Hofstra Law Review

Volume 44 | Issue 1 Article 3

1-1-2015

The Cyber Civil War

Eldar Haber

THE CYBER CIVIL WAR

*Eldar Haber**

I. INTRODUCTION

Suppose that someone hacked into your email account, stole the content of your emails, and posted them online. All of your email correspondence is now searchable in every search engine. Whomever you mentioned in any of your emails can easily find those emails by a quick search of his or her name. Most of us are terrified by such a scenario. We might not only lose and alienate our family, friends, and colleagues, but there could also be various other economic, social, and legal implications resulting from such information disclosure.[1] This scenario has recently become non-fictional. On November 24, 2014, a group of hackers identified as the "Guardians of Peace" launched a cyber-attack[2] on Sony Pictures Entertainment ("Sony"), obtaining and releasing personally identifiable information of the company's employees and their dependents—emails between employees, information about executive salaries, copies of unreleased Sony films, and other information—commonly referred to as "the Sony Hack".[3] The motivation behind the Sony Hack was linked to a new, pre-released Sony movie entitled "The Interview," which satirically presented North Korea's leader, Kim Jong-un.[4] Many U.S. government authorities attributed the Sony Hack to North Korea, but it is still unclear whether it was a geopolitical act of retaliation.[5]

---

* Postdoctoral Research Fellow, Haifa Center for Law & Technology and Cyber Forum, Faculty of Law, Haifa University. I wish to thank Deborah Housen Couriel, Amnon Reichman, and Tal Zarsky for their insightful suggestions and comments. This research was funded by the Israeli Ministry of Science, Technology and Space (MOST).

1. *See infra* text accompanying notes 2-23.

2. This Article uses the phrases "cyber-attack" and "cyber-warfare" to refer to activities centered on the use of a computer system or computer network.

3. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014), http://www.wired.com/2014/12/sony-hack-what-we-know.

4. *See* THE INTERVIEW (Columbia Pictures 2014); Zetter, *supra* note 3.

5. *See* Choe Sang-Hun, *North Korea Denies Role in Sony Pictures Hacking*, N.Y. TIMES,

The Sony Hack raises many legal questions of various aspects: Should the U.S. government protect private companies and/or their employees from cyber-warfare? Should the government respond to such attacks, and if so, how? And furthermore, what are the legal mechanisms available to Sony to enforce its rights? The Sony Hack also demonstrated and emphasized how individuals could launch an attack entirely through electronic warfare that could highly affect other individuals: a digital civil war through cyber means.

Civilians are not new to cyber-warfare. Some individuals are hackers. Others are targets. There is nothing new about that. What could gradually be changing are the potential non-monetary risks to civilians due to cyber-attacks on third parties. We should no longer only fear that someone might steal our credit card numbers, but rather, we must be concerned for our personal information, generally. Vast amounts of end-users' information is stored online and could one day be released through a cyber-attack, such as in the Sony Hack.[6] Emails, search queries, credit card numbers, purchase histories, and basically anything else we do online could be posted for everyone to search and freely view.[7] How do U.S. laws cope with this new information threat? Not well. Current legal measures are insufficient to deal with such new threats.[8] When hacks occur, even if the law enables the civilian to bring charges against the hacker, the company, the publisher, or the search

---

Dec. 7, 2014, at B2; Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Jan. 5, 2015, 12:36 PM), http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645.

6. *See* Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 976-77 (2011); Eugene E. Hutchinson, Note, *Keeping Your Personal Information Personal: Trouble for the Modern Consumer*, 43 HOFSTRA L. REV. 1149, 1151-55, 1162-63 (2015) (discussing online data collection practices and the frequency of data breaches).

7. *See, e.g.*, John E. Dunn, *Google Web History Vulnerable to Firesheep Hack*, PC WORLD (Sept. 10, 2011, 11:19 AM), http://www.pcworld.com/article/239826/google_web_history_vulnerable_to_firesheep_hack.html (discussing a hacking tool that can be used to access victim's Google web history); Dan Goodin, *Ashley Madison Hack Is Not Only Real, It's Worse Than We Thought*, ARSTECHNICA (Aug. 19, 2015), http://arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought (discussing the hack of the website Ashley Madison, which resulted in the publication of intimate data and personal information including credit card data, transaction history, and email addresses for more than 30 million accounts); Laurie Segall, *Hackers Expose Ashley Madison CEO's Emails*, CNNMONEY (Aug. 20, 2015), http://money.cnn.com/2015/08/20/technology/ashley-madison-hack-emails (discussing the hack of emails).

8. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterence in Cyberspace*, 25 HARV. J.L. & TECH. 431, 488-89 (2012); Valerie Richardson, *Hacking Victims Have Few Options as First Amendment Protects Media Disclosures*, WASH. TIMES, (Dec. 24, 2014), http://www.washingtontimes.com/news/2014/dec/24/hacking-first-amendment-open-private-email-to-publ/?page=all.

engines that link to the misappropriated information, it will not cease the dissemination of this information. The answer could possibly emerge from a relatively new legal framework that has developed in the European Union ("EU"), known as the "right to be forgotten."[9]

In the last few years, the EU discussed the right to be forgotten as part of a new General Data Protection Regulation ("GDPR") regime.[10] It refers to "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes."[11] Narrowly, it is a right to prevent people from knowing something about others—a right to control what the Internet knows, essentially. But even prior to legislative enactment, the spirit of the right to be forgotten reigns over EU courts decisions due to the European Data Protection Directive.[12] On May 13, 2014, the Court of Justice of the EU held that search engine operators are responsible for their processing of personal data appearing on web pages published by third parties.[13] Thus, the right to be forgotten is alive and kicking in Europe under the current version of the European Data Protection Directive.

The Sony Hack should raise the possibility of implementing a right to be forgotten anywhere. If indeed we are all becoming targets of cyber-attacks, which could lead to the revelation of personal information, then free speech might take a step back, as people will become more hesitant to share their information. But enforcing the right to be forgotten is problematic. It is complex, costly, creates higher barriers of market entry, leads to possible manipulation and fragmentation of search results, and is not necessarily applicable in many situations.[14] But mainly, it leads to undesired levels of Internet censorship, also endangering free speech.[15] Moreover, it does not solve the most important problem, as it mostly deals with personal information posted online which is outdated or no longer relevant.[16] This calls for a different solution that grants a right to remove *non-newsworthy* content that was *unlawfully* obtained. Under this proposal, each data holder will be obliged to implement

9. *See infra* Part V.A.

10. *See infra* Part V.A.

11. European Commission, *A Comprehensive Approach on Personal Data Protection in the European Union*, at 8, COM (2010) 609 final (Apr. 11, 2010).

12. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 42 [hereinafter Directive 95/46/EC].

13. Case C-131/12, Google Spain SL v. Agencia Española de Proteccion de Datos (AEPD), 2014 EUR-Lex CELEX 62012CJ0131 ¶¶ 21-41 (May 13, 2014).

14. *See infra* notes 213-18 and accompanying text.

15. *See infra* notes 218-19 and accompanying text.

16. *Google Spain SL*, 2014 EUR-Lex CELEX 62012CJ0131 ¶¶ 93-94.

technological measures to identify information (for example, a digital fingerprint). If someone illegally obtained your non-newsworthy information, then you can file a complaint with law enforcement agencies, and request the removal of the content and any connecting links. Under a court order, Online Service Providers ("OSPs") will be required to delete such information and/or links to it. While this is not a perfect solution, it would be the best enforceable mechanism for removing online content that was stolen through a cyber-attack.

This Article examines the new informational threat to civilians in cyberspace and proposes a modest solution. It proceeds as follows: Part II examines the two traditional roles individuals play in cyberspace—attackers and potential targets.[17] Part III describes new threats of cyber-warfare to civilians—the dissemination of personal data online.[18] Part IV analyzes the current legal measures that civilians could use.[19] Part IV also argues that current legal measures are insufficient in aiding civilians to face the new informational threat.[20] Part V discusses the need for a forgetful Internet by introducing and discussing the EU's right to be forgotten.[21] While the right to be forgotten, as accepted in the EU, is inadequate and should not be adopted in the United States in its current state, a newly proposed framework, which could aid civilians to better deal with the new cyber threat, is offered in this Article.[22] Finally, Part VI summarizes the discussion and raises further concerns about the future of the Internet.[23]

II. THE ROLE OF CIVILIANS IN CYBER-WARFARE

There are three main ways states are vulnerable to cyber-attacks.[24] The first is governmental and military. Much like the kinetic world, states could encounter a cyber-attack on their governmental and military infrastructures.[25] The second is industrial. Perhaps differently from the kinetic world, private companies could be attacked by other entities,

17. *See infra* Part II.
18. *See infra* Part III.
19. *See infra* Part IV.
20. *See infra* Part IV.
21. *See infra* Part V.
22. *See infra* Part V.
23. *See infra* Part VI.
24. *See* George R. Lucas, Jr., *Privacy, Anonymity, and Cyber Security*, 5 AMSTERDAM L.F., Spring 2013, at 107, 107 (2013).
25. *See id.* at 108; Gordon Lubold & Damian Paletta, *Pentagon Sizing Up Email Hack of Its Brass*, WALL STREET J. (Aug. 7, 2015, 7:16 PM), http://www.wsj.com/articles/pentagon-sizing-up-email-hack-of-its-brass-1438989404 (reporting email hack of Pentagon officials).

whether by other nations, competitors, or even individuals.[26] The third relates to individuals. Individuals are involved in cyber-attacks as both attackers and potential direct targets.[27]

There is almost nothing new about the first two types of cyber-warfare. States have used cyber-attacks against other states,[28] and perhaps against companies.[29] Companies are many times attacked by hackers.[30] Along the way, individuals have entered the digital battlefield. Some individuals play the role of attackers, whether actively or passively, and some are targets.[31] But the role of the civilian in cyber-warfare, and the nature of the attacks against them, might currently be changing. At first, civilians were usually a target of cyber-crimes, either by serving as a proxy in a cyber-attack, usually through a Distributed Denial of Service ("DDoS") or when someone obtained their personal information, such as passwords or credit card numbers.[32] Today, civilians could become victims of cyber-attacks and cyber-warfare against the government, the industry, or even against themselves as individuals.[33] Thus, civilians should now fear cyber-attacks in a different manner—not only can their personal computer be attacked, hacked, and/or hijacked, but they could also suffer devastating harm from attacks on third parties.[34] It is no longer merely fear of monetary implications;

---

26. *See* RILEY WATERS, HERITAGE FOUND. NO. 4289, ISSUE BRIEF: CYBER ATTACKS ON U.S. COMPANIES IN 2014, at 2-4 (2014), http://thf_media.s3.amazonaws.com/2014/pdf/IB4289.pdf (listing private company hacks in 2014 by individuals, as well as state actors); Kim Zetter, *Ashley Madison Leak Reveals its Ex-CTO Hacked Competing Site*, WIRED (Aug. 24, 2015, 6:06 PM) http://www.wired.com/2015/08/ashley-madison-leak-reveals-ex-cto-hacked-competing-site (reporting that a former Ashley Madison executive hacked a competing website).

27. *See infra* Part II.A–B.

28. *See* Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, ARSTECHNICA (June 1, 2012, 6:00 AM), http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it.

29. The Sony Hack represents such an example. U.S. government officials stated on various accounts that the North Korean government is behind the attack. *See* Grisham, *supra* note 5. However, it is still unclear whether these accusations are correct. *See* Kim Zetter, *The Evidence That North Korea Hacked Sony Is Flimsy*, WIRED (Dec. 17, 2014), http://www.wired.com/2014/12/evidence-of-north-korea-hack-is-thin.

30. *See* WATERS, *supra* note 26.

31. *See infra* Part II.A–B.

32. *See infra* notes 50-56 and accompanying text; Part III.

33. There could be a difference between the levels of threats to civilians online. For example, civilians who do not engage, or engage less, in online activities are statistically less vulnerable than civilians who are more active online. Moreover, civilians from traditionally disadvantaged classes, such as women and people of color, could be more subject to some forms of cyber-attacks due to "anonymous mobs," which come together to victimize and subjugate vulnerable people. *See generally* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

34. For example, the hack of the Ashley Madison website revealed the first and last names of users, partial credit card data, phone numbers, transaction history, email addresses, PayPal account information, and other forms of personal information for more than 30 million users. *See* Goodin,

attacks on third parties could potentially reveal personal data and jeopardize their privacy rights and online liberties.[35]

Thus, although civilians have been a part of cyber-warfare for a long time, they only played a relatively small role until recently.[36] This is about to change. The vulnerability of civilians could play an important role in future cyber-warfare. Furthermore, if civilians' role as targets continues to increase, it could create a global cyber civil war. This fear is still premature, however. Before analyzing the new possible role of civilians in cyber-warfare, and the possibility of such a cyber civil war, a short, but nonetheless important, taxonomy must take place. This Part outlines the different roles of individuals in cyber-warfare and examines their new role as victims.[37]

A. Individuals as Attackers

Individuals engage in cyber-warfare by way of two main methods: as hackers or as proxies.[38] Many individuals are hackers. They operate either by themselves or through a group of people.[39] While the result of cyber-attacks might be similar in some cases, there are various types of hackers with various motives.[40] Some hackers are hired by the government,[41] some by companies,[42] and others act alone.[43] In the category of potential attackers, there are "Black Hat Hackers," who are

---

supra note 7. Data about the intimate details of individuals was also exposed, such as clandestine affairs and sexual predilections. *See id.*

35. *See id.*

36. *See infra* Part II.B.

37. *See infra* Part II.A–B.

38. For more on the increasing role of civilians in cyber-warfare, see generally Logan Liles, *The Civilian Cyber Battlefield: Non-State Cyber Operators' Status Under the Law of Armed Conflict*, 39 N.C. J. INT'L L. & COM. REG. 1091 (2014).

39. For examples of hacker groups and individual hackers, see Abhishek Awasthi, *Top Ten Most Infamous Hackers of All Time*, TECHWORM (Sept. 15, 2015), http://www.techworm.net/2015/09/top-ten-most-infamous-hackers-of-all-time.html; Elise Viebeck, *Three Hacking Groups You Need to Know*, HILL (Feb. 23, 2015, 6:11 PM), http://thehill.com/policy/cybersecurity/233552-three-hacking-groups-you-need-to-know.

40. Generally, there are six primary categories: addiction, curiosity, boredom, power, recognition, and politics. *See* Q. Campbell & David M. Kennedy, *The Psychology of Computer Criminals*, *in* COMPUTER SECURITY HANDBOOK 12-2 (Seymour Bosworth et al. eds., 6th ed. 2014).

41. Shane Huang, *Proposing a Self-Help Privilege for Victims of Cyber Attacks*, 82 GEO. WASH. L. REV. 1229, 1234 (2014) (arguing that the Chinese government sponsored hackers to conduct cyber-attacks).

42. "Spy Hackers" are hackers hired by corporations to infiltrate the competition and steal trade secrets. *See* Robert Siciliano, *7 Types of Hacker Motivations*, MCAFEE (Mar. 16, 2011), http://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations (exploring seven types of hackers and dividing them into "good" and "bad" guys).

43. *Id.*

usually simply referred to as "hackers."[44] These hackers usually break into networks or computers, or create computer viruses for destructive purposes or financial gain.[45] They are individuals with purely personal or criminal motives.[46] The second type of attacker is a "Hacktivist"[47]—motivated mostly by politics, religion, or to expose wrongdoing in a strategy to exercise civil disobedience.[48] Third, and finally, there are attackers that merely "hack back," where they are hacking in reaction to other hackers.[49]

Another form of cyber-attack occurs through "hijacking."[50] In this form of attack, individuals attack without realizing it.[51] The hacker creates a network of "botnets" by infecting a large amount of computers.[52] These "zombie" computers can be used to send spam, steal passwords or valuable financial information, or display ads.[53] But the botnet operator can also use the zombie computers for cyber-attacks.[54] It will usually occur through a DDoS attack, where a virus compromises end-users' computers and the attacker hijacks their computers to flood a target with too much data for it to handle.[55] Therefore, the individual's computer could actually engage in a cyber-attack without his knowledge.

B. Individuals as Targets

The digital environment, much like the kinetic world, has its share of crime. Individuals are often victims of various cyber-crime activities, such as, identity theft and identity fraud.[56] There are vast amounts of online frauds that often succeed.[57] Most of these attacks are directed

---

44. These hackers are sometimes referred to as "crackers." *See id.*

45. *Id.*

46. *See* George O'Malley, *Hacktivism: Cyber Activism or Cyber Crime?*, 16 TRINITY C. L. REV. 137, 140 (2013).

47. *Id.*

48. *Id.*

49. *See* Paul Rosenzweig, *International Law and Private Actor Active Cyber Defensive Measures*, 50 STAN. J. INT'L L. 103 (2014) (defining and describing "back hacks").

50. Josh Wepman, *Definition of Computer Hijack*, EHOW, http://www.ehow.com/about_6465909_definition-computer-hijack.html (last visited Nov. 22, 2015).

51. *See, e.g.*, Huang, *supra* note 41, at 1235-36.

52. *See id.*

53. *See id.*

54. *See id.*

55. *See id.* For more on DDoS attacks and legal responsibility, see generally Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23 (2006).

56. *See generally* JOHN Q. NEWMAN, IDENTITY THEFT: THE CYBERCRIME OF THE MILLENNIUM (1999) (describing and providing examples of various methods of identity theft).

57. *See Common Fraud Schemes*, FBI, https://www.fbi.gov/scams-safety/fraud/internet_fraud (last visited Nov. 22, 2015).

against civilians.[58] These are typically the classic (mostly) monetary attacks.[59] Think of it as robbery in the digital age. Lately, a new form of indirect cyber-attack through third parties has emerged, which could be no less harmful for civilians than the classic direct monetary attacks.[60]

There are two main forms of indirect cyber-attacks on civilians: attacks on critical infrastructure[61] and attacks targeted at obtaining personal data.[62] To illustrate the first, consider a cyber-attack that shuts down an electrical grid, causing millions of Americans to live without electricity for a few days.[63] Apart from experiencing major inconvenience, those individuals might be harmed physically, emotionally, and financially, as a lack of electricity could affect various aspects of their lives. They might not be able to purchase food or medicine, they could suffer financial losses, or they may experience countless other consequences. This illustrates the need to protect critical infrastructure from any malfunction or attack, including through digital means.[64]

The second form of indirect attacks target data, both for monetary and non-monetary purposes.[65] Usually, attackers will launch the attack on either governmental agents or commercial entities that possess data about civilians.[66] Monetary reasons are behind the "classic" attacks,[67]

---

58. *See id.*

59. *See id.*

60. *See infra* notes 63-75 and accompanying text.

61. *See generally* Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319 (2013) (discussing cybersecurity threats that compromise critical infrastructure). Critical infrastructure in the United States is defined as follows: "[S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 42 U.S.C. § 5195c(e) (2012).

62. *See generally* WATERS, *supra* note 26 (listing cyber-attacks on U.S. companies in 2014 that predominately focused on the theft of customer's personal data).

63. In August 2003, an electrical blackout affected millions of people across several U.S. states. Joe D. Whitley et al., *Homeland Security, Law, and Policy Through the Lens of Critical Infrastructure and Key Asset Protection*, 47 JURIMETRICS 259, 269 (2007). Transportation, emergency services, information, and telecommunications began to fail. *See id.*

64. For more on the importance of protecting critical infrastructure, see, for example, JOHN D. MOTEFF, CONG. RESEARCH SERV., RL30153, CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION 1-2, 2 n.6 (2014), http://www.fas.org/sgp/crs/homesec/RL30153.pdf, and Zhang, *supra* note 61, at 322-23.

65. *See* WATERS, *supra* note 26, at 1-5; Zetter, *supra* note 3.

66. *See* Huang, *supra* note 41, at 1233-34. It is obvious that hackers can obtain information through a direct attack on a home computer. However, it is far more efficient to hack into a data center and acquire data on multiple users than to hack each user separately. For example, as discussed, the hack of the website Ashley Madison resulted in the theft of personal information for over 30 million users. *See* Goodin, *supra* note 7.

67. For example, a cyber-attack on Target caused leakage of 40 million credit card numbers.

but non-monetary reasons are also part of the game.[68] For example, if someone hacks into Google, he might steal your entire search history and any data stored on Google drives, as well as your email correspondence through your G-mail account.

The target in critical infrastructure attacks is not the civilian.[69] Although individuals are potentially harmed, attacks against critical infrastructure are usually a form of national cyber-warfare.[70] Sony was likely the target more so than its employees were, and thus it was not necessarily much different from a critical infrastructure attack.[71] The difference between the two forms of attack lies mainly within the outcome. Indeed, both incidents could be harmful for civilians, but the nature of the harm is different.[72] In critical infrastructure attacks, the fear is mostly physical harm.[73] In the second form of attack, the fear is both financial and personal.[74] But, the nature of the second form of attack is also changing.

III. THE NEW THREAT: PERSONAL INFORMATION

The government holds enormous amounts of information on its citizens (and likely on non-citizens, as well).[75] Specifically, governmental agencies hold taxation information, social security numbers, health records, and other sensitive data.[76] We recently learned from Edward Snowden's revelations that the government knows even more about us than we thought.[77] When we discovered that George

---

See Michael Riley et al., *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

68. Hackers are often motivated by religious or political beliefs and attempt to create fear and chaos, while others attack with military objectives, among other reasons. *See* Siciliano, *supra* note 42.

69. *See* Shackelford & Andres, *supra* note 6, at 978-80.

70. *See id.* at 978-80, 1004-05.

71. *See* Zetter, *supra* note 3.

72. *See* Shackelford & Andres, *supra* note 6, at 1004-05.

73. *See id.* at 978-80.

74. *See* Huang, *supra* note 41, at 1235-36.

75. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 756, 766-82 (2014) (discussing methods of collection information from both citizens and non-citizens of the United States by the government and the type of information collected).

76. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R-C.L. L. REV. 435, 439-51 (2008).

77. Edward Snowden, a former employee of the National Security Agency ("NSA") and perhaps the most famous whistleblower thus far, revealed two main NSA "internal" programs. The first program was a bulk collection of call record information "metadata" pursuant to orders issued by the Foreign Intelligence Surveillance Court ("FISC"). Peter Marhulies, *The NSA in Global*

Orwell's "Big Brother" prognostications were non-fictional, we were scared.[78] Now, we should be terrified. The government stores massive amounts of information that could one day be hacked, stolen, and published by anyone.[79]

The same concern applies to commercial entities. Many commercial entities store vast amounts of information gathered from, or about, their users.[80] Various types of OSPs know our search queries, the content of our emails, and have access to our files on the Cloud.[81] We allow them to obtain and use such information in exchange for their services.[82] Consider Google and its possession of data,[83] and every mobile application you have ever installed.[84] Can you recall what you agreed to when accepting the terms of use? Probably not. You likely did not even read the terms, as most people do not.[85] But you likely granted permission for the owners to listen through your microphone, trace your location, read through your emails, and take photos from your device.[86]

Perspective: Surveillance, Human Rights, and International Counterterrorism, 82 FORDHAM L. REV. 2137, 2140-41 (2012). This gathering of information is supposedly issued under section 215 of the USA Patriot Act. 50 U.S.C. § 1861 (2012); Marhulies, *supra*, at 2140-41. The second program was gathering electronic communications using two methods: PRISM and upstream collection. *See* Marhulies, *supra*, at 2140-41. Under PRISM, the NSA targets the contents of communications of non-U.S. persons reasonably believed to be located abroad and where such surveillance will result in acquiring foreign intelligence information. *See id.* PRISM is supposedly operated pursuant to section 702 of the Foreign Intelligence Surveillance Act ("FISA"). 50 U.S.C. § 1881a (2012); *see* Marhulies, *supra*, at 2140-41. Under upstream collection, the NSA gathers electronic communications, including metadata and content, of foreign targets overseas whose communications flow through American networks, supposedly pursuant to section 702 of FISA and Executive Order 12333. *See* Exec. Order No. 12333, 40 Fed. Reg. 235 (Dec. 4, 1981), as amended by Executive Order 13284 (Jan. 23, 2003), and by Executive Order 13355 (Aug. 27, 2004), and further amended by Executive Order 13470 (July 30, 2008); Marhulies, *supra*, at 2141-42. For more on NSA programs, see Donohue, *supra* note 75, at 770-76.

78. *See generally* GEORGE ORWELL, 1984 (First Plume Printing 1949); Lewis Beale, *We're Living '1984' Today*, CNN, http://www.cnn.com/2013/08/03/opinion/beale-1984-now (last updated Aug. 3, 2013, 9:22 AM).

79. *See* Cate, *supra* note 76, at 439-51.

80. *See* Hutchinson, *supra* note 6, at 1151-55.

81. *Id.* at 1152.

82. *Id.*

83. *Id.*

84. *See* Neil McAllister, *How Many Mobile Apps Collect Data on Users? Oh . . . Nearly All of Them*, REGISTER (Feb. 21, 2014, 2:28 PM), http://www.theregister.co.uk/2014/02/21/appthority_app_privacy_study.

85. One study suggests that reading all of the privacy policies you encounter would require you to take a month off from work each year. *See* Mike Masnick, *To Read All of the Privacy Policies You Encounter, You'd Need to Take a Month Off from Work Each Year*, TECHDIRT (Apr. 23, 2012, 7:04 AM), https://www.techdirt.com/articles/20120420/10560418585/to-read-all-privacy-policies-you-encounter-youd-need-to-take-month-off-work-each-year.shtml.

86. *See* Nina Pineda, *Popular Apps that Spy on You*, WABC-TV (Dec. ,22, 2014), http://7online.com/technology/popular-apps-that-spy-on-you/447016.

It is scary enough that these companies might use your information themselves or sell it for targeted marketing, but even more terrifying is that, if these companies are hacked, your information could be released to the public online.[87]

Lately, there have been some incidents where hacking led to the release of personal information, in addition to the theft of "traditional" sensitive information, such as usernames, passwords, and credit card details usually obtained through phishing.[88] Through a cyber-attack on Apple's cloud services suite, iCloud,[89] hackers stole nude photos of celebrities and released them online.[90] This incident emphasized how anything we store online or even on our mobile devices could be breached and published one day. Bear in mind that famous individuals should be treated a bit differently here from non-famous individuals. They enjoy less privacy than the common citizen in both the kinetic and digital worlds. Although, normatively, we all deserve similar liberties, fame has its price. The Sony Hack, however, showed that anonymity is not a safeguard. Civilians could be less resilient to cyber-attacks than they once were.

Cyber security is hardly a new issue. Companies are, or at least should be, well aware that any online website or database could be breached, and thus needs protection. The level of protection required varies between different online websites, depending mainly on their risk assessment of the probability of hacking, the nature of information they possess, and their financial resources.[91] It is not much different from the kinetic world. Banks and jewelry stores will probably invest in physical security more than a local bookstore. Setting aside insurance requirements, they are all at risk of burglary, but at different levels and with different potential losses. Cyberspace is not exactly synonymous with the kinetic world. An attack stealing customers' information could

87. *See* Hutchinson, *supra* note 6, at 1152-53, 1162-65.

88. For a description of "phishing," see *Online Fraud: Phishing*, NORTON, http://us.norton.com/cybercrime-phishing (last visited Nov. 22, 2015).

89. iCloud is a storage service created by Apple, Inc. iCloud allows users to connect Apple products to each other, ensuring successful backup of their important information, such as documents, photos, notes, and contacts. iCloud is accessible from iPhones, iPads, iPod Touches, Mac computers, or any computer browser. *See iCloud: What is iCloud?*, APPLE, https://support.apple.com/kb/PH2608?locale=en_US&viewlocale=en_US (last visited Nov. 22, 2015).

90. *See* David Raven & Jess Wilson, *Jennifer Lawrence Leaked Nude Photos: Apple Launches Investigation into Hacking of iCloud*, MIRROR, http://www.mirror.co.uk/3am/celebrity-news/jennifer-lawrence-leaked-nude-photos-4155078 (last updated Sept. 23, 2014, 10:24 AM).

91. *See generally Cyber Security Planning Guide*, FED. COMM. COMMISSION, https://transition.fcc.gov/cyber/cyberplanner.pdf (last visited Nov. 22, 2015).

be harmful for the website owner, but he does not necessarily suffer direct loses comparable to the jewelry store owner.[92]

Online protection for end-users is also hardly new.[93] We are all constantly reminded to protect ourselves online, either by being wary of opening emails that can contain viruses, raising the level of security of our personal computers by implementing anti-virus software, or choosing sophisticated passwords and keeping them secure.[94] The Sony Hack did not change anything in that area. What changed is our awareness of the rising threat of the visibility of our personal information due to cyber-attacks on third parties. Even if we are cautionary online, acquire the best software, and secure our passwords, our information might be stolen from other sources. These sources might also act properly to secure your information and still be hacked. Anything can be breached. The question is what happens after someone has stolen the information and released it online. In the past, most anonymous users were probably still not concerned. They could not grasp why someone would be interested in their personal information for non-monetary purposes.[95] This is what the Sony Hack changed—the vivid possibility of finding vast amounts of our personal, non-monetary, information online. Our privacy, and perhaps more importantly, our liberty to freely use the Internet are at risk more than ever before.

IV. FACING THE NEW INFORMATION THREAT

If you did not secure your home computer sufficiently, or acted carelessly when browsing online, and someone stole data from your computer, you can only blame yourself. But what can you do when third parties are hacked and your personal information was stolen and published because of that hack? The legal analysis first calls for an understanding of the various issues that could arise from cyber-attacks

92. For companies, data breaches can cause a loss of business due to higher customer turnover, increased customer acquisition costs, and a hit to reputations and goodwill. *See* Maria Korolov, *Ponemon: Data Breach Costs Now Average $154 Per Record*, CSO (May 27, 2015, 6:22 AM), http://www.csoonline.com/article/2926727/data-protection/ponemon-data-breach-costs-now-average-154-per-record.html.

93. *See* Kevin McAleavey, *The Birth of the Antivirus Industry*, INFOSEC ISLAND (July 11, 2011), http://www.infosecisland.com/blogview/15068-The-Birth-of-the-Antivirus-Industry.html (describing the origins of the computer antivirus industry that dates back to the 1980s).

94. *See, e.g.*, *Q&A: Safe Online Banking*, BBC NEWS (Nov. 5, 2004, 3:13 PM), http://news.bbc.co.uk/2/hi/business/3986097.stm.

95. *See* Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 133 (David Buckingham ed., 2008) ("Most people believe that security through obscurity will serve as a functional barrier online. For the most part, this is a reasonable assumption. Unless someone is of particular note or interest, why would anyone search for them?").

on third parties.[96] Consider this scenario: someone hacked into a company's database, stole data, and later published it online on his own website and across the Internet on other websites. This database has photos you took, your entire log of email correspondence (for example, all emails from the last ten years), and your browsing history. Search engines, such as Google, link to the websites, and, thus, when someone searches your name, your entire database will appear in its search results.

What could civilians do in light of such threat? Legally speaking, there are a few issues that could arise.[97] There are generally four main players that could be legally liable: the hacker, the company (the entity that holds the information), the publisher (who publishes the information), and the search engines (which link to the websites).[98]

A. The Hacker

The attackers' responsibility for hacking is obvious. Under the Computer Fraud and Abuse Act ("CFAA")[99] and state computer hacking statutes,[100] hackers face criminal and civil liability.[101] Such civil liability

96. *See* Kristen Shields, Note, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 351-54 (2015).

97. The focus here is on the civilian as a target and not the company or the attacker. There are a few possible violations of legal rights here. *See id.* at 354-57. But the identity of the data holder and the nature of the data matters. For example, the government holds vast amounts of information on its citizens (and non-citizens) and could generally be liable for its disclosure. Moreover, some private parties are also required to keep some forms of information confidential. *See id.* at 357-58. Examples of these parties are attorneys, psychologists, financial institutions, and even libraries. *See, e.g., id.*; Sue Michmerhuizen, *Confidentiality, Privilege: A Basic Value in Two Different Applications*, CTR. FOR PROF'L RESP. (May 2007), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/confidentiality_or_attorney.authcheckdam.pdf; *Protecting Your Privacy: Understanding Confidentiality*, AM. PSYCHOL. ASS'N, http://www.apa.org/helpcenter/confidentiality.aspx (last visited Nov. 22, 2015); *Questions and Answers on Privacy and Confidentiality*, ALA, http://www.ala.org/Template.cfm?Section=interpretations&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15347 (last visited Nov. 22, 2015). Here, the goal is to generally analyze the *common* data holder.

98. *See infra* Part IV.A–D. A few more intermediaries could also be liable—for example, OSPs, various manufacturers, civilians acting as "zombie" computers, and even the civilian herself. But as the likelihood of such liability is low, they are excluded from current discussion. For more on the possible liability of intermediaries, see Jennifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231, 243-48 (2004); Luis de Guzman, *Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges*, 59 CATH. U. L. REV. 527, 528 (2010) (discussing the unlikelihood that zombie computer owners are liable for maintaining an under-protected computer).

99. 18 U.S.C. § 1030 (2012).

100. *See, e.g.*, ALA. CODE §§ 13A-8-112 to -113 (2012). For the updated list of all U.S. state statutes, see *Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (2015), http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx (last visited Nov. 22, 2015).

could also be imposed under state tort law.[102] The problem here is that, in many instances, the hacker is irretraceable due to "the attribution problem,"[103] or even if detected, geographically located somewhere that makes it difficult to bring him to justice.[104] In many other instances, defendants are judgment proof and, therefore, are unable to compensate victims.[105] Furthermore, even if the hacker was identified, apprehended and held liable,[106] both in criminal and civil law, the civilians' data will still remain online—the main cause of concern here. Therefore, suing the hacker may compensate the victim to some extent, but it does not generally solve the problem.

B. The Company/Information Holder

The company, which holds its users' information, could face liability under theories of tort law or contract law.[107] The company could be liable in tort on two causes of action: strict liability or negligence.[108] Strict liability, here, is unlikely, as no abnormally dangerous activity occurred.[109] That leaves negligence. Does the company owe a duty to the ultimate victim? Generally, company owners could be liable for a

101. *See* 18 U.S.C. § 1030; ALA. CODE § 13A-8-112(b)(1). There are many possible offenses: intentionally accessing a computer without authorization; exceeding authorized access of a protected computer; knowingly causing the transmission of a program, information, code, or command and, as a result of such conduct, intentionally causing damage, without authorization, to a protected computer; intentionally accessing a protected computer without authorization and, as a result of such conduct, recklessly causing damage; or intentionally accessing a protected computer without authorization and, as a result of such conduct, causing damage and loss. *See* 18 U.S.C § 1030(a).

102. Under common law, the primary cause of action will most likely be committing an intentional tort. *See* Kesan & Hayes, *supra* note 8, at 496-98. For a full list of state computer hacking statutes, see *Computer Crime Statutes*, *supra* note 100.

103. *See, e.g.*, David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SECURITY J. 323, 329 (2011); Shackelford & Andres, *supra* note 6, at 979.

104. Clark & Landau, *supra* note 103, at 329.

105. For a full list of civil law shortcomings in cyber-attacks, see Kesan & Hayes, *supra* note 8, at 469-70.

106. If the attacker is located outside the jurisdiction of U.S. criminal courts, and U.S. authorities can locate him, they can either ask the foreign jurisdiction to extradite him or alert the host nation and hope that they will pursue criminal sanctions. *Id.* at 467-69. However, many states will not necessarily extradite or prosecute cyber criminals within their borders. Moreover, the proper venue for a lawsuit would be difficult to determine due to the nature of the Internet. *See id.*; Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 6-10 (2009).

107. Kesan & Hayes, *supra* note 8, at 496-98.

108. Intentional tort is also a potential cause of action, but it is generally against the attacker, not the company. *See id.*

109. *Id.* at 482 & n.45.

negligent failure to secure their computer system.[110] But this is not necessarily the case. To hold these companies liable will require proving proximate cause.[111] Still, much like with the hacker, even if the victim could sue the company, it does not necessarily compensate him appropriately because the content will still remain available online.

Then, there is contract law.[112] At least some of our data held online is subject to contract law.[113] It would be difficult to locate a website that does not have a listed set of "Terms and Conditions."[114] Indeed, we are all familiar with the two-word phrase: "I Agree." It is usually a binding enforceable contract with the OSP, at least to some extent.[115] The contract could exist even if you do not actively click on anything and just use the service.[116] Google is an example of such an OSP. When you use Google, you agree to their terms of service, at least as long as they are reasonable.[117] It is not surprising that Google can use your data in, pretty much, any way they wish.[118] Most likely, the license agreement

110. *Id.* at 498.

111. *Id.* at 500-01.

112. *See, e.g.*, Edwards, *supra* note 55, at 52 (stating software companies are liable under contract law for data breaches). It is obvious that a case-by-case analysis will be required under such evaluation, as other forms of legal implications could arise, depending on a specific case. The Sony Hack, for example, requires an examination of the relationship between Sony employees and their employer in a sense of labor law.

113. Nearly every company website has a page displaying its "Terms of Use" to which users assent by using the website or clicking "Agree to Terms of Use," which is often upheld by the courts. *See* David R. Collins, Note, *Shrinkwrap, Clickwrap, and Other Software License Agreements: Litigating a Digital Pig in a Poke in West Virginia*, 111 W. VA. L. REV. 531, 558-66 (2009); Hutchinson, *supra* note 6, at 1165-66 (discussing the shortcomings of Terms of Use agreements); *Google Terms of Service*, GOOGLE, https://www.google.co.il/intl/en/policies/terms/regional.html (last modified Apr. 30, 2014).

114. *See, e.g.*, *Google Terms of Service*, *supra* note 113.

115. *See* Collins, *supra* note 113, at 559-60.

116. *See supra* note 113.

117. *See* Hutchinson, *supra* note 6 at 1167-69.

118. Google's potential use of users' information is vast:

> When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.
>
> Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored

will limit or disclaim all available warranties and potential liabilities against the company.[119] But even if the contract is invalid, and the company is liable, contract law does not generally aid the civilian here. After all, the issue here is not whether Google misused the information, because the information was *stolen* from the company. Moreover, contractual obligations apply to parties that are privy to the contract;[120] Google is, generally, not to blame.

C. *The Publisher*

After information is stolen, several websites can publish it online. The recent Sony Hack demonstrated this potential scenario. In the Sony Hack, several media groups published email correspondence between employees, information about executive salaries, and other delicate personal information.[121] After the Sony Hack, Sony's attorney, David Boies, sent a letter to various media groups, warning them that if they indeed possessed "stolen information" from Sony, and they intended to publish it, they might face legal repercussions.[122] In his own words:

> If you do not comply with this request, and the Stolen Information is used or disseminated by you in any manner, [Sony] will have no choice but to hold you responsible for any damage or loss arising from such use or dissemination by you, including any damages or loss to [Sony] or others, and including, but not limited to, any loss of value of intellectual property and trade secrets resulting from your actions.[123]

Does Sony have legal standing? Perhaps, but any conclusion requires further legal analysis, which is beyond the scope of this Article. The focus here is on the civilian and not the company. Mainly, beyond

---

> advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.
>
> If you have a Google Account, we may display your Profile name, Profile photo, and actions you take on Google or on third-party applications connected to your Google Account (such as +1's, reviews you write and comments you post) in our Services, including displaying in ads and other commercial contexts. We will respect the choices you make to limit sharing or visibility settings in your Google Account. For example, you can choose your settings so your name and photo do not appear in an ad.

Google Terms of Service, *supra* note 113.

119. Collins, *supra* note 113, at 548; Kesan & Hayes, *supra* note 8, at 499-500.

120. Meg Leta Ambrose, *It's About Time: Privacy, Information Life Cycles, and the Right to Be Forgotten*, 16 STAN. TECH. L. REV. 369, 375 (2013).

121. *See* Zetter, *supra* note 3.

122. Mike Fleming Jr., *Read David Boies' Legal Letter On Sony Hack Attack Coverage*, DEADLINE (Dec. 15, 2014, 10:20 AM), http://deadline.com/2014/12/sony-pictures-letter-david-boies-deadline-1201326203.

123. *Id.*

possible duties of data protection, there are two possible claims available for the civilian: invasion of privacy and intellectual property infringement.[124]

1. Privacy Torts

Privacy law has various applications. Constitutional law refers to privacy mostly as a right to protect the civilian against an overbearing and powerful government.[125] It is a right of autonomy—to "decide how to live and to associate with others."[126] Over time, new applications of privacy have emerged, beginning with Samuel Warren and Louis Brandeis who articulated the need for a "right to be let alone."[127] Their suggestion marked the emergence of the common law version of privacy and the recognition of its need.[128] Mostly, Warren and Brandeis's articulation of privacy was of a right of selective anonymity.[129] Since then, various forms of privacy rights have appeared with various levels of legal protections.[130] Privacy evolved into a tort law concept. Privacy tort law in most American jurisdictions is reiterated in the *Restatement (Second) of Torts*.[131] Accordingly, there are four possible types of privacy tort claims that can be invoked: unreasonable intrusion upon seclusion,[132] public disclosure of private facts,[133] misappropriation,[134] and false light.[135]

---

124. *See* discussion *infra* Part IV.C.1–2.

125. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

126. *See* Diane Leenheer Zimmerman, *False Light Invasion of Privacy: The Light that Failed*, 64 N.Y.U. L. REV. 364, 364 (1989).

127. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

128. Zimmerman, *supra* note 126, at 375-76.

129. *Id.* at 375-77.

130. The right to privacy has different definitions globally. In U.S. law, for example, certain aspects of the right to privacy are protected by the Fourth Amendment and by specific legal regulations, such as the Children's Online Privacy Protection Act of 1998 ("COPPA"). The right to privacy is also part of many European constitutions—for example, section 13 of the Swiss Constitution; section 10 of the German Federal Constitution; sections 3 and 6 of chapter B in the Swedish Constitution—as well as several human rights conventions, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") adopted in Rome on November 4, 1950, and declarations, such as section 12 of the Universal Declaration of Human Rights, 1948. *See* Directive 95/46/EC, 31-34; Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 281) 11, 46.

131. RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW INST. 1977); Patricia Sanchez Abril, *"A Simple, Human Measure of Privacy": Public Disclosure of Private Facts in the World of Tiger Woods*, 10 CONN. PUB. INT. L.J. 385, 389 (2011).

132. *See* Abril, *supra* note 131, at 389.

133. *Id.*

134. *Id.*

135. RESTATEMENT (SECOND) OF TORTS § 652A; Abril, *supra* note 131, at 389; *see* Ambrose,

What is most relevant here is the tort of public disclosure.[136] The tort of public disclosure applies when private and highly offensive information (to a reasonable person) is publicized without legitimate concern to the public.[137] A valid defense against such claim should rely on either consent or newsworthiness.[138] If information, stolen or not, is in the public interest, it will be protected by the First Amendment, and such information will not be protected by privacy rights.[139]

Many scholars argue that the tort of public disclosure is very weak,[140] inapplicable, or even dead.[141] For example, any newsworthy content that "the public has a proper interest in learning about" is protected speech, warranting a defense to privacy claims.[142] What will be deemed as public interest? This is hard to say. Take the Sony Hack as an example. Some of the stolen documents could be viewed as "of public concern." Perhaps these documents could reveal unlawful or unethical behavior of a very large company with many customers

---

supra note 120, at 375-76; Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 329 (1966); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

136. False light invasion of privacy is not at stake here. This tort claim arises only when the communicated data is factually untrue or when the data is true but carries a false implication. *See* Zimmerman, *supra* note 126, at 370. Defamation claims require that the claim must generally be false and, therefore, will not be applicable here. *See* Time, Inc. v. Firestone, 424 U.S. 448, 451-58 (1976); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964); RESTATEMENT (SECOND) OF TORTS § 581A; Ambrose, *supra* note 120, at 375; Zimmerman, *supra* note 126, at 370-97 (discussing false light invasion of privacy).

137. RESTATEMENT (SECOND) OF TORTS § 652D. However, note that some jurisdictions rejected the public disclosure of private facts tort. *See* Geoff Dendy, *The Newsworthiness Defense to the Public Disclosure Tort*, 85 KY. L.J. 147, 158-59 (1997); Jacqueline R. Rolfs, The Florida Star v. B.J.F.*: The Beginning of the End for the Tort of Public Disclosure*, 1990 WIS. L. REV. 1107, 1112.

138. Dendy, *supra* note 137, at 151 ("The primary two defenses to the public disclosure tort are consent and newsworthiness.").

139. The U.S. Supreme Court has discussed a relatively similar matter in the past. In *Bartnicki v. Vopper*, the Court examined what degree of protection the First Amendment provides to speech that discloses the contents of an illegally intercepted communication. 532 U.S. 514, 517 (2001). The Court examined three questions to determine whether media's use of illegally obtained information was permissible: Did the media play a part in the illegal activity? Was their access to the information obtained lawfully? And was the subject matter of the conversation a matter of public concern? *See id.* at 525; *see also* Warren & Brandeis, *supra* note 127, at 214 ("The right to privacy does not prohibit any publication of matter which is of public or general interest.").

140. Rodney A. Smolla, *Accounting for the Slow Growth of American Privacy Law*, 27 NOVA L. REV. 289, 290-91, 296-312 (2002).

141. Samantha Barbas, *The Death of the Public Disclosure Tort: A Historical Perspective*, 22 YALE J.L. & HUMAN. 171, 172 (2010); Jonathan Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Public Domain*, 55 MD. L. REV. 425, 426 (1996) ("[O]ne third of the Supreme Court and most of privacy academia have pronounced dead the more than century-old tort of public disclosure of private facts.").

142. Ambrose, *supra* note 120, at 377; *see* Time, Inc. v. Hill, 385 U.S. 374, 382-85 (1967); *see also* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 487-97 (1975) (holding that truthful publication of a rape victim's name was constitutionally protected).

worldwide. However, it might take more than that to establish a matter of public concern.

Overall, some civilians will possess a real claim against the publisher. Ordinary email correspondence with your mother is not generally newsworthy content. But once again, the legal system will not necessarily aid the civilian. Even if the publisher is culpable, bringing him to justice might be impractical.[143] And even if all this is possible, still, it will not achieve the desired purpose—permanently and expeditiously removing the stolen content from public viewing.[144]

2. Intellectual Property

Data can be copyrightable. Copyright law grants copyright protection to original works of authorship fixed in any tangible medium of expression.[145] Although registration is not a condition for copyright protection,[146] it is nonetheless necessary in order to accrue certain rights and benefits.[147] Thus, if copyright law protects the stolen data, civilians could possibly make use of its provisions to recover damages and/or even remove it.

But not all data is copyrightable, as copyright law requires originality and fixation.[148] Consider emails as an example. Emails could be copyrightable as literary works,[149] as long as they meet a certain level of originality, which necessitates independent creation plus a modicum

143. *See* Barbas, *supra* note 141, at 199-200 (arguing that the expansive definition of matters of public concern leaves few privacy plaintiffs successful); Dendy, *supra* note 137, at 158 n.77 (noting that several states do not recognize a cause of action for the publication of private facts); Mintz, *supra* note 141, at 446 ("[P]laintiffs' privacy rights rarely prevail over the public's interests, rendering the limitation on the scope of the public interest essentially theoretical and leaving plaintiffs with rare success." (footnote call number omitted)).

144. *See* RESTATEMENT (SECOND) OF TORTS § 652H (AM. LAW INST. 1977) (outlining the form of relief available in a cause of action for invasion of privacy as compensatory rather than injunctive).

145. 17 U.S.C. § 102(a) (2012). Works of authorship include literary, musical, dramatic, pantomimes, choreographic, pictorial, graphic, sculptural, motion pictures, audiovisual, and architectural works, as well as sound recordings. *See* § 102(a)(1)–(8). Ideas, procedures, processes, systems, method of operations, concepts, principles, and discoveries are not protected. § 102(b).

146. Registration in the United States is codified at 17 U.S.C. §§ 408–412 (2012).

147. *See* Erin Hogan, *Survey, Approval Versus Application: How to Interpret the Registration Requirement Under the Copyright Act of 1976*, 83 DENV. U. L. REV. 843, 843 (2006) ("Although an original work is protected the moment it is fixed in a tangible form, certain rights and benefits accrue only upon copyright registration." (footnote call number omitted)). For example, in a civil action, registration or preregistration of a domestic work is a necessary requirement in order to sue for copyright infringement and to claim attorney's fees and statutory damages. *See* 17 U.S.C. §§ 411(a), 412.

148. *See supra* note 147 and accompanying text.

149. *See* 17 U.S.C. § 101 (defining copyrightable "literary works" as works "expressed in words . . . regardless of the nature of the material objects . . . in which they are embodied").

of creativity.[150] Whether emails are "creative" enough to meet the threshold of originality is debatable, but in most cases they are. In those cases, publishing emails, or a portion of them, could be considered copyright infringement.

Three main issues arise from using copyright as a tool for compensating victims and/or removing content. First, as mentioned, the subject matter is not necessarily copyrightable. It depends on the nature of the data that was stolen and published online. Thus, not every civilian could acquire the benefits of copyright law, that is, use it for data removal and possibly receive damages.[151] Second, the civilian is not necessarily the copyright owner of the work. If a stolen photo from your database was photographed by someone else, then you will be excluded from copyright protection.[152] Third, even if the subject matter is copyrightable and the civilian is its rightful owner, she would be required to pre-register the work to sue for copyright infringement.[153] Even assuming compensation is feasible, it would still prove insufficient to solve the problem. A different claim could aid in solving the problem, even if the work is not registered. This is due to the notice-and-takedown provision set by the Digital Millennium Copyright Act ("DMCA").[154] Under notice-and-takedown, even if the work is not registered, a copyright owner can request to remove online content from the publisher.[155] However, the DMCA also sets a timing requirement if the OSP receives a counter-notification from the allegedly infringing party.[156] In that case, the copyright owner must file suit within ten to fourteen days to prevent the OSP from replacing the material.[157] If not registered, the lawsuit will be subject to dismissal.[158]

---

150. *See, e.g.*, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991) (noting that the requisite level of creativity in copyright law is extremely low); John Muller & Co. v. N.Y. Arrows Soccer Team, Inc., 802 F.2d 989, 990 (8th Cir. 1986) (affirming a refusal to register a logo which lacked the minimal creativity necessary to support a copyright).

151. *See infra* text accompanying notes 170-77. For more on the removal process of infringing copyrighted materials, see *infra* note 170.

152. 17 U.S.C. § 201(a) (granting copyright protection only to author or authors of a work).

153. Under U.S. copyright law, no civil action for infringement of the copyright shall be instituted until preregistration or registration of the copyright claim has been made. *See* 17 U.S.C. § 411(a).

154. Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended at 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001 (2012)).

155. 17 U.S.C. § 512.

156. *See* Schenck v. Orosz, No. 3:13-CV-0294, 2013 WL 5963557, at *1 (M.D. Tenn. Nov. 7, 2013).

157. *See id.*

158. Such decision will depend upon the jurisdiction. Some jurisdictions adopted a "registration approach" whereas copyright is "registered" only when the Copyright Office passes on the material submitted by the applicant. Others have adopted an "application approach," under

Using copyright law to fight the release of unlawfully obtained data is problematic. Although it could be useful in some cases, it is fairly limited to original (and creative) works that were created by the civilian.[159] Moreover, even if civilians can make use of the DMCA's notice-and-takedown provisions, the data could orbit the digital environment for a long time before its removal, and it might be viewed by others before being taken down.[160] Still, it seems like the best current mechanism for quickly removing at least some types of content.

D. The Search Engine

Search engines are generally not directly liable for the hack or its consequences.[161] They only link to the website and, therefore, could only possibly face secondary liability.[162] With respect to torts, if the search engine will be deemed an "interactive computer service"[163] under the Communications Decency Act ("CDA"),[164] it will be immunized from civil liability for defamatory material.[165] Such providers will not be "treated as the publisher or speaker of any information provided by another . . . ."[166] But, moreover, search engines will most likely be exempt from liability for linking to the websites. Regarding copyright infringement, they are generally exempt from liability if they implement certain enforcement methods, such as notice-and-takedown mechanisms, and identify subscribers who allegedly infringed upon copyrighted content after receiving a subpoena.[167] Thus, it is difficult for civilians to receive damages from the search engine.

But can they nonetheless request removal of the links to the content? Much like in the case of the publisher, the civilian can use the

---

which the copyright is "registered" upon submitting the requisite fee, deposit, and application. *See id.* at 1106-07.

159. *See* Ambrose, *supra* note 120, at 375 (arguing that although copyright could be very useful for preventing the replication of content created by the information subject, it only "reaches the creative aspects of that work and does not reach information created by another related to the subject").

160. *See id.* at 394-95.

161. *See* Seema Ghatnekar, *Injury by Algorithm: A Look into Google's Liability for Defamatory Autocompleted Search Suggestions*, 33 LOY. L.A. ENT. L. REV. 171, 185-88 (2013).

162. *See id.*

163. An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." 47 U.S.C. § 230(f)(2) (2012).

164. Pub. L. No. 104-104, 110 Stat. 133 (1996) (codified at 47 U.S.C. §§ 223, 230 (2012)).

165. *See* Ghatnekar, *supra* note 161, at 189.

166. *See* 47 U.S.C. § 230(c)(1). For a discussion on whether Google is an "interactive computer service" under the CDA, see Ghatnekar, *supra* note 161, at 194-201.

167. *See* 17 U.S.C. § 512(g)(1), (h)(5) (2012).

DMCA's notice-and-takedown provision for removing the content.[168] But other than copyrighted materials, removing non-copyrightable content is not an easy task. Take Google U.S.'s removal policy as an example.[169] Say you wish to remove a link from Google search results. Typically, Google will respond by referring you to "the website owner (webmaster) and ask them to remove the information."[170] Generally, Google will intervene only when "sensitive personal information" is involved.[171] Information is deemed sensitive when its disclosure, if made public, puts someone at greater risk for "identity theft, financial fraud, and other harms."[172] More specifically, Google refers to national identification numbers, bank account numbers, credit card numbers, images of signatures, and offensive images.[173] Thus, the current U.S. legal regime will most likely protect search engines in their refusal to remove links to the data, or at least, to any data that does not enjoy copyright protection or falls into narrowly predefined categories.

Civilians can use the legal system to recover damages. However, it might not be an easy task, and they will not necessarily win. But, moreover, it will only grant insufficient damages *ex post facto*.[174] The problem here is different. The damage is not monetary in the classical sense. When everyone in the world is able to view your personal data, there could be many negative consequences that are not necessarily monetary. As we saw, only a valid copyright infringement claim and/or limited predefined conditions set by the OSP will allow an individual to remove online content. This is absurd, of course. Even if some data will be copyrightable, it will not cover all types of data. What is missing from the current legal system is an effective remedy for civilians—an immediate removal of the content and erasing of any traces of it—the "right to be forgotten" which exists, to some extent, in the EU.[175]

---

168. The DMCA allows a person to send a statutorily compliant notice, which notifies the OSP of the copyrighted material and requests its removal. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or 'Chilling Effects?' Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621, 624-25, 625 n.12 (2006).

169. *Remove Information from Google*, GOOGLE, https://support.google.com/websearch/troubleshooter/3111061?hl=en (last visited Nov. 22, 2015). For an empirical study of Google's removal of content policy, see generally Jane R. Bambauer & Derek E. Bambauer, *Vanished*, 18 VA. J.L. & TECH. 137 (2013).

170. *Remove Information from Google*, *supra* note 169.

171. *Id.*

172. *Removal Policies*, GOOGLE, https://support.google.com/websearch/answer/2744324 (last visited Nov. 22, 2015).

173. *Id.*

174. Kesan & Hayes, *supra* note 8, at 474.

175. *See infra* Part V.A.

V. THE NEED FOR A FORGETFUL INTERNET

The Internet rarely forgets. Once information is accessible online, it could forever orbit in the digital atmosphere.[176] Thus, in the digital world, we might have lost the ability to be forgotten. Every picture posted, comment made, or video uploaded is there to stay and for others to see. Search engines make this information easily accessible to the public. Isn't it great to live in an ever-knowing society with endless information and possibilities of knowledge? Not always. Constantly being under a magnifying glass could prove harmful to our opportunities in the future. For example, a picture of a teenager drinking at a party could affect her career opportunities for the rest of her life.[177] A never-forgetting Internet could lead to "Reputation Bankruptcy."[178] We are in a conflict between the thirst to know and the fear of consumption. The EU recently recognized the need for a forgetful Internet by articulating a right to be forgotten.[179] This Part will analyze the right to be forgotten in the EU while arguing that such a right is overbroad, and among its many flaws, poses a threat to the future of the Internet.[180] However, as our liberty to freely use the Internet should be preserved, other, more limited solutions could suffice.

A. The Right to Be Forgotten

The EU recognized the importance of protecting end-users long before the Sony Hack. The EU examined the right to privacy and found it as insufficient to the extent it does not protect the interests of end-users in controlling their information online.[181] Under this view of privacy, end-users are in need of a legal right which will enable them to decide what personal information could be posted online or available via search engines. This gave birth to a proposed new right to be forgotten.

The right to be forgotten originates from the French "right of oblivion" (*le droit à l'oubli*) which censors the facts of an ex-criminal's

176. *See* Ambrose, *supra* note 120, at 394-96.

177. For an example of the possible effect of an online photo on career opportunities, see Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG., July 26, 2010, at 30, 32.

178. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 228-29 (2008).

179. *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. 88, 91 (2012); *infra* Part V.A.

180. *See infra* Part V.A–B.

181. *See* Viviane Reding, Vice President, European Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Speech to the Innovation Conference Digital, Life, Design 5 (Jan. 22, 2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm.

conviction and incarceration, designed to allow rehabilitation.[182] The right to be forgotten has been debated for more than two years in the EU as part of the GDPR.[183] Proposed by Viviane Reding, the European Commissioner for Justice, Fundamental Rights, and Citizenship,[184] the right to be forgotten is designed to enable the data subject to "obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child." The right is available under the following circumstances: (1) when the data is no longer necessary in relation to the original purposes;[185] (2) when the data subject withdraws consent or when the storage period consented to has expired, and there is no other legal ground for processing of the data;[186] (3) when the data subject objects to the processing of personal data;[187] and (4) when the processing of the data does not comply with EU regulations for other reasons.[188]

A limited right to be forgotten is already part of EU law through the Data Protection Directive ("Directive").[189] The Directive sets the right to access data and the conditions for blocking data when "processing . . . does not comply with the provisions of th[e] Directive, in particular because of the incomplete or inaccurate nature of the data."[190] Member States must guarantee that every data subject has the right to obtain from the controller "the rectification, erasure or blocking of data, when the data processing is not in compliance with the Directive and particularly in instances where the data are incomplete or inaccurate."[191] Article 6 ensures that personal data must be:

> (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes . . . [in addition to] historical, statistical or scientific purposes . . . provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further

182. *See* Rosen, *supra* note 179, at 88.

183. *See id.*

184. Reding, *supra* note 181, at 3, 5. *See generally* Rosen, *supra* note 179 (exploring the right to be forgotten proposal in the EU).

185. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement Of Such Data (General Data Protection Regulation)*, at COM (2012) 11 final (Jan. 1, 2005) [hereinafter *General Data Protection Regulation*].

186. *Id.*

187. *Id.*

188. *Id.*

189. Directive 95/46/EC.

190. *Id.* art. 12(b).

191. *Id.*

> processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed [personal data stored for longer periods should be] stored for historical, statistical or scientific use.[192]

Thus, a limited right to be forgotten already exists in the EU, as long as member states legislate that right. Recently, the Court of Justice of the EU implemented Article 6 of the Data Protection Directive, giving life to the right to be forgotten, or a "right of erasure," in the EU.[193] Back in 1998, Mario Costeja González's house was repossessed and put up for auction for the recovery of social security debts.[194] *La Vanguardia Ediciones SL* published this information in its newspaper, which was also available online.[195] Since that time, when someone Googled González, two links to *La Vanguardia*'s articles, from January and March of 1998, would show up.[196] Dissatisfied with Google's results, on March 5, 2010, Mr. González and the Spanish Data Protection Agency lodged a complaint against *La Vanguardia Ediciones*, Google Spain, and Google, Inc.[197]

González requested that *La Vanguardia* remove or alter those search pages so that the personal data relating to him no longer appeared, or that the company use certain tools made available by search engines to protect the data.[198] González also requested that Google "remove or conceal the personal data relating to him so that they cease to be included in the search results and no longer appeared in the links to La Vanguardia."[199] The reason for such requests, according to González, was that the context of the attachment proceedings concerning him was now entirely irrelevant, as it had been fully resolved for a number of years.[200]

---

192. *Id.* art. 6.

193. Case C-131/12, Google Spain SL v. Agencia Española de Proteccion de Datos (AEPD), 2014 EUR-Lex CELEX 62012CJ0131 ¶ 4 (May 13, 2014).

194. *Id.* ¶ 14.

195. *Id.*

196. *Id.*

197. *Id.*

198. *Id.* ¶ 15.

199. *Id.*

200. *Id.*

The Court of Justice found in Mr. González's favor and held that search engine operators are responsible for their processing of personal data appearing on web pages published by third parties.[201] The court held that processing of personal data and the free movement of such data are interpreted as "processing of personal data" within the meaning of the Directive when the information contains personal data, and that search engines are the "controllers" with respect to that processing, within the meaning of Article 2(d) of the Directive.[202] Thus, search engines should exclude results "where they appear to be *inadequate*, *irrelevant* or *no longer relevant*, or *excessive* in relation to those purposes and in the light of the time that has elapsed."[203] In other words, search engines that operate in the EU are required to remove any material that is "inadequate, irrelevant" or "excessive," but this must be "fair[ly] balanced" against the public's right to the information.[204] An individual is entitled to ask the search engine to remove the links, and the search engine (Google in this case) is obliged to remove links to web pages. The exceptions include "particular reasons, such as the role played by the data subject in public life . . . justif[ying] a preponderant interest of the public in having . . . access to the information when such a search is made."[205] Though limited to some extent, the ruling sets the ground for a right to be forgotten, or more accurately to a right of erasure, even prior to the Directive.

Google complied with the Court of Justice's decision not long after its ruling, and the company offered all Europeans a chance to exercise their new right online, by filing a removal request.[206] These requests must clarify why the URL requested to be removed from Google's search results is now irrelevant, outdated, or otherwise inappropriate.[207] Subsequently, many Europeans chose to exercise their right; in less than a year, more than 200,000 individuals filed removal requests to Google.[208] After a removal request is filed, Google examines the link

201. *Id.* ¶¶ 23–41.

202. *Id.* ¶¶ 26–41.

203. *Id.* ¶ 93 (emphasis added).

204. *Id.* ¶¶ 81, 92–94.

205. *Id.* ¶ 97.

206. *See Legal Removal Requests*, GOOGLE, https://support.google.com/legal/answer/311040?rd=1&hl=en (last visited Nov. 22, 2015).

207. *Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch&vid=null (last visited Nov. 22, 2015). The removal request also demands a copy of a valid form of photo ID, personal details, and links associated with the content that you want removed. *See id.*

208. *See* Lance Whitney, *Google Wants to Limit 'Right to Be Forgotten' Requests to Europe*, CNET (Jan. 20, 2015, 1:12 PM), http://www.cnet.com/news/google-aims-to-limits-right-to-be-forgotten-requests-to-european-sites.

and determines whether it should be removed from Google services in the EU.[209] When possible, Google notifies the website that the link was removed, but the website cannot object to Google's decision by any means.[210]

Does the current right to be forgotten solve our problem? Not really, as the EU ruling refers to personal information posted online which is outdated or no longer relevant. If someone stole your email from last week, it does not fall into this category. However, Article 6 also ensures that personal data must be processed fairly and *lawfully* and collected for specified, explicit, and *legitimate purposes*.[211] Moreover, the data should be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed.[212] Stealing personal information through a cyber hack, without public interests, and posting them online could fall into Article 6 categories. But this broad interpretation of the Directive is not likely.

B. The Need for Cyber Liberty

The right to be forgotten is highly problematic. It is complex,[213] costly,[214] raises high barriers of market entry,[215] leads to possible

209. *See Transparency Report: Frequently Asked Questions*, GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#how_do_you_decide (last visited Nov. 22, 2015).

210. For an example of how Google exercised the right to be forgotten on six articles published on the Guardian website, see James Ball, *EU's Right to Be Forgotten: Guardian Articles Have Been Hidden by Google*, GUARDIAN (July 2, 2014, 10:34 AM), http://www.theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google.

211. *See General Data Protection Representation*, *supra* note 185, at art. 6.

212. *Id.*

213. For example, how will search engines comply with such a right? Most likely, and as Google has already began implementing, by creating a "removal process" and examining every "removal" request thoroughly, while deciding whether the search results are, in fact, inadequate, irrelevant, or excessive. *See Search Removal Request Under Data Protection Law in Europe*, *supra* note 207. Creating an online "removal" form for EU members is the easy part for search engines. It is relatively inexpensive and does not require allocating human resources. The more difficult aspect of the EU ruling is the method of examining whether the request to remove search results is inadequate, irrelevant, or excessive. No doubt, human intervention is required for this step. Currently, computers cannot simply make an educated decision on whether a link's content falls into one of the categories set by the directive. Naturally, such a subjective decision is not easy for humans, let alone computers. But on which grounds will Google employees decide? Which information will fall into one of the Directive's categories?

214. Exercising the right to be forgotten will not come cheap. The "removal" process requires a decision by a human being and, therefore, demands allocating financial resources. Unlike a semi-automated process of decision making, such as the notice-and-takedown regime of copyright infringement under the Electronic Commerce Directive or the DMCA in the United States, 17 U.S.C. § 512 (2012), the right to be forgotten requires human intervention and, thus, human resources. For more on the possible negative impact of the EU decision, see Craig A. Newman, *'A Right to be Forgotten' Ruling Will Cost Europe*, WASH. POST (May 27, 2014),

manipulation and fragmentation of search results,[216] and is not necessarily applicable,[217] among other things. Mainly, it leads to undesired levels of Internet censorship. The right to be forgotten negatively affects free speech and freedom of information.[218] Normatively, civilians should possess a right to ensure that some data is deleted from the Internet, or at least, is not searchable by search engines. But this right should not extend to everything. There is a huge difference between a person who typed and posted personal information and regrets it and a person whose information was stolen and posted without her knowledge or consent. It is also different if information was posted lawfully by someone other than the end-user, such as in the González case.[219] If you posted something, and now want to delete it—tough

---

http://www.washingtonpost.com/opinions/a-right-to-be-forgotten-will-cost-europe/2014/05/26/93bb0e8c-e131-11e3-9743-bb9b59cde7b9_story.html.

215. Even if some search engines possess sufficient financial resources to comply with the EU decision, other search engines that are not that wealthy will not. Thus, high costs of compliance create another problem—high barriers of market entry. Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKLEY J. INT'L L. 161, 186-87 (2012). The right to be forgotten does not affect merely Google—in fact, Google might actually benefit from the right to be forgotten, as it could reduce competition, especially from new competitors. New search engines will have much more difficulty complying with the EU decision. We all lose from such a scenario, as innovation will feel a huge impact. If this occurred at the beginning of the twenty first century, we likely would never have even heard of Google. Additionally, this EU decision could also negatively affect investments in the EU, as new companies will choose to ban their services in the EU due to the financial implications.

216. Until now, Google in the United States and Google in the EU were not much different: U.S. and EU users would receive similar search results with respect to previously determined algorithm differences set by Google. *See Google Begins Taking Requests to Censor Search Results in Europe*, CBS NEWS (May 30, 2014, 11:25 AM), http://www.cbsnews.com/news/google-begins-taking-requests-to-censor-search-results-in-europe. However, the European court's decision fragments the search results between Google U.S. and Google EU. *See* Whitney, *supra* note 208. From now on, EU citizens will see different search results than U.S. citizens. *See id.* Fragmentation of search results will change the Internet. The world should have the opportunity to explore the vast amounts of information globally, without major differences from jurisdiction to jurisdiction.

217. If Europeans know that their search results are being manipulated, some will find a way to bypass this form of censorship. Employers, for example, might wish to compare U.S. and EU Google results, to find out if their workers are trying to hide something from them. Currently, you only need basic computer skills to achieve that—just click on the link saying "Use Google.com" in the bottom right-hand corner of your Google homepage. Such a comparison will enable these employers to quickly discover the more "interesting" search results, as it will be missing from Google in the EU. *See* Jonathan Zittrain, *Don't Force Google to 'Forget,'* N.Y. TIMES, May 14, 2014, at A29 ("Even in Europe, search engine users will no doubt cultivate the same Internet 'workarounds' that Chinese citizens use to see what their government doesn't want them to see.").

218. Freedom of expression in the EU is set mainly by ECHR (along with article 11 of the European Charter of Fundamental Rights). *See* Charter of Fundamental Rights of the European Union, art. 11, 2000 O.J. (C 364) 1; Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, Nov. 4, 1950, E.T.S. No. 5.

219. Case C-131/12, Google Spain SL v. Agencia Española de Proteccion de Datos (AEPD), 2014 EUR-Lex CELEX 62012CJ0131 ¶ 65 (May 13, 2014).

luck.[220] Same goes for when someone else took your picture eating a hotdog down the street or drunk at a party. But if someone broke into your house, installed a hidden video camera, and posted private videos of you online—you should have a right to remove those videos.[221]

Thus, what we should prevent is the availability of *non-newsworthy data* that was obtained *unlawfully*. It is not merely a matter of privacy. It is a liberty to trustfully use cyberspace. Call it the right to cyber liberty. What is the most efficient method to ensure such right? If we embrace Lawrence Lessig's approach, there are four modalities (or constraints) for regulating behavior: law, market, social norms, and architectural design (code).[222] Any of the four modalities can aid civilians in their quest for protection against data linkage.

We begin with social norms and the market. In theory, under this approach, if society condemned such behavior, it would cease. I am rather skeptical here. Many hackers are nonconformists by nature.[223] Their operations are not based on social norms to begin with. Therefore, changing social norms will unlikely succeed in regulating unlawful information from the hacker perspective. That leaves the users. Will Internet users not "use" data that was stolen through a cyber-attack? Even if technologically feasible, meaning that end-users can identify which data was released from a cyber-attack, it is implausible that everyone will comply with such a norm. Thus, the market will also be fairly limited in solving the problem.[224]

Can technology (code) grant cyber liberty? It can, to some extent. For example, using privacy-by-design ("PBD") could change the

220. An exception could possibly be made for minors who carelessly post data online and, perhaps, should have the ability to delete it because they simply do not understand the possible future consequences of their actions. For example, California recently signed a new law that gives minors the right to erase posts they have made to online sites. *See* Cal. St. Leg., S.B. 568, 2013 Leg., Reg. Sess. (Cal. 2013); *California Enacts Poor Man's Right to Be Forgotten*, INFOSECURITY (Sept. 24, 2013), http://www.infosecurity-magazine.com/view/34693/california-enacts-poor-mans-right-to-be-forgotten.

221. In this case, copyright law does not apply, as you are not the right holder of the videos.

222. *See* LAWRENCE LESSIG, CODE: VERSION 2.0 121-37 (2006); LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 116-73 (2004). Michael Birnhack suggested that social norms and the market could be addressed as one because crediting importance to the free market makes it a social value. *See* Michael Birnhack, *Lex Machina: Information Security and Israeli Computer Act*, 4 SHA'AREY MISHPAT 315, 320 n.13 (2006) (Isr.).

223. Roger G. John, *Physical Vulnerability Assessment*, *in* CRITICAL INFRASTRUCTURE SECURITY: ASSESSMENT, PREVENTION, DETECTION, RESPONSE 21, 29 (Francesco Flammini ed., 2012) ("Hacker-type people are often nonconformists.").

224. For more on the market solution, see Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J.L. & TECH. 188, 200 (2006).

defaults of information storing.[225] Various values of privacy could be built into the systems that preserve our online data. In that way, using preventative technological measures could reduce the instances of data theft. A restrictive PBD system could completely ban information storage—no one will be allowed to retain data. A less restrictive measure would be setting expiration dates for information retention[226]—a "Reputation Bankruptcy" which will grant civilians an ability to de-emphasize or entirely delete online information about them.[227] On the other hand, using such mechanisms would also be problematic because we need data storage to enjoy our online experience. From emails to cloud computing storage, data retention has become essential for the Internet. Thus, although technology could potentially aid civilians to preserve their online liberties, it will probably not address the issue, and furthermore, its implementation will be highly problematic. However, technology could aid in identifying which data was stolen by using digital fingerprints. All data has unique fingerprints and could be located by others, if desired. It resembles the well-known practice of marking bills, often used by law enforcement agencies to trace and identify money used for illegal activities.[228] Combined with a complementary legal framework, utilizing digital fingerprints could aid in solving the problem, but will not be sufficient on its own.

Turning now to the law, a few legal mechanisms could aid in accomplishing the desired goal. We can strengthen current civil and criminal penalties and, thereby, increase their effectiveness. However,

---

225. For more on privacy-by-design, see ANN CAVOUKIAN & JEFF JONAS, PRIVACY BY DESIGN, PRIVACY BY DESIGN IN THE AGE OF BIG DATA 7-9 (2012), https://www.privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf.

226. To some extent, there could be a technological solution for the phenomenon of a "never-forgetting-web." TigerText, for example, offers a service that restricts text-message copying and forwarding and the ability to control message lifespan. *See Features*, TIGERTEXT, http://www.tigertext.com/features (last visited on Nov. 22, 2015). There are similar apps for social media postings. *See* Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525, 1535 (2012) (describing technological solutions to the right to be forgotten). Viktor Mayer-Schönberger suggested incorporating an "expiration meta tag" into digital files, so that like our memory, information will have a life span. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 15, 171-73 (2009). There are a few examples of technologies that embraced this viewpoint, such as XPire—an app developed to reduce your digital footprint. XPIRE, http://www.getxpire.com (last visited Nov. 22, 2015); *see also* Muge Fazlioglu, *Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet*, 3 INT'L DATA PRIVACY L. 149, 152-53 (2013) (discussing XPire and Viktor Mayer-Schönberger's approach to information).

227. ZITTRAIN, *supra* note 178, at 228-29.

228. *See* Adam Tanner, *The Web Cookie Is Dying. Here's the Creepier Technology That Comes Next*, FORBES (June 17, 2013, 12:29 PM), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next (describing the practice of digital fingerprinting).

deterrence will unlikely solve this problem, as it will be ineffective.[229] Data retention regulation is another possible solution. Congress could impose liability in various forms on companies that hold and process personal information of civilians.[230] But this is not practical, and, even if it were, it is not enough.[231] Cyber-attacks would still occur, as no company is resilient to zero-day exploits.[232] We can take this one step further by completely banning information storing. But as previously discussed, on a cost-benefit scale, this would be a poor decision—we need data storage. It is crucial for the existence of many online activities.[233] Besides, as Snowden revealed,[234] the government already holds vast amounts of information, and they could also be hacked one day, and thus, it will not solve the problem. We could also enable counterstrikes, such as granting a civil "self-defense" provision for civilians, which could enable them to hack back the perpetrators. But, not only would such a provision not solve the problem, it could also potentially backfire.[235]

Another possible solution, which I have already mentioned, is a right to be forgotten, which applies solely to *non-newsworthy data* that was obtained *unlawfully*. Such right should be secured by an easy and accessible procedure for those civilians whose information was stolen and published in a cyber-attack. Under this right, website and search engines owners will be required to adopt and implement a notice-and-takedown policy, similar to copyright infringement under the DMCA.[236]

---

229. On skepticism of computer legislation as a deterrent to commence crimes, see U.S. SENTENCING COMM'N, REPORT TO THE CONGRESS: ADEQUACY OF FEDERAL SENTENCING GUIDELINE PENALTIES FOR COMPUTER FRAUD AND VANDALISM OFFENSES 6, 9 (1996).

230. For more on data retention in the United States, see generally Catherine Crump, Note, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191 (2004) (discussing data retention policies in the United States and the legal implications).

231. Public choice theories alone will prove how difficult such a move could be. Organized groups with shared interests and defined goals tend to influence legislation more than the general public. *See* JAMES M. BUCHANAN & GORDON TULLOCK, THE CALCULUS OF CONSENT 285-88 (1965); DENNIS C. MUELLER, PUBLIC CHOICE II: A REVISED EDITION OF PUBLIC CHOICE 308-10 (1989).

232. A zero-day exploit refers to a software vulnerability for which a malicious hacker creates an exploit prior to when the software vendor is made aware of the vulnerability. *See Top Cyber Security Risks—Zero-Day Vulnerability Trends*, SANS INST. (Sept. 2009), http://www.sans.org/top-cyber-security-risks/zero-day.php; *see also* Kesan & Hayes, *supra* note 8, at 474 ("[P]assive defense is all but useless against zero-day exploits.").

233. Online data is used for marketing, verifying transactions, shipping products, and many other functions for online companies. *See* Hutchinson, *supra* note 6, at 1152.

234. *See supra* note 77.

235. For a counterattack privilege proposition, see Huang, *supra* note 41, at 1259-63.

236. Under the DMCA, OSPs are exempt from liability when they act expeditiously to remove infringing material after notification of its presence by a copyright holder. *See* 17 U.S.C. § 512(c)(1)(C) (2012); Meg Leta Ambrose et al., *Seeking Digital Redemption: The Future of*

How could this work? All online hosts would be required to implement an accessible removal process. Under such a removal process, any individual could file a request to remove online content when it is non-newsworthy and unlawfully obtained.[237] The request should have to identify the data in a reasonably sufficient manner to permit the host to locate the material, provide information reasonably sufficient to contact the complaining party, and provide a statement that the notification is accurate. To avoid potential legal liability, upon receiving notice from an individual or her agents, the online host will act expeditiously to remove the content. At this point, the publisher could then send a counter-notification. If such counter-notification is filed, the complaining party then must bring a lawsuit against the publisher, and if such lawsuit is not filed within a limited time frame set by the law, the data will become accessible again.

But this notice-and-takedown mechanism also possesses many flaws. Much like the implementation of the right to be forgotten in the EU, the removal process is complex and costly; it raises high barriers for market entry for non-wealthy online hosts, which will not be able to bear the costs of compliance; it creates fragmentation of search results; it is not necessarily applicable; and most significantly, it burdens free speech and places censorship on the Internet.[238]

Perhaps, some of these flaws could be solved with a proper legal design. The process could be designed to be relatively cheap and simple, as it should not require human intervention. If someone made a claim that fell within the defined categories, the online host would remove it. If such claim is falsely made, the market could force its correction. Unlike the current right to be forgotten in the EU, the online host should not evaluate the content and decide what is "newsworthy." This is a subjective decision, but if something is newsworthy, then it will be quickly republished anyway. How? Through proper transparency. We should have the ability to know generally what was removed.[239] Upon

---

Forgiveness in the Internet Age, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 99, 158-62 (2012).

237. A proper notice should be similar to the current notice-and-takedown provision regarding copyright infringement. Hence, it should be a written communication provided to the designated agent of a service provider and include: a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; identification of the material that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material; and a statement that the information in the notification is accurate. *See* 17 U.S.C. § 512(c)(3) (2012).

238. *See supra* notes 213-22 and accompanying text.

239. In response to a possible chilling effect due to a DMCA notice-and-takedown request, Wendy Seltzer created a website that allows the recipients of notices to submit them to the

removal of the content, the online host could publish the complaint. Moreover, newsworthy data will most likely continue to orbit the Internet, even if it was removed from most websites.

Nevertheless, a right to be forgotten, even if more limited, has too high a social cost. It could be misused to change the way we consume information. But we should not be naive. Google already decides on our freedom to access information.[240] Google can place anyone so far down the list of search results that the information is inaccessible *de facto*.[241] But still, the dangers to free speech are too high here. Because of this, it is implausible that Congress will enact such a law. The main barrier would be the First Amendment, which states that "Congress shall make no law . . . abridging the freedom of speech."[242] Free speech has permitted restrictions depending on the content, for example, in cases including obscenity, defamation, fraud, incitement, and speech integral to criminal conduct.[243] A right to be forgotten in the United States clearly could impose a restriction on free speech, but it depends on the target. The "speech" of a website from abroad is unlikely to be protected under the U.S. Constitution.[244] But suppose that the restriction is placed on a U.S. company. Whether or not the company's posting is regular or commercial speech,[245] such a restriction imposes a restriction on free speech, and must withstand constitutional scrutiny.[246] Content-neutral restrictions only need to meet an intermediate standard of scrutiny.[247] However, here we have content-based restrictions on freedom of speech

---

site. *See About Us*, CHILLING EFFECTS, http://www.chillingeffects.org/pages/about (last visited Nov. 22, 2015).

240. *See Google Terms of Service*, *supra* note 113. Google does not deny that there are also human elements in the search results, but insists that such intervention only occurs in very limited cases where the manual control is necessary to improve the users experience. *See Inside Search: Policies*, GOOGLE, http://www.google.com/insidesearch/howsearchworks/policies.html (last visited Nov. 22, 2015). Under these limited cases, Google lists security concerns, legal issues, exception lists, and spam. *Id.*

241. *See Inside Search: Policies*, *supra* note 240.

242. U.S. CONST. amend. I.

243. *See* United States v. Stevens, 559 U.S. 460, 468 (2010) ("From 1791 to the present, the First Amendment has permitted restrictions upon the content of speech in a few limited areas, . . . including obscenity, . . . defamation, . . . fraud, . . . incitement, . . . and speech integral to criminal conduct . . . .").

244. *See generally* Timothy Zick, *The First Amendment in Trans-Border Perspective: Towards More Cosmopolitan Orientation*, 52 B.C. L. REV. 941 (2011) (discussing the cross-border application of the First Amendment right to free speech).

245. Commercial speech is less protected by the Constitution than regular speech. *See* Cent. Hudson Gas & Electric Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 562-63 (1980).

246. *Id.* at 566.

247. Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994); United States v. O'Brien, 391 U.S. 367, 376-77 (1968).

that are subject to strict scrutiny.[248] These restrictions must be narrowly tailored to serve a compelling state interest and be the least restrictive means available to further the articulated interest.[249]

The state might have a compelling interest to preserve the liberties of civilians, including in cyberspace. Such disclosure of personal information could violate a basic human right, strip them of their dignity, cause emotional distress, and socially and professionally harm or alienate them.[250] Thus, as the proposal serves a compelling state interest, it must not be under-inclusive, nor over-inclusive, to survive strict scrutiny.[251] For the framework to avoid under-inclusiveness, it must not be applied only upon the speech. For the framework to avoid over-inclusiveness, its coverage should not apply to data that does not advance legitimate governmental objectives. Generally, the right to be forgotten would not likely pass strict scrutiny.[252]

The most proper solution for information theft is a combination of legal and technological measures. On the technological aspect, while recognizing the drawbacks of such a move, we need to make sure that each bulk of data is easily traceable.[253] For example, we should make sure that all emails have a digital fingerprint, and that in a simple act, OSPs could locate them and quickly remove them. Now the legal part: first, the law must set initial technological standards for data held by any

248. *See, e.g.*, Sable Commc'ns v. FCC, 492 U.S. 115, 126 (1989) (holding that content-restrictions must promote a compelling government interest and that it must be the least restrictive means of achieving that interest); Patrick M. Garry, *A New First Amendment Model for Evaluating Content-Based Regulation of Internet Pornography: Revising the Strict Scrutiny Model to Better Reflect the Realities of the Modern Media Age*, 2007 BYU L. REV. 1595, 1596 (arguing that First Amendment doctrine requires that any content-based speech regulation is subject to strict scrutiny by the courts). For more on strict scrutiny in the United States, see generally Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793 (2006).

249. *See, e.g.*, Ashcroft v. ACLU, 542 U.S. 656, 660, 665, 673 (2004) (finding that the Child Online Protection Act ("COPA"), designed to regulate minor's access to harmful material on the Internet, is unconstitutional because it "was likely to burden some speech that is protected for adults" while there were "plausible, less restrictive alternatives"); Reno v. ACLU, 521 U.S. 844, 849, 871-72, 875, 885 (1997) (finding that two provisions of the Communications Decency Act of 1996, indecent transmission and patently offensive display, abridge freedom of speech and are therefore, unconstitutional); *Sable Commc'ns*, 492 U.S. at 126 (holding that the government may "regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest").

250. *See* Eugene Volokh, *Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People Speaking About You*, 52 STAN. L. REV. 1049, 1110 (2000).

251. *See id.* at 1116-17.

252. *See generally* Robert Kirk Walker, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257 (2012) (arguing that only a limited form of a right to be forgotten could be compatible with the U.S. Constitution).

253. Such a move is problematic to some extent, as digital fingerprints will eliminate anonymity over the Internet. *See* Crump, *supra* note 230, at 216.

OSP. If the data is not quickly identifiable and searchable, it cannot be retained. Second, much like stealing in the kinetic world, civilians that are aware that their information was stolen could file an online complaint at a designated law enforcement agency. Third, the agency will review the complaint, with transparent judicial review available, to decide whether the data was obtained unlawfully. If so, the agency or the court could order OSPs to remove any content linked to the theft.

Aside from costs, this proposition could be problematic in other regards. It grants censorship powers to enforcement and judicial entities that might be misused. Free speech, for that matter, is endangered here. But whether or not it will pass strict scrutiny, we should change our perception of data and, much like the kinetic world, allow for remedies when it is stolen. Such remedies should not only be limited to intellectual property, but any stolen information. This is why technology is important. The legal system should only locate data that was stolen and "return" it to its rightful owner.

Surely, this new liberty will not solve the problem completely. Not every civilian will be able to locate the data, and even if she does, it could be too late. Moreover, not every civilian will be able to fully enjoy such liberty. When data is viral, there is not much to do to stop its dissemination. Take recent issues involving celebrities for example. In 2008, Erin Andrews (an American sportscaster) was filmed in different hotel rooms through the peepholes.[254] One of the videos, in which she appeared nude, was posted online in 2009.[255] The filmmaker, Michael David Barrett, was arrested that year; he pled guilty and was sentenced to thirty months in prison followed by three years of probation, and he was charged $5000 in fines and ordered to pay $7366 in restitution.[256] Andrews also sued the hotels in which she stayed for negligence and invasion of privacy.[257] The video? It is still available online.[258] Andrews cannot remove it, as she is not the copyright owner.

Another example occurred in late 2014, when Oscar-winning actress Jennifer Lawrence discovered that her nude photos were leaked

254. *See* Abigail Pesta, *The Haunting of Erin Andrews*, MARIE CLAIRE (July 13, 2011), http://www.marieclaire.com/celebrity-lifestyle/celebrities/erin-andrews-interview.

255. *Id.*

256. Associated Press, *Andrews' Stalker Gets 2 ½ Years in Prison*, ESPN (Mar. 15, 2010), http://sports.espn.go.com/espn/news/story?id=4998324.

257. CNN Wire Staff, *ESPN's Andrews Files Invasion of Privacy Suit over Hotel Incident*, CNN (Dec. 6, 2011, 6:19 PM), http://www.cnn.com/2011/12/06/us/erin-andrews-lawsuit.

258. A Google video search of "Erin Andrews Nude" still results in over 150,000 hits. Search of "Erin Andrews Nude," GOOGLE, https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#safe=off&tbm=vid&q=erin+andrews+nude (last visited Nov. 22, 2015).

online.[259] She was among many other celebrities, mostly women, whose accounts were hacked and their private pictures posted online.[260] Unlike the Andrews case, this was a result of cyber-attack on Apple's cloud services suite, iCloud.[261] But the distinction should make no difference. In both cases, the result is that someone acted unlawfully and harmed another individual by posting materials online. Unlike Andrews, however, Lawrence is the copyright holder of the nude photos, or at least of most of them. Presumably, she can make use of copyright law to remove the images. But as you might have guessed, those photos are still available online. Even if Google removes links to the pictures, or forces websites to remove the content, end-users who have saved the images will still possess the ability to transfer the files among themselves. Thus, even existing "removal" policies set by the DMCA have proven to be insufficient mechanisms to stop viral data, and unfortunately, my proposed solution will not be different. Nevertheless, the scenario I deal with in this Article is different. Our emails typically do not go viral, unless we are well known. Therefore, using legal mechanisms could actually stop the dissemination of such information, or at least substantially reduce its accessibility. It may not be a perfect solution to eradicating the unauthorized dissemination of personal information, but the proposal would be better than current U.S. policies and vital for securing our online liberties.

VI. CONCLUSION

The Internet plays an integral role in our daily life. We need to feel safe when we use it for our various activities. It is an important liberty in any democratic society. But cyber-warfare endangers such liberty. As the Sony Hack showed, the data of even unknown individuals could one day be published online, viewable and searchable by all. Thus, if the Sony Hack truly marks a new paradigm of cyber-attacks, then we should rethink how to better secure civilians. As this Article showed, a possible solution could be a digital fingerprint requirement under a new legal framework.[262] Under this framework, when someone steals your data, you could file a complaint online with a designated U.S. law enforcement agency, which, along with accompanying judicial review,

259. Kelli Bender, *Lena Dunham, Emma Watson, and More Celebrities React to Jennifer Lawrence Nude Photo Hack*, PEOPLE (Sept. 2, 2014, 1:00 PM), http://www.people.com/article/twitter-reactions-jennifer-lawrence-nude-photo-leak.

260. *Id.*

261. *See* Raven & Wilson, *supra* note 90.

262. *See supra* Part V.B.

could order OSPs to remove the content and any links to such content.[263] While this is not a perfect solution, it is much better than current U.S. law or the EU's right to be forgotten.

The new threats to civilians online demonstrate how the rules of cyber-warfare might be changing. Civilians now play a major role in the digital battlefield, both as attackers and targets. Until now, although sometimes it has caused inconveniences and perhaps been harmful to some extent, cyber-warfare has not lived up to its destructive potential. U.S. critical infrastructure has not been affected yet. More broadly, states, companies, and individuals might have suffered some harm and inconvenience due to cyber-attacks, but to date, it has been nevertheless negligible. The new role of civilians might change this, however. As more civilians enter the battlefield, from both ends, cyber-warfare could lead to destructive outcomes—an equivalent of a civil war in cyberspace. We ought to reduce this possibility using legal and technological measures to ensure the liberties of civilians to safely explore the digital realm, because if civilians do not feel safe, digital riots could ensue.

263. *See supra* Part V.B.

***