurity and affirmed the FTC's ability to prosecute companies with insufficient cybersecurity, on the grounds that this deficiency could constitute an unfair or deceptive trade practice under the Federal Trade Commission Act.[24]

When the Wyndham Worldwide Corporation's ("Wyndham") computer system was breached, hackers stole thousands of customers' personal and financial information.[25] The FTC found that Wyndham engaged in unfair cybersecurity practices that unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.[26] In fact, "contrary to its policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data."[27] On these grounds, the FTC brought action against Wyndham.[28]

It appears that Ashley Madison, likewise, also maintained deficient cybersecurity measures. Prior to the hacking, Ashley Madison's CEO touted the website's security, even though its protections were insufficient and the company was aware of its susceptibility to a hack.[29] Ashley Madison also advertised a service whereby users could pay $19 to have their account information permanently deleted, in spite of the fact that all supposedly deleted data survived and was recoverable.[30] Supposedly Ashley

---

[23] The Federal Trade Commission Act, 15 U.S.C. § 45(a)(2) (2006).

[24] FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015); *see also* Andy Greenberg, *Court Says the FTC Can Slap Companies for Getting Hacked*, Wired (Aug. 24, 2015, 4:51 PM), http://www.wired.com/2015/08/court-says-ftc-can-slap-companies-getting-hacked (last visited Nov. 7, 2015).

[25] FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

[26] *Id.*

[27] *Id.* at 241.

[28] *Id.* at 236.

[29] Compl. at 36, J. DOE 1 v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a Ashley Madison, No. 8:15-cv-01347 (C.D. Cal. Aug. 24, 2015), 2015 WL 5012608.

[30] Compl. at 14, Doe v. Avid Life Media, Inc. and Avid Dating Life, Inc. d/b/a/ Ashley Madison, No. 6:15-cv-01464-LSC (N.D. Ala. Aug. 25, 2015),

Madison's deleted files may not have been permanently erased and thus remained potentially accessible; a user must take additional steps to permanently delete files, such as overwrite a hard disk's data multiple times with random characters.[31] If a reviewing court found that Ashley Madison's actual security measures were deficient, like it found Wyndham's, then the FTC could likely prosecute Avid Life Media and Ashley Madison on that basis. However, such action would not provide the most beneficial remedy to the victims of the hack because it would not compel the removal of victims' information from third-party sites.

II. PRIVACY IN EUROPE AND THE UNITED STATES

A. The Right to be Forgotten in the European Union

By contrast, the right to be forgotten provides European victims of data hacks with a form of relief unavailable to victims in the United States: the removal of their personal information from third-party sites. In *Google Spain SL, Google v. Ageñcia Espanola de Protección de Datos*, the Court of Justice of the European Union ("CJEU") interpreted the European Union's 1995 Data Protection Directive "as creating a presumption that Google must delete links to personal information from search results at the request of the data subject unless a strong public interest suggests otherwise."[32] Specifically, the CJEU held that the Directive applies to search engines like Google and applies even when the physical server of the company is located outside the European Union.[33]

2015 WL 5023966.

[31] Mark Promerleau, *How hard is it to permanently delete data?*, GCN (Mar. 31, 2015), available at https://gcn.com/articles/2015/03/31/deleted-emails.aspx.

[32] *Internet Law--Protection of Personal Data--Court of Justice of the European Union Creates Presumption That Google Must Remove Links to Personal Data Upon Request.-- Case C-131/12, Google Spain SL v. Agencia Española De Protección de Datos*, 128 Harv. L. Rev. 735, 735 (2014).

[33] *Factsheet on the "Right to be Forgotten" Ruling (c-131/12)*, European Commission (last visited Nov. 7, 2015), *available at* http://ec.europa.eu/justice/data-

The CJEU further held that individuals have the right to ask search engines to remove personal information about them when the information is inaccurate, inadequate, irrelevant, or excessive for the purposes of data processing.[34]

However, the right to be forgotten is not absolute, and must be balanced against other fundamental rights, such as freedom of expression and freedom of the media.[35] Courts assess the right on a case-by-case basis, paying particular attention to the sensitivity of the information to the individual's private life and the interest of public access to that information.[36] Theoretically, European Union citizens who are victims of the Ashley Madison hack could satisfy these elements to invoke this right, and thereby request that their leaked information be removed from third-party sites.

However, a removal request may not be implemented in the same manner throughout the various nations of the European Union. Thus, the actual extent of a removal following a request could vary by country. For example, the Spanish Data Protection Authority interpreted this right narrowly in a recent Spanish case, when it held that Google was not required to remove certain user-generated content because the blog owner controlled the processing of this content.[37] Only the blog owner could remove the content entirely—Google could only be required to remove the links to this content.[38] In contrast, France's data protection regulator, the Commission Nationale de l'Informatique et des Libertés, has interpreted this right broadly.[39] It recently issued a

---

protection/files/factsheets/factsheet_data_protection_en.pdf.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Glyn Moody, *Spanish Court Limits Scope of EU's Right To Be Forgotten*, TechDirt TechDirt (Mar. 6, 2015), available at https://www.techdirt.com/articles/20150306/03342530222/spanish-court-limits-scope-eus-right-to-be-forgotten.shtml.

[38] *Id.*

[39] Peter Fleischer, *Implementing a European, not global, right to be forgotten*, Google Europe Blog (Jul. 30, 2015), available at http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html.

formal notice to Google, ordering it to delist French-based removal requests not just from google.fr and other European versions of Google Search, but from all versions of Google Search globally.[40] Thus, although the right to be forgotten is recognized throughout the European Union, current jurisprudence suggests that if Ashley Madison hack victims issue removal requests in the European Union, such requests would be granted to varying extents in different countries.

B. Privacy in the United States

Though the DMCA enables the takedown of infringing copyrighted works,[41] currently no right to be forgotten exists in the United States.[42] In *Garcia v. Google, Inc.*, the Ninth Circuit recently denied an actress' request that an anti-Islamic video in which she had performed be removed from YouTube,[43] on the grounds that her performance in the video was not copyrightable. In its ruling, the court noted that "Garcia would like to have her connection to the film forgotten and stripped from YouTube . . . such a 'right to be forgotten' . . . is not recognized in the United States."[44]

However, the United States has recognized numerous forms of individual privacy protections and various privacy-related causes of action in tort law. Former United States Supreme Court Justice Louis Brandeis originally introduced the right to privacy in the United States in a *Harvard Law Review* article in 1890, though this right has been narrowly interpreted.[45] Professor William Prosser

---

[40] Google is currently challenging France's authority to compel such a broad request. *See id.*

[41] Garcia v. Google, Inc., 786 F.3d 733, 745 (9th Cir. 2015).

[42] A bill recognizing a right to be forgotten has, however, been introduced in the Massachusetts state legislature. 2015 Massachusetts House Bill No. 1356, Massachusetts One Hundred Eighty-Ninth General Court.

[43] Garcia at 733.

[44] *Id.*

[45] Chelsea E. Carbone, *To Be or Not to be Forgotten: Balancing the Right to Know with the Right to Privacy in the Digital Age*, 22 Va. J. Soc. Pol'y & L. 525, 555 (2015).

later described invasion of privacy as four separate but related torts: unreasonable intrusion upon seclusion of another, publicity that places another in a false light before the public, public disclosure of embarrassing private facts about another, and appropriation of another's name or likeness.[46]

Further, much of individual personal data is currently protected under various privacy laws at both the state and federal levels. Washington State, for example, has implemented a data breach notification law, codified in Chapter 19.255 RCW. This law describes when entities must notify customers of data breaches, and defines when and how these entities may subsequently be liable thereunder.[47]

The F.T.C., in turn, enforces the privacy provisions in many federal privacy laws, including: the Fair Credit and Reporting Act, 15 U.S.C. §§ 1681-1681(u); the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108; the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506; the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6827; and the Identity Theft Assumption and Deterrence Act, 18 U.S.C. § 1028.[48] Furthermore, two new data privacy acts—the Consumer Privacy Bill of Rights and the Data Security Breach Notification Act of 2015—are currently under development, and could one day be enacted into law. If enacted, the Consumer Privacy Bill of Rights "would govern the collection and dissemination of consumer data,"[49] while the Data Security Breach Notification Act of 2015 would replace state data breach notification laws and "require companies to secure the personal data they collect and

---

[46] Joe Dickerson & Associates, LLC v. Dittmar, 34 P.3d 995, 1000 (Colo. 2001).

[47] RCW §§ 19.255.010-.020.

[48] *Overview of Statutory Authority to Remedy Privacy Infringements*, Electronic Privacy Information Center (last visited Nov. 8, 2015), available at epic.org, https://epic.org/privacy/internet/ftc/Authority.html.

[49] Andrew Lustigman and Adam Solomon, *An overview and the impact of the Consumer Privacy Bill of Rights*, Inside Counsel (Mar. 12, 2015), available at http://www.insidecounsel.com/2015/03/12/an-overview-and-the-impact-of-the-consumer-privacy.

maintain about consumers and to provide notice to individuals in the event of a breach of security involving personal information."[50]

C. The Right to be Forgotten in the United States: Balancing First Amendment Protections

Scholars debate whether and how a right to be forgotten could translate to United States law, and specifically how it would be balanced against First Amendment protections. Some suggest that, even if such a right is implemented, its reach will be limited. For example, Meg Ambrose of Georgetown University's Communication, Culture & Technology Program has argued that such a right would be limited and "apply only to data voluntarily submitted and deletion would require legislative action to establish an implied-in-law covenant in contracts between data controllers and data subjects."[51]

Other scholars suggest that such a right could pose problematic threats to free speech if implemented. As another example, Neil M. Richards of Washington University in St. Louis suggests that a strong form of the right to be forgotten, such as a tort right to censor the media, is an unconstitutional threat to free speech, while a more limited right that resembles an ordinary commercial regulation of the data trade may be constitutional—but pose other problems.[52]

The First Amendment does not protect all forms of speech. Courts have held that speech that impinges upon an individual's right to privacy, is obscene, or falsely associates one with a particular ideology, is not protected.[53] In determining whether a

---

[50] Jason C. Gavejian, *The Data Security and Breach Notification Act of 2015*, National Law Review (Mar. 31, 2015), available at http://www.natlawreview.com/article/data-security-and-breach-notification-act-2015.

[51] Carbone, *supra* note 45. (*quoting* Meg Leta Ambrose, *Speaking of Forgetting: Analysis of Possible non-EU Responses to the Right to be Forgotten and Speech Exception*, 38 TELECOMM. POL'Y 800, 805 (2014)).

[52] *See* Neil M. Richards, *Why Data Privacy Law is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501, 1531-32 (2015).

[53] *See* U.S. v. Alvarez, 617 F.3d 1198, 1214 (9th Cir. 2010); Action for

form of speech invades a person's right to privacy—and is therefore not protectable—courts may consider the truthfulness of the information, whether it was legally obtained, the newsworthiness of the information, and its significance to the public.[54]

Moreover, in certain circumstances, certain governmental agencies may also have the authority to regulate some forms of speech—such as speech that may be potentially offensive. For example, the FCC has the power to regulate radio and television broadcasts to promote compelling governmental interests if its means are carefully tailored to achieve those ends.[55] Thus, the limits of the First Amendment and the government's regulation thereof model similarly applicable limits for and regulation of a narrow right to be forgotten.

A narrow right to be forgotten, if enacted into law, could thus become operable in the United States insofar as it is narrowly tailored to balance consumer protection with free speech concerns. It would be best applied in this manner if administered by the FTC, the agency already charged with enforcing the privacy provisions of numerous federal laws and with the authority to prosecute companies that engage in unfair or deceptive trade practices—and thus an agency already adept at maintaining this crucial balance. That the two newly proposed federal privacy bills, the Consumer Privacy Bill of Rights and the Data Security and Breach Notification Act of 2015, designate the FTC as the enforcer of these potential laws, further demonstrates that the FTC would be equally adept at enforcing a right to be forgotten.[56]

Children's Television v. F.C.C., 58 F.3d 654, 660 (D.C. Cir. 1995); Russell L. Weaver, *Understanding the First Amendment*, 54-64 and 68-72 (5th ed. 2014); Steven H. Shiffrin and Jesse H. Choper, *The First Amendment*, 548-51 (3d ed. 2001).

[54] Russell L. Weaver, *Understanding the First Amendment*, 56 (5th ed. 2014).

[55] Action for Children's Television v. F.C.C., 58 F.3d 654, 659 (D.C. Cir. 1995).

[56] *See* Andrew Lustigman and Adam Solomon, *An overview and the impact of the Consumer Privacy Bill of Rights*, Inside Counsel (Mar. 12, 2015), available at http://www.insidecounsel.com/2015/03/12/an-overview-and-the-

Once Congress statutorily creates this right and delegates enforcement thereof to the FTC, the commission could issue removal requests to third-party sites hosting such illegally obtained information on behalf of consumers affected by data-breached companies. The right would remain narrowly tailored: takedown notices could only be issued for information illegally obtained after a company in violation of the Federal Trade Commission Act suffers a data breach. That is, the FTC would only be authorized to provide such a remedy when a hack results from deficient cybersecurity measures that violate the FTCA. This is so because to allow such a remedy in other circumstances—such as for a data hack that is not the result of an FTCA violation—oversteps the FTC's prosecutorial authority.

FTC enforcement would benefit both individual victims and companies obliged to follow removal requests. Such enforcement would benefit individuals because they can expect that their personal information will in fact be removed when requests are issued under this particular legal authority; this is not the case with requests now issued under the DMCA. Currently, the DMCA does not apply to such personal information; as such, requests issued thereunder may not prove successful. Because the right would be enforceable only by the FTC, enforcement would also benefit companies obliged to fulfill removal requests. Thus companies would likely not receive nearly as many takedown requests as in Europe, where the right is privately enforceable. Thus, compliance with such enforcement actions would likely not impose additionally burdensome operational expenses on affected companies.

---

impact-of-the-consumer-privacy (last visited Feb. 14, 2016); Jason C. Gavejian, *The Data Security and Breach Notification Act of 2015*, National Law Review (Mar. 31, 2015), available at http://www.natlawreview.com/article/data-security-and-breach-notification-act-2015.

CONCLUSION

When large corporations suffer data breaches and their customers' personal information is compromised, those customers are left vulnerable. As evidenced in the Ashley Madison hack, victims are left with little recourse with which to truly recover. The meager financial payout victims may receive in a class action settlement[57] is almost certainly not enough to "make whole" a person who must suffer the effects of identity theft or a ruined reputation for many years. Such a remedy thereby subverts the purpose of tort law because a victim is not made completely whole. However, authorizing the FTC to compel the removal of such unlawfully obtained personal information would allow hack victims to re-privatize their personal information, and thus make them more truly whole. Ultimately, such a solution better satisfies the purpose of tort law.

PRACTICE POINTERS

- Review data storage policies. They should indicate that when customer data is "deleted", it must be removed from every storage location and effectively overwritten so that it is no longer retrievable in its original form.
- Ensure that your company actually follows its own privacy policies, and that it does not promise more data protections than it actually implements. For example, if your company promises to delete customer data upon request, ensure that that data is actually deleted. Be sure to communicate this need to managers who implement data security measures.
- In the event of a data breach, ensure that appropriate personnel notify customers of the breach as soon as possible.

---

[57] *See generally* Charles Riley and Jose Pagliery, *Target will pay hack victims $10 million*, CNNMoney (Mar. 19, 2015), available at http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement.