CYBERSECURITY OF THE PERSON

Jeff Kosseff*

ABSTRACT

U.S. cybersecurity law is largely an outgrowth of the early-aughts concerns over identity theft and financial fraud. Cybersecurity laws focus on protecting identifiers such as driver's licenses and social security numbers, and financial data such as credit card numbers. Federal and state laws require companies to protect this data and notify individuals when it is breached, and impose civil and criminal liability on hackers who steal or damage this data.

This Article argues that our current cybersecurity laws are too narrowly focused on financial harms. While such concerns remain valid, they are only one facet of the cybersecurity challenge that our nation faces. The cybersecurity profession too often overlooks the harm to individuals, such as revenge pornography and online harassment. Accounting for such harms in our conception of cybersecurity will help to better align our laws with these threats. This Article explains how a broadened understanding of cybersecurity can inform our laws regarding data breach notification, security requirements, and computer hacking.

INTRODUCTION

The RSA Conference in San Francisco is the cybersecurity industry's most prominent annual gathering, bringing together thousands of leaders from the corporate, government, and academic worlds to discuss emerging cyberthreats, trends, and new technologies to better secure systems, networks, and data.[1] The conference boasts an impressive schedule of panels and presentations, many of which are in break-out format.[2] The most attended—and coveted—

---

* Assistant Professor, Cyber Science Department, United States Naval Academy. J.D., Georgetown University Law Center; M.P.P., B.A., University of Michigan. The views expressed in this article are only those of the author and do not necessarily represent those of the Naval Academy, Department of Navy, or Department of Defense.

[1] *About RSA Conference*, RSA CONF., https://www.rsaconference.com/about (last visited Mar. 1, 2019).

[2] *See, e.g.*, *RSA Conference 2019*, RSA CONF., https://www.rsaconference.com/events/us19 (last visited Mar. 1, 2019).

spots are the keynote presentations. When the RSA released the schedule for its April 2018 conference, there was one glaring problem: of the 20 keynote speakers, there were 19 men.[3] Monica Lewinsky, an anti-cyber-bullying advocate, was the only female speaker scheduled for the conference. The keynote imbalance was noteworthy but not terribly surprising; just a few months earlier, CES, the consumer electronics trade industry conference in Las Vegas, hosted zero female keynoters.[4] RSA, to its credit, quickly responded to the criticism and added more female keynote speakers, including Homeland Security Secretary Kirstjen Nielsen,[5] whose department is responsible for civilian cybersecurity and had more reason to be speaking at the conference than any other official in the United States government.

Although RSA attempted to rectify its gender imbalance, the initial list of keynoters speaks volumes about the overwhelmingly male perspective that shapes the cybersecurity field. One study estimates that women comprise only 14 percent of the U.S. cybersecurity workforce.[6] When major conferences such as RSA all but completely exclude female keynote speakers, they discourage women from pursuing careers in the field. Such exclusionary behavior is always appalling, but it also is a significant national and economic security issue, as the cybersecurity industry faces a dire shortage of workers.[7]

The insular nature of the cybersecurity profession is more than just a workforce issue. The leadership of the public and private sector determines the fields' priorities: including what we consider to be cybersecurity threats, and how we will combat them. The current patchwork of laws that purport to address cybersecurity are focused largely on preventing economic harms

---

[3] *See* Verne Kopytoff, *Prominent Tech Conference Faces Backlash for Keynote Lineup: 19 Men, 1 Woman*, FORTUNE (Mar. 2, 2018), http://fortune.com/2018/03/01/rsa-tech-conference-backlash-keynote-gender-gap/?utm_content=buffer84a07&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

[4] *See* Adam Lashinsky, *That Metaphorically Appropriate Power Outage at CES*, FORTUNE (Jan. 11, 2018), http://fortune.com/2018/01/11/ces-power-outage-tech-backlash/ ("While waiting for Ford CEO Jim Hackett's enlightening keynote Tuesday morning I listened to CES poo-bah Gary Shapiro mouth words about diversity. This from the head of an organization that didn't see fit to program one woman as a keynote speaker at its annual event.").

[5] Verne Kopytoff, *After Intense Criticism, RSA Tech Conference Adds More Women to Top Speaking Slots*, FORTUNE (Apr. 15, 2018), http://fortune.com/go/tech/rsa-tech-conference-adds-more-women-to-top-speaking-slots/.

[6] Tim Johnson, *Why Are So Few Women in Cybersecurity?*, GOV'T TECH. (Jan. 25, 2018), http://www.govtech.com/workforce/Why-Are-So-Few-Women-in-Cybersecurity.html.

[7] *Id.* ("A study last year by Frost & Sullivan, a consulting firm, found that North America will face a shortage of 265,000 cybersecurity workers by 2022.").

such as identity theft. This Article argues that the cybersecurity field—and its laws and policies—focus too narrowly on these economic harms, at the exclusion of other harms that often are disproportionately suffered by women and minority groups.

Case in point: the only woman who was initially scheduled to deliver an RSA keynote—Lewinsky—is not the standard RSA speaker. She is not a technology executive, nor is she a lawmaker. Lewinsky has become one of the most prominent advocates to address online bullying and harassment. Lewinsky—whose name was thrown into the public spotlight via an online gossip blog in 1998—understands these reputational harms better than possibly anyone else in the United States; as she put it, she was "patient zero" of the cyber-bullying era.[8] Lewinsky urged the audience to protect particularly sensitive information that could be used against victims. "Make people more aware of cybersecurity and how to protect themselves, particularly the young," she said.[9]

Lewinsky's message would not have been as impactful coming from anyone else in the crowd of RSA regulars. Her life experiences—some of which are well known to the public in great detail thanks to the Internet—have shaped her unique view on cybersecurity threats and solutions. Yet the agenda for RSA—and the cybersecurity industry at large—is shaped by the standard roster of technology executives, hacking whizzes, and government officials. Voices such as Lewinsky's have largely been left out of our discussions about what it means to secure cyberspace. And it shows.

This Article ultimately argues that the legal system must broaden its focus on cybersecurity to include non-economic harms, such as online harassment, cyberbullying, and revenge pornography. Part I examines the types of personal harms that individuals face in cyberspace, and argues that the current system of civil lawsuits and criminal prosecutions does not sufficiently deter bad actors, in part because of the First Amendment protections for online speech. Part II provides an overview of the current framework of statutes, regulations, and that broadly encompasses cybersecurity law, and argues that these laws do not adequately cover many of the personal harms. It suggests improvements and modernizations to cybersecurity law to better protect individual rights.

---

[8] Laura Hautala, *Monica Lewinsky Wants Cybersecurity Pros to Aid the Vulnerable*, CNET (Apr. 18, 2018, 9:30 PM), https://www.cnet.com/news/monica-lewinsky-asks-cybersecurity-pros-to-aid-the-vulnerable/.
[9] *Id.*

I. CYBER THREATS TO THE PERSON

The term "cybersecurity" is often associated with white-hat and black-hat hackers engaging in digital battles against one another in a battle to protect servers, confidential trade secrets, and cyber-physical systems.[10] To be sure, such national security and macroeconomic concerns are pervasive—and legitimate. Too often overlooked, however, are the harms that individuals face, stemming not only from attempts to steal their money, but also pervasive harassment and hateful online activities. States have increasingly passed statutes to address cyberbullying and revenge pornography, though these admirable efforts have encountered some First Amendment challenges and other obstacles. This Part argues that while these after-the-fact remedies are an important component of fighting cyberthreats to the person, they are not sufficient.

Perhaps the most comprehensive look at these individual harms was Danielle Citron's 2014 book, *Hate Crimes in Cyberspace*. Citron succinctly describes the wide range of individual harms that exist in cyberspace:

> Cyber harassment involves threats of violence, privacy invasions, reputation-harming lies, calls for strangers to physically harm victims, and technological attacks. Victims' in-boxes are inundated with threatening e-mails. Their employers receive anonymous e-mails accusing them of misdeeds. Fake online advertisements list victims' contact information and availability for sex. Their nude photos appear on sites devoted to exacting revenge. On message boards and blogs, victims are falsely accused of having sexually transmitted infections, criminal records, and mental illnesses. Their social security numbers and medical conditions are published for all to see. Even if some abuse is

[10] *See, e.g.*, *What Is Cybersecurity?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security (last visited Mar. 1, 2019).

> taken down from a site, it quickly reappears on others. Victims' sites are forced offline with distributed-denial-of-service attacks.[11]

A. New Threats, New Harms

As social media and newer technology proliferates, we learn about new ways that individuals suffer at the hands of bad actors. Sextortion is a prime example of this trend. A 2016 Brookings report reviewed court filings to find 80 cases of "sextortion" involving at least 3,000 victims.[12] The authors of the report define sextortion as "old-fashioned extortion or blackmail, carried out over a computer network, involving some threat—generally but not always a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity."[13] The report provided a chilling example of how sextortion works:

> It started with an email from an unknown sender with the subject line, "Read this and be smart."
>
> When the victim opened the email, she found sexually explicit photos of herself attached and information that detailed where she worked. Following that were details of her personal life: her husband and her three kids. And there was a demand.
>
> The demand made this hack different: This computer intrusion was not about money. The perpetrator wanted a pornographic video of the victim. And if she did not send it within one day, he threatened to publish the images already in his possession, and "let [her] family know about [her] dark

[11] DANIELLE K. CITRON, HATE CRIMES IN CYBERSPACE 3–4 (2016).
[12] Benjamin Wittes et al., *Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault*, CTR. FOR TECH. INNOVATION BROOKINGS (May 11, 2016), https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.
[13] *Id.* at 11.

> side." If she contacted law enforcement, he promised he would publish the photos on the Internet too.
>
> Later in the day, to underscore his seriousness, the hacker followed up with another email threatening the victim: "You have six hours."
>
> This victim knew her correspondent only as yosoylammer@hotmail.com, but the attacker turned out to be a talented 32-year-old proficient in multiple computer languages. Located in Santa Ana, California, his name was Luis Mijangos.
>
> On November 5, 2009, yosolammer@hotmail.com sent an email to another woman with the subject line: "who hacked your account READ it!!!" In the email, Mijangos attached a naked photo of the victim and told her "im [sic] in control of your computers right now."[14]

B. Barriers to Common-Law Claims

Victims of revenge pornography, cyber-harassment, cyber-bullying, sextortion, and other highly personal cyberattacks face a tough road if they want to hold bad actors liable. Consider, for instance, the case of Alyssa Backlund. In 2009, Christopher Stone posted a picture of a girl on his website, StickyDrama.com. Alongside the picture was a description claiming that the photo "appears to depict Alyssa Marie Robertson masturbating next to an infant. Such an act, in addition to being morally repugnant, probably violates several statutes pertaining to exposing children to obscenity."[15] Stone posted Backlund's contact information alongside the image, even though Backlund was not the person in the photo.[16] The

---

[14] *Id.* at 1.
[15] Backlund v. Stone, No. B235173, 2012 Cal. App. Unpub. LEXIS 6467, at *2 (Cal. Ct. App. Sept. 4, 2012).
[16] *Id.*

post was viewed thousands of times. Visitors commented the Backlund was a "whore," and contacted her directly.[17] Backlund allegedly contacted a friend of Stone. A few months later, after obtaining a topless picture of Backlund, Stone publicly tweeted to her, "[m]essage him again, and your floppy titties are spammed all over the place. Last warning."[18] Backlund claims that Stone filed a defamation lawsuit against her in small claims court but did not serve it, and that he encouraged the visitors to his website to campaign for his case to be heard on *Judge Judy*.[19] After Stone had threatened Backlund on Twitter, Backlund had been pseudonymously quoted in a Gawker article entitled "StickyDrama's Christopher Stone is a 'Sextortion' Expert in More Ways Than One.'"[20] Quoted as "Sarah," Backlund stated, "[h]e scares me shitless . . . he'll take anything he can to smash you."[21] Backlund sued Stone for defamation and false light invasion of privacy, and her claim survived an initial motion to strike, and Stone did not appeal the denial.[22]

But that was not the end of the legal wrangling for Backlund. After he lost his motion to strike, he sued Backlund for defamation and intentional infliction of emotional distress arising from the Gawker article.[23] Stone claimed to protect "naïve and unsuspecting [Internet] users [who] are easy prey to sex offenders[.]"[24] Stone disputed the claim that he had committed sextortion.[25] "I did not engage in `sextortion' because I never demanded that Backlund send me additional topless photos or any money or property in exchange for refraining from posting her photograph," he wrote in a declaration.[26] Backlund moved to strike the claims under California's anti-SLAPP statute.[27] The trial court denied the motion, concluding that the subject of the claims was not a public interest matter, but rather Backlund's "own comments, regarding an individual experience, concerning alleged threats" by Stone.[28] The allegations of Backlund "blindly answering questions about one's individual experience, without any awareness of the author's intended topic of the publication, distinguishes it from others described in

[17] *Id.*
[18] *Id.* at *3.
[19] *Id.*
[20] *Id.* at *6.
[21] *Id.* at *7.
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

published opinions, where defendants themselves speak on issues of public interest," the trial court reasoned.[29]

The California Court of Appeal reversed the denial of the motion to strike, concluding that Backlund's statements to Gawker "were a public comment about a publicly disseminated threat against her made by public figure Stone."[30] Although Backlund ultimately escaped liability, she was forced to not only litigate her defamation claim against Stone, but to defend against his counter-claims in two different courts. Backlund's case demonstrates the difficulty that victims face in using common-law remedies such as defamation and privacy torts. The extensive litigation, uncertainty, significant personal legal risks, and public attention serve as a strong disincentive for a victim to bring such civil litigation, even in cases that involve appalling facts.

C. Addressing New Harms Via Statute

Recognizing the limits of common law torts, many states have passed statutes that specifically address cyberbullying, revenge pornography, cyberstalking, and online harassment. But even these statutes, which provide criminal or civil penalties, have faced constitutional obstacles.

For instance, North Carolina's state legislature enacted a statute that made it "unlawful for any person to use a computer or computer network to . . . [p]ost or encourage others to post on the Internet private, personal, or sexual information pertaining to a minor" "[w]ith the intent to intimidate or torment a minor."[31] A male North Carolina high school student posted on Facebook a text message that a classmate had accidentally sent him.[32] Robert Bishop, who also attended the same high school, commented below the post that the message was "excessively homoerotic."[33] Other classmates posted similar comments.[34] The mother of the boy who was the subject of the Facebook post found him in his room, hysterically crying.[35] After viewing the Facebook post, she called the police, which launched the investigation.[36] Bishop and other students involved in the Facebook comments were charged under the North Carolina

---

[29] *Id.*
[30] *Id.*
[31] State v. Bishop, 787 S.E.2d 814, 815 (N.C. 2016) (quoting N.C. GEN. STAT. § 14-458.1 (2015)).
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.* at 816.
[36] *Id.*

cyberbullying law.[37] After Bishop's conviction, he appealed, arguing that the statute violates the First Amendment.[38] Although the North Carolina Court of Appeals rejected his appeal, the North Carolina Supreme Court in 2016 agreed with Bishop that the cyberbullying statute was unconstitutional.[39] The Court reasoned that the cyberbullying statute "restricts speech, and not just nonexpressive conduct; that the restriction created is content based, not content neutral; and that the statute's scope is not sufficiently narrowly tailored to serve the State's asserted interest in protecting children from the harms resulting from online bullying."[40] Although the state's goal to prevent cyberbullying is "laudable," the Court wrote, the North Carolina law "'create[s] a criminal prohibition of alarming breadth.'"[41]

Likewise, Albany County, N.Y., passed a law that imposed misdemeanor penalties of up to a year in jail and a $1,000 fine for the offense of cyberbullying, which it defined as:

> any act of communicating or causing a communication to be sent by mechanical or electronic means, including posting statements on the internet or through a computer or email network, disseminating embarrassing or sexually explicit photographs; disseminating private, personal, false or sexual information, or sending hate mail, with no legitimate private, personal, or public purpose, with the intent to harass, annoy, threaten, abuse, taunt, intimidate, torment, humiliate, or otherwise inflict significant emotional harm on another person.[42]

An Albany County high school student, Marquan M., pseudonymously posted on Facebook detailed allegations of classmates' sex lives.[43] Marquan was charged under the county cyberbullying law, and after the trial court rejected his First

---

[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.* at 817.
[41] *Id.* at 821 (quoting United States v. Stevens, 559 U.S. 460, 474 (2010)).
[42] LOCAL L. NO. 11 OF COUNTY OF ALBANY § 1 (2010).
[43] People v. Marquan M., 24 N.Y.3d 1, 6 (2014).

Amendment objections to the law, he pleaded guilty with the right to appeal the constitutionality.[44] On appeal, the New York Court of Appeals agreed with Marquan, finding that the county law was of "alarming breadth," and that it would "criminalize a broad spectrum of speech outside the popular understanding of cyberbullying, including, for example: an email disclosing private information about a corporation or a telephone conversation meant to annoy an adult."[45] The county acknowledged that portions of its law were unconstitutionally overbroad but as applied to Marquan, comported with the First Amendment.[46] As the New York Court of Appeals characterized the County's position, it believed the law only applies to "particular types of electronic communications containing information of a sexual nature pertaining to minors and only if the sender intends to inflict emotional harm on a child or children."[47] The Court refused to sever the portions of the law that the County conceded to be unconstitutional while retaining the remainder.[48] "[T]o accept the County's proposed interpretation, we would need to significantly modify the applications of the county law, resulting in the amended scope bearing little resemblance to the actual language of the law," the majority wrote.[49] "Such a judicial rewrite encroaches on the authority of the legislative body that crafted the provision and enters the realm of vagueness because any person who reads it would lack fair notice of what is legal and what constitutes a crime."[50]

Such First Amendment obstacles extend to state efforts to combat revenge pornography. For instance, Texas enacted a revenge pornography statute that provides:

> A person commits an offense if:
>
> (1) without the effective consent of the depicted person, the person intentionally discloses visual material depicting another person with the person's intimate parts

[44] *Id.*
[45] *Id.* at 9.
[46] *Id.*
[47] *Id.* at 7.
[48] *Id.* at 11.
[49] *Id.*
[50] *Id.*

> exposed or engaged in sexual conduct;
>
> (2) the visual material was obtained by the person or created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private;
>
> (3) the disclosure of the visual material causes harm to the depicted person; and
>
> (4) the disclosure of the visual material reveals the identity of the depicted person in any manner[.][51]

The statute defines "intimate parts" as "the naked genitals, pubic area, anus, buttocks, or female nipple of a person."[52] It defines "visual material" as "any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide"[53] and "any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method."[54]

The constitutionality of this statute soon came under question when Jordan Bartlett Jones, who was charged under the statute, facially challenged the law as a First Amendment violation.[55] The trial court rejected his pretrial argument, but in April 2018, the Court of Appeals of Texas reversed.[56] The court concluded that the ban was a content-based speech regulation, requiring strict scrutiny.[57] Texas argued that the law survived strict scrutiny because the government had a compelling interest in protecting individuals' privacy.[58] The Court found particularly "problematic" the application of the law to *either* visual material

---

[51] TEX. PENAL CODE ANN. § 21.16(b) (West 2017).
[52] *Id.* § 21.16(a)(1).
[53] *Id.* § 21.16(a)(5)(A).
[54] *Id.* § 21.16(a)(5)(B).
[55] Ex Parte Jones, No. 12-17-00346-CR, 2018 WL 2228888 (Tex. App. Apr. 18, 2018).
[56] *Id.*
[57] *Id.*
[58] *Id.*

"obtained by the person" *or* "created under circumstances in which the depicted person had a reasonable expectation that the visual material would remain private."[59] To illustrate its problem with the wide range of potentially covered materials, the Court provided a hypothetical:

> Adam and Barbara are in a committed relationship. One evening, in their home, during a moment of passion, Adam asks Barbara if he can take a nude photograph of her. Barbara consents, but before Adam takes the picture, she tells him that he must not show the photograph to anyone else. Adam promises that he will never show the picture to another living soul, and takes a photograph of Barbara in front of a plain, white background with her breasts exposed.
>
> A few months pass, and Adam and Barbara break up after Adam discovers that Barbara has had an affair. A few weeks later, Adam rediscovers the topless photo he took of Barbara. Feeling angry and betrayed, Adam emails the photo without comment to several of his friends, including Charlie. Charlie never had met Barbara and, therefore, does not recognize her. But he likes the photograph and forwards the email without comment to some of his friends, one of whom, unbeknownst to Charlie, is Barbara's coworker, Donna. Donna recognizes Barbara and shows the picture to Barbara's supervisor, who terminates Barbara's employment.[60]

---

[59] *Id.* (quoting TEX. PENAL CODE ANN. § 21.16(b) (West 2017)).
[60] *Id.*

Chief Justice James T. Worthen, writing for the panel, wrote that Charlie and Donna—in addition to Adam—could be liable under Texas's law.[61] Charlie, he wrote, "had no reason to know that the photograph was created under circumstances under which Barbara had a reasonable expectation that the photograph would remain private."[62] Although the charges against Jones only involved images that he allegedly obtained, the Court sought an extreme hypothetical to justify a facial invalidation of the law.[63] In September 2018, the Texas Court of Criminal Appeals agreed to hear an appeal of the ruling.[64]

The rulings from North Carolina, New York, and Texas demonstrate the significant limitations that legislatures face when they enact laws intended to penalize perpetrators of cyberbullying, revenge pornography, and other similar acts. Even if the laws appear to be tailored to protect a compelling interest, they may overreach into other speech. Of course, if legislatures draft their laws too narrowly, they might not fully address the harms.

D. Free Speech or Equality?

It is difficult to read these court opinions without thinking about the criticisms of First Amendment protections for pornography advanced by Catharine Mackinnon. Working with Andrea Dworkin, MacKinnon had convinced Indianapolis to prohibit certain types of trafficking in pornography.[65] Dworkin, MacKinnon, and other supporters of the ban argued that pornography led to the suppression of women, encouraging men to treat women as sexual objects.[66] The Seventh Circuit struck down the ordinance as a First Amendment violation.[67] "Speech treating women in the approved way — in sexual encounters 'premised on equality' — is lawful no matter how sexually explicit," Judge Frank Easterbrook wrote.[68] "Speech treating women in the disapproved way — as submissive in matters sexual or as enjoying humiliation — is unlawful no matter how significant the literary, artistic, or political qualities of the work taken as a whole. The state may not ordain preferred viewpoints

[61] *Id.*
[62] *Id.*
[63] *See id.*
[64] Chuck Lindell, *Court to Decide If Texas Can Enforce 'Revenge Porn' Law*, STATESMAN (Sept. 25, 2018), https://www.statesman.com/news/20180725/court-to-decide-if-texas-can-enforce-revenge-porn-law.
[65] Am. Bookseller's Ass'n v. Hudnet, 771 F.2d 323, 324 (7th Cir. 1985).
[66] *Id.* at 325.
[67] *Id.*
[68] *Id.*

in this way."[69] MacKinnon rejected Easterbrook's comparison of the Indianapolis ordinance to restrictions on political speech.[70] "Behind his First Amendment façade, women were being transformed into ideas, sexual traffic in whom was protected as if it were a discussion, the men uninhibited and robust, the women wide-open," MacKinnon wrote.[71] "Judge Easterbrook did not say this law was not a sex discrimination law, but he gave the state interest it therefore served—opposition to sex inequality—no constitutional weight."[72]

Just as MacKinnon and Dworkin faced insurmountable First Amendment barriers in their attempts to restrict pornography, so to do people who seek to reduce the amount of cyberbullying, revenge pornography, and other types of harmful online speech. By restricting speech, they inevitably will encounter First Amendment objections that likely will limit their efforts.

However, the First Amendment is not the only reason that cyber-harms cannot be addressed purely through retrospective penalties. There is another significant barrier to relying on victims to file lawsuits or bring criminal charges: the immense personal toll of reliving a traumatic experience. As Danielle Citron aptly summarized:

> Victims are often reluctant to sue privacy invaders because they do not want to further expose their lives to them. As David Bateman and Elisa D'Amico (who represent victims of nonconsensual pornography on a pro bono basis) have explained, victims often fear the exposure that discovery inevitably entails. They do not want their medical records revealed to their attackers. They are anxious about sitting across from their abusers during a deposition. It is not hard to see why many victims do not sue privacy invaders.[73]

---

[69] *Id.*
[70] CATHARINE MACKINNON, ONLY WORDS 98 (1993).
[71] *Id.*
[72] *Id.*
[73] *See* Danielle K. Citron, *Sexual Privacy*, YALE L.J. (forthcoming 2019).

Laws that penalize people for revenge pornography and cyberbullying play an important role in combatting cyber-harms to the person. However, these backward-looking laws have limits. In some cases, the laws as applied or facially will be struck down as unconstitutional. And, even when the cases do not fail on constitutional grounds, civil litigants or prosecutors face significant burdens to demonstrate harm that already has occurred. While these laws are integral in combatting online harassment, they should not be the only part of the equation. We need to look at prophylactic legal measures that stop these wrongs from occurring in the first place. As the above cases demonstrate, our current laws are woefully inadequate.

II. A BROADER CONCEPTION OF CYBERSECURITY LAW

Despite the efforts of legislators, prosecutors, and litigants, civil litigation and criminal prosecution only addresses one aspect of cyber-harms to individuals. These punitive measures not only face constitutional challenges, but they largely penalize behavior after the harm has occurred. In addition to these retrospective laws, we should consider how to best align prospective cybersecurity laws to reduce the likelihood of these cyber threats. In other words, legislatures have determined when and how to punish certain types of online behavior. The next step is to figure out how the law might prevent this behavior from occurring in the first place.

The United States has very few laws that explicitly use the term "cybersecurity." This is likely because many cybersecurity-related laws were enacted decades ago, before the term "cybersecurity" was commonplace.[74] This Part provides an overview of the statutes that broadly fall underneath the umbrella of cybersecurity, analyzes the harms that they seek to protect against, and explains how they could better protect individuals from the types of harms outlined in Part I.

A. Notification Laws

The first general category of cybersecurity laws are statutes that require companies to notify individuals, regulators, and credit bureaus of data breaches. The United States does not have a national data breach notice law; instead, every state and the District of Columbia has enacted its own statute that requires

[74] *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 1010 (2018) ("[T]here are a number of U.S. state and federal statutes, regulations, and court opinions regarding data security, hacking, and related issues that address some aspects associated with cybersecurity law.").

notification in certain circumstances.[75] The laws are triggered only if there is unauthorized access to "personal information."[76] All of the statutes include in their definition of personal information an individual's name in combination with at least one of the following: social security number, driver's license or state identification number, or full financial account number.[77] Some states protect additional categories of data; North Dakota, for instance, includes birth date and mother's maiden name in its definition of "personal information."[78] Maryland's breach notice law, passed in 2007 but updated in 2017, also includes health insurance account numbers and biometric identifiers.[79] Although some states, like Maryland, are gradually updating their breach notification to reflect more modern threats, the breach notice statutes are largely a creature of the few years after California became the first state to pass a breach notice law. Although crimes such as revenge pornography and online harassment existed at the time,[80] regulators and the media were heavily focused on identity theft and financial crimes with amendments to the Fair Credit Reporting Act in 2003.[81]

What do data breach notification laws not cover? For starters, they do not require individuals to be notified of the disclosure of information that could be used to stalk, harass, or dox them. Let's say that a company is breached and a list of its customers' names, home addresses, work addresses, personal email addresses, and home phone numbers is disclosed. No state breach notification law requires companies to notify the individuals, law enforcement, or regulators about that disclosure. Of course, such a breach would be less likely to be used for financial fraud than, say, the disclosure of a Social Security number. However, such information could—and is—used not only for directly sending threats, but to launch systematic online harassment campaigns. For instance, in October 2018, a Washington D.C. man was arrested for posting on Wikipedia the home addresses, phone numbers, mobile phone numbers, and

---

[75] *See Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[76] *Id.*
[77] *See id.*
[78] N.D. CENT. CODE §§ 51-30-01–51-30-03 (2017).
[79] MD. CODE ANN., COM. LAW §§ 14-3501–3503.
[80] *See, e.g.*, Barnes v. Yahoo, 570 F.3d 1096 (9th Cir. 2009) (describing a case of revenge pornography that occurred in 2004).
[81] *See, e.g.*, Press Release, Federal Trade Commission, FTC Committed to Fighting Identity Theft (Dec. 15, 2003).

email addresses of three United States senators.[82] It is unclear how he obtained the information, but such contact details are not typically available to the public. Had he obtained the data via a breach of a public company, that company would be under no legal obligation to notify the senators or law enforcement unless the breach also included protected information such as Social Security numbers or driver's license information.

In addition to the narrow definition of personal information, most state data breach notification laws also contain "risk of harm" thresholds, which allow a company to avoid notifying if it determines that the breach does not pose a serious risk of harm to individuals. As with the definition of personal information, these thresholds are typically focused on financial harm. For instance, Ohio's breach notification law is triggered only if the unauthorized access and acquisition of data "causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident."[83] While the term "other fraud" might be charitably read to include some types of harassment, the wording suggests that the statute is more focused on notifying individuals who are at risk of financial harms such as identity theft.

Breach notification laws should require companies to notify individuals of the unauthorized disclosure of non-public information that could be used to harm them. In addition to requiring notification regarding financial information and data that could be used for identity theft, the laws should notify individuals of unauthorized disclosure of information about their families, home addresses, personal phone numbers, and any other details that could be used to intimidate, harass, or threaten.

The notification laws also should reach beyond the concept of data breaches, and cover other compromises that could lead to harm to an individual. For instance, if the maker of an Internet-connected camera discovers a vulnerability that allows unauthorized parties to access video feeds, that manufacturer should face an obligation to notify individuals of the problem and help them to patch it.

B. Data Security Laws

Another category of laws that generally falls into the category of cybersecurity are data security requirements. The United States does not have a single general law, at the federal

---

[82] *See* Katherine Tully-McManus, *Suspect in Congressional Doxxing Cases Arrested*, ROLL CALL (Oct. 3, 2018), https://www.rollcall.com/news/politics/suspect-in-doxxing-arrested.

[83] OHIO REV. CODE ANN. § 1349.19(B)(1).

level, that sets data security standards. The closest thing that the United States has to a general data security and privacy regulator is the Federal Trade Commission, but its legal authority is limited. The FTC does not have explicit authority to regulate cybersecurity. Instead, it claims data security enforcement authority under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[84] The FTC challenges data security practices as deceptive if companies have misrepresented how they secure data.[85] Under the statute, an act is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[86] Although the FTC has issued informal guidance as to the types of data security practices that might be "unfair,"[87] it does not have formal rulemaking authority for data security. In addition to the lack of specificity, the FTC's data security enforcement authority falls short because it typically enters into consent decrees with companies, requiring some changes to security practices but not levying a monetary fine for a first violation. Contrast this with Europe's General Data Protection Regulation, which penalizes companies up to 4 percent of global annual revenues or 20 million Euros, whichever is greater.[88]

More stringent data security requirements are found in some federal sector-specific laws. The Gramm-Leach-Bliley Act allows federal financial regulators to set standards for regulated financial institutions.[89] The Health Insurance Portability and Accountability Act of 1996 allows the Department of Health and Human Services to regulate the data security of health plans, healthcare clearinghouses, healthcare providers, and their business associates.[90] Although protecting financial and healthcare data is crucial to privacy values, these laws are limited only to particular types of businesses. Even though health data could be used to blackmail or harass an individual, many types

---

[84] 15 U.S.C. § 45(a)(1).
[85] *See, e.g.*, Complaint at 3–5, In re Upromise, Inc., F.T.C. File No. 102-3116, No. C-4351 (2012), 2012 WL 1225058.
[86] 15 U.S.C. § 45(n).
[87] *See* FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205startwithsecurity.pdf.
[88] *See* Michelle Cheng, *How You Can Cash in on Europe's New Data-Privacy Law*, INC. MAG. (May 3, 2018), https://www.inc.com/michelle-cheng/gdpr-how-smart-businesses-can-cash-in-on-europes-new-data-privacy-law.html.
[89] *See* 15 U.S.C. § 6801.
[90] *See* 42 U.S.C. § 1320d.

of companies that might hold individuals' health data are not necessarily covered by HIPAA's rigorous requirements.

C. Personal Information Security

In addition to these sector-specific laws, about a dozen states have enacted general data security laws that apply to the personal information of their residents. Most of these statutes do not have terribly specific requirements; for instance, Indiana's data security statute requires that a company that owns a data base with personal information of Indiana residents "implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[91] Massachusetts has the most detailed general data security requirements, with its regulations spelling out the specific components of written information security plans that companies must adopt.[92] Massachusetts also requires specific technological safeguards, such as "reasonable monitoring of systems" and "encryption of all transmitted records and files containing personal information that will travel across public networks."[93]

The primary shortcoming of these state laws is that they adopt the narrow definition of personal information seen in the data breach notification laws. For instance, the Massachusetts data security regulation only protects "personal information," which it defines as

> a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or

[91] IND. CODE § 24-4.9-3-3.5(b).
[92] *See* 201 MASS. CODE REGS. 17.00 (2019).
[93] *Id.* § 17.04.

> password, that would permit access to a resident's financial account.[94]

The Massachusetts regulations do not apply to "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."[95]

The Massachusetts regulation does not require companies to protect a wide swath of personal information about Massachusetts residents, such as information that could be used to stalk, harass, or embarrass them. Like the breach notification laws, it is an outgrowth of the concern over financial harm and does not adequately address the harms to individuals that increasingly encountered online.

D. Protecting the "Internet of Things"

Both the data security and breach notice laws also largely fail to account from the growing threat of attacks on connected devices. Known as the "Internet of Things," everyday devices connected to the Internet are proliferating, driven in part by the shift in the Internet Protocol system to IPv6 that has increased the number of IP addresses available.[96] Internet of Things connects everything from cars to webcams to refrigerators. With the new technological benefits come new risks. In 2015, the FTC staff spoke with security and industry experts and issued a report on Internet of Things privacy and security issues. The staff concluded that the connected devices "may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks."[97] Indeed, connected devices are notoriously insecure. This lack of security can lead to personal harms such as sextortion. For instance, the Brookings report on sextortion found that although some of the extortion involved images obtained without authorization from individuals' computers or social media accounts, some involved "the actual hacking of their computers and the remote controlling of their

---

[94] *Id.* § 17.02.
[95] *Id.*
[96] *See* Charles Sun, *No IoT Without IPv6*, COMPUTERWORLD (May 19, 2016, 4:00 AM), https://www.computerworld.com/article/3071625/internet-of-things/no-iot-without-ipv6.html ("How much of a difference would IPv6 make? A lot. It has a total of 340 undecillion (that is 340 trillion trillion trillion) addresses. Even with the IoT fulfilling Cisco's expectations, that should be enough for years to come.").
[97] FEDERAL TRADE COMMISSION, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 10 (2015).

webcams."[98] As the Brookings report concluded, webcams are "often insecure and offer sextortionists and other bad cyber actors literal visibility into the activity of non-consenting targets. Similarly, relatively lax password controls—and relatively simple password recovery—on social media platforms makes hacking accounts too easy."[99]

Only one state—California—has attempted to address Internet of Things security, passing a law in 2018 that requires connected device manufacturers to adopt "reasonable" security features that are (1) "[a]ppropriate to the nature and function of the device," (2) "[a]ppropriate to the information it may collect, contain, or transmit," and (3) "[d]esigned to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."[100] While the new law is well-intentioned, it does not provide specific guidance as to the technical measures that manufacturers should take to secure connected devices. It only states that if the device can authenticate outside of a local network, the manufacturer should ensure that either "[t]he preprogrammed password is unique to each device manufactured" or "[t]he device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time."[101] Although this requirement is a good start, as security expert Robert Graham has written, it only addresses one of many vulnerabilities in Internet of Things devices.[102]

III. MATCHING LAWS TO THE HARMS

To better align cybersecurity laws with the harms to individuals, this Article provides six recommendations for lawmakers to consider. As I argue in a forthcoming article in *Wake Forest Law Review*, such reforms should, when possible, occur at the federal level, given the inherently interstate nature

---

[98] Wittes et al., *supra* note 12, at 17.
[99] *Id.* at 28.
[100] CAL. CIV. CODE § 1798.91.04 (West 2019).
[101] *Id.*
[102] Robert Graham, *California's Bad IoT Law*, ERRATA SECURITY (Sept. 10, 2018), https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W9MnZ2hKjIW (emphasis in original) ("It's based on the misconception of *adding* security features. It's like dieting, where people insist you should eat more kale, which does little to address the problem you are pigging out on potato chips. The key to dieting is not eating more but eating less. The same is true of cybersecurity, where the point is not to add 'security features' but to remove 'insecure features'. For IoT devices, that means removing listening ports and cross-site/injection issues in web management. Adding features is typical 'magic pill' or 'silver bullet' thinking that we spend much of our time in infosec fighting against.").

of cybersecurity and the benefits of uniform requirements for service providers, manufacturers, and other companies:

> This uncoordinated regulatory approach is ill-suited to any field, and particularly to one as vital as cybersecurity. Cybersecurity regulation is determined by more than 7,000 state legislators, and enforced by 50 governors and 50 state attorneys general, and their staffs. This bouillabaisse of state cybersecurity laws makes it impossible for the United States to develop a cohesive strategy to secure itself from increasingly persistent and advanced cyber threats. Although new cybersecurity threats emerge daily, many state cybersecurity laws are more than a decade old and have not changed, addressing the threats of the mid-aughts rather than today.[103]

First, companies should be required to notify individuals not only of breaches of their social security numbers and financial account information, but also of any personal data that reasonably could be contemplated of causing harm to their person or reputation. Because this conceivably could include data such as home address, email address, and private communications, this should be defined broadly. The United States should consider a definition of covered "personal data" that is in line with the General Data Protection Regulation in Europe: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[104]

---

[103] Jeff Kosseff, *Hamiltonian Cybersecurity*, WAKE FOREST L. REV. (forthcoming 2019).
[104] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 33 (EU).

This definition is not narrowly tied to a particular type of harm, and ensures that individuals (and regulators) will be aware of potential harms. Risk of harm thresholds for notifications should consider not only risks of economic harm, but also harm to individuals' privacy, safety, and reputation.

Second, companies should face specific and rigorous requirements to secure a similarly broad swath of personal data. Data security threats evolve at a rapid pace, as do the safeguards that best protect against these threats. For both political and practical reasons, legislatures cannot keep up with the new technological developments. If Congress passes a national data security law, it should delegate rulemaking authority to an expert agency, likely the FTC. The agency's experts could promulgate regulations that set forth specific requirements for safeguarding this more broadly defined category of personal information.

Third, just as companies are required to notify individuals of breaches of their personal information, Internet of Things device manufacturers and service providers should be obligated to notify individuals upon discovery of vulnerabilities that could compromise their privacy, security, or safety. For instance, if a webcam manufacturer learns of a vulnerability that could allow hackers to surreptitiously record people, the manufacturer should face a specific requirement—outside of general tort liability—to inform users and help remediate the problem.

Fourth, data security requirements should evolve to more comprehensively cover cybersecurity. These requirements should cover not only personal information, but also the security of devices, systems, and networks. California's Internet of Things statute is a good first step, but a more comprehensive bill at the national level would address issues beyond password security, and would allow for regulations that require more specific and effective technological safeguards. To be sure, a number of cyber-related harms are caused by compromises of data confidentiality, however, as seen with cases such as the hijacking of webcams, cybersecurity reaches beyond mere data breaches.

Fifth, the government should collaborate with service providers and other companies to crack down on cyber-harassment, sextortion, and similar acts. The FBI and state and local law enforcement may be best positioned to understand how, for instance, sextortionists remotely hijack webcams. Just as the Department of Homeland Security, through US-CERT, shares information with companies regarding botnets and software vulnerabilities, the government should work with service providers to ensure that they are aware of emerging threats that target individuals (such as IP addresses associated

with bad actors, tools that they use to carry out their acts, and vulnerabilities that they exploit).

Sixth, once cybersecurity is viewed as more than an economic threat, but also a threat to individual safety, the nation could begin more comprehensive efforts to educate the public about cybersecurity. Beginning in elementary school and lasting into adulthood, individuals should be educated about online safety and methods to reduce the likelihood of falling victim to a cybercriminal. Although there are some steps to educate the public, such as the October National Cybersecurity Awareness Month, cybersecurity should be an integral part of classroom education, and it should receive the same level of attention from law enforcement as non-digital crimes and wrongdoings.

IV. CONCLUSION

Nearly two decades ago, state legislatures recognized that identity theft and other economic crimes required laws to protect data security. As individuals continue to be victimized online, we need to reimagine cybersecurity laws to address these broader harms. Cybersecurity laws should protect a wider range of data, and they should require manufacturers and service providers to adopt safeguards that protect individuals. To be sure, we cannot rely on cybersecurity law alone to prevent harms to individuals. Like retrospective tort lawsuits and criminal prosecution, cybersecurity laws only address part of the problem. However, cybersecurity should be one part of a more comprehensive long-term strategy to make the Internet safer for all.