# INFORMATION LAW JOURNAL

A Publication of the Information Security & Internet of Things Committees
ABA Section of Science & Technology Law

SPRING 2018 VOLUME 9 ISSUE 2 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.


## New Book for Data Protection Officers under the GDPR – Inside and Outside the EU

By Thomas Shaw

The General Data Protection Regulation (GDPR) starts from May 25 of this year. One of the new specifications is for a Data Protection Officer (DPO), mandatory in some cases and voluntary in others. GDPR applies to both firms located within the EU and non-EU companies which process personal data of EU residents. *Read more*

## Fake News Meets Social Media: Is There a Solution?

By Kornel Rady and Dustin Mauck

Conspiracy theories about prominent figures and historically significant events have always been a puzzling component of American life. From multiple shooters in the JFK assassination to NASA faking the moon landing, Americans never fail to be skeptics. However, with the recent invention of social media the spread *Read more*

## States Come Out Fighting as the Battle Over the Repeal of Net Neutrality Continues On

By Sherri Marie Carr

On December 14, 2017, the Federal Communications Commission (FCC) voted down party lines, with the Restoring Internet Freedom Declaratory Ruling, Report and Order, and Order, to repeal the net neutrality regulations put in place in 2015; Title 47 U.S. Code Section 161 (b) may have provided the FCC *Read more*

## The Cyber Cold War: How Stockpiling Malware Moves the World Closer to a Technological Armageddon

By Justin Evans

The world is currently experiencing a digital revolution, where access to the internet and technology has increased significantly in all age groups. Technology has improved the quality of life for everyone, *Read more*

## How Belgium is preparing for life under the GDPR

By Maarten Stassen

May 25 is marked in red in the agendas of privacy professionals around the globe. The day on which the General Data Protection Regulation (GDPR) becomes applicable will also be the birthdate of the new Belgian data protection regulator. Belgium already has a data protection regulator, but its structure, *Read more*

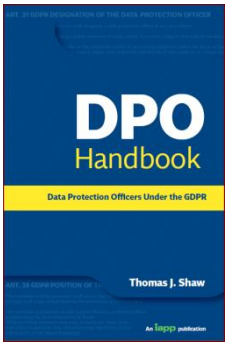
## ****Editor's Message****

We are into the ninth full year of publishing the *Information Law Journal* each quarter, continuing to welcome authors and readers from across the ABA. This issue again presents articles focusing on various aspects of leading-edge domestic and international practice in information, Internet, and emerging technologies law. More than 200 authors have written for the *Information Law Journal* and antecedents. Four authors are writing here for the first time.

Our next issue (Summer 2018) is scheduled to be published in June 2018. All readers of the *Information Law Journal* may share their experiences and knowledge with their fellow professionals by writing an article. Every qualified submission within the scope and requirements as explained in the **Author Guidelines** will be published. The issue following the next issue (Autumn 2018) is scheduled to be published in September 2018.

## New Book for Data Protection Officers under the GDPR – Inside and Outside the EU

***By Thomas Shaw***




*The General Data Protection Regulation (GDPR) starts from May 25 of this year. One of the new specifications is for a Data Protection Officer (DPO), mandatory in some cases and voluntary in others. GDPR applies to both firms located within the EU and non-EU companies which process personal data of EU residents.* So it likely applies to just about any firm involved in global business. With many new obligations and a wider territorial scope, obtaining and maintaining a deep enough understanding of the GDPR's rules is not a simple proposition even for the deepest privacy departments of the largest EU firms, let alone SMEs and non-EU companies. The DPO position is a way to ascertain and monitor the compliance status of controllers and processors located inside or outside the EU.

A new book available in March 2018, DPO Handbook – Data Protection Officers under the GDPR, is a hands-on manual essential for all DPOs. It starts by introducing the role of DPO, explaining why one would be needed, the jobs skills and professions of a DPO under the GDPR, and whether to insource or outsource the role. Once a DPO is identified and engaged, they will need to undertake a variety of startup tasks trying to initially evaluate the organization's compliance with the GDPR and suggest remediations. While the controller or processor at all times remain legally responsible for complying with the GDPR, the role of DPO is to facilitate that compliance through advice, assessments, and audits. One aspect of that compliance are the communications channels with the board of directors, with data protection supervisory authorities enforcing the GDPR, and with data subjects may need assistance in exercising their data subject rights.

The book goes through the entire lifecycle of the DPO's many tasks, from the GDPR's general requirements to the more detailed tasks required of the role. These include assessing and auditing GDPR compliance, advising on data protection impact assessments (DPIAs), assessing and advising on information security, data breach response, anonymization, Privacy by Design, and transfers outside the EEA. It also addresses how to deal with controllers or processors who are located outside the EU and when the DPO themselves may be located outside the EU. In the final chapter, the book illustrates how to apply all these techniques using practical case studies of an EU SME and a non-EU multinational. Everything that a DPO under the GDPR must know and do to competently and comprehensively perform their role to the highest standards of professional skill is described in detail in this book.

***Thomas J. Shaw, Esq.*** *is an EU-based attorney at law, CPA, CIPP/EU, CIPP/US, CRISC, ECM$^{M}$, CISM, ERM$^{P}$, CISA, CGEIT and CCSK who runs DPO Services, which provides Data Protection Officer (DPO) functions for all firms required to comply with the EU's new General Data Protection Regulation. He is asst. professor of emerging technologies, information, and Internet law at leading universities in the EU, and author of the books* DPO Handbook – Data Protection Officers under the GDPR (2018); Emerging

Technologies Law – Global Practice (2016-18); Information and Internet Law – Global Practice (2016-18); World War I Law and Lawyers – Issues, Cases, and Characters (2014); Cloud Computing for Lawyers and Executives - A Global Approach, Second edition (2013); World War II Law and Lawyers – Issues, Cases, and Characters (2013); Children and the Internet – A Global Guide for Lawyers and Parents (2012); Cloud Computing for Lawyers and Executives – A Global Approach (2011); *lead author/editor of* Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists (2011), *and editor/founder of this publication and its antecedents. He can be reached at thomas@tshawlaw.com*.

## Fake News Meets Social Media: Is There a Solution?

***By Kornel Rady and Dustin Mauck***


*Conspiracy theories about prominent figures and historically significant events have always been a puzzling component of American life. From multiple shooters in the JFK assassination to NASA faking the moon landing, Americans never fail to be skeptics. However, with the recent invention of social media the spread* of these theories has become far less innocent. Today's conspiracy theories and their viral growth on social media have created a dangerous phenomenon called fake news.

There is no single definition of fake news as the term has been attached as a universal term to address a variety of news reports. The category of fake news focused on in this paper revolves around the creation and dissemination of fabricated stories on social media.[1] Fake news on social media is frequently well disguised and looks identical to many of the far more legitimate news articles from reputable sources.[2] The term has gained prominence mainly because of the recent U.S election and President Trump's common use of the term when referring to the mainstream media.[3] During the 2016 election fake news was widely consumed on social media platforms and many believe that it influenced the outcome of the race.[4]

There are a multitude of fake news stories, but one that best exemplifies the danger originating from fake news is known as "Pizzagate."[5] In this particular fake news story there were accusations from conspiracy theorists that Hillary Clinton was participating in a child sex ring.[6] The theory also involved Clinton campaign chairman John Podesta and claimed that he was involved in satanic rituals associated with the child sex ring.[7] These rumors spread all over social media and the Internet.[8] Twitter contributed significantly to the spread of this theory as evidenced by one tweet that received more than six thousand retweets.[9] All of this hysteria and fake news spread to conspiracy theorists like Alex

---

[1] David O. Klein & Joshua R. Wueller, Fake News: A Legal Perspective, 20 J. INTERNET L. 1, 6 (2017).
[2] James Carson, What Is Fake News? Its Origins and How It Grew In 2016, THE TELEGRAPH (Mar. 16, 2017), http://www.telegraph.co.uk/technology/0/fake-news-origins-grew-2016/.
[3] See id.
[4] See id.
[5] Klein & Wueller, supra note 1, at 1.
[6] Marc Fisher, John Woodrow Cox, & Peter Hermann, Pizzagate: From Rumor, To Hashtag, To Gunfire In. D.C., THE WASHINGTON POST (Dec. 6, 2016), https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html?utm_term=.075fd5a3ccb4.
[7] See id.
[8] See id.
[9] See id.

Jones.[10] Eventually, the "reality" of Pizzagate grew so unbearable for an individual named Edgar Welch, that he drove from North Carolina to Washington D.C. to investigate.[11] He arrived armed with an assault rifle at Comet Ping Pong, which was the pizzeria where the supposed child sex ring was located.[12] He searched the restaurant and unsurprisingly found nothing to corroborate the stories he read online.[13] Fortunately, he was apprehended and no one was injured in the bizarre situation.[14]

The spread of fake news based on completely fabricated information has the ability to do much more harm than that of what occurred at Comet Ping Pong, as it threatens the very nature of America's informed democracy.[15] Despite this threat the legal implications of spreading and creating fake news remains unclear. Do social media platforms have a duty to prevent the spread of fake news? Are there concerns about free speech if fake news bans are employed on social media? These are just a few of the most important legal questions related to the conundrum.

This paper summarizes the applicable laws that have the potential to originate from fake news on social media. It also discusses changes that social media platforms like Facebook have employed to combat fake news. Examples of fake news lawsuits against these platforms are also analyzed. Lastly, suggestions to remedy the problem of fake news conclude the paper.

**Current and Proposed Laws Addressing Fake News**

There are a variety of laws that may be applicable to fake news on social media. Despite this there are none in the United States that have been enacted specifically to combat the problem. It will remain interesting to watch legislatures across the country debate the issue that has become so prominent in our society.

i. Section 5 of the Federal Trade Commission Act

One of the entities that could regulate the spread of fake news is the Federal Trade Commission ("FTC").[16] The FTC has broad authority to address a variety of matters that give it the foundation to specifically regulate those participating in the creation and dissemination of fake news.[17] The FTC can

[10] Tom O'Connor, Alex Jones Apologizes For 'Pizzagate' Fake News, NEWSWEEK (Mar. 24, 2017), http://www.newsweek.com/alex-jones-apologize-pizzagate-fake-news-574025.
[11] Fisher, Cox, & Hermann, supra note 6.
[12] See id.
[13] See id.
[14] See id.
[15] Carson, supra note 2.
[16] 21 No. 10 CYBERSPACE LAWYER NL 5.
[17] See id.

exert this authority through Section 5 of the Federal Trade Commission Act.[18] Section 5 establishes that "unfair or deceptive acts or practices in or affecting commerce" are unlawful.[19]

Use of Section 5 to regulate fake news is exemplified *by Federal Trade Commission et al. v. LeadClick Media LLC* in the Second Circuit.[20] In this particular case LeadClick, a marketing company, looked to recruit online publishers to create fake news sites to market products.[21] The majority of the Internet traffic to a client, LeanSpa, came from LeadClick's fake news websites.[22] These fake news websites looked very realistic and had similar characteristics to those of other news sites.[23] These fake news sites had articles claiming that all of LeanSpa's products were effective and had comment sections corroborating the articles.[24]

LeadClick did not create these specific websites, but hired affiliates by LeadClick were using these sites commonly.[25] By knowingly approving the use of the websites and providing these sites content, LeadClick violated Section 5 of the Federal Trade Commission Act.[26] The FTC alleged that these specific violations showed it engaging in a deceptive act or practice.[27] Proving a deceptive act or practice under Section 5 requires "a representation, omission, or practice, that is likely to mislead consumers acting reasonably under the circumstances, and the representation, omissions, or practice is material."[28] Any intent to deceive is not necessary to prove the deceptive act or practice rather it is only important that the actions would likely mislead reasonably acting consumers.[29] Combining these elements with the facts, the Second Circuit decided LeadClick deceived LeanSpa and consumers.[30]

This case does not speak exactly to the newest and more commonly referenced fake news that travels across social media but it does provide an example of what it would take to shut down fake news producers. The FTC, under Section 5, could have the ability to bring enforcement actions against those who create and disseminate the type of fake news concerning most today.[31] For example, if companies

---

[18] 47 A.L.R. Fed. 393 (Originally published in 1980).
[19] 15 U.S.C.A. § 45 (West).
[20] By Melissa J. Sachs, Manager of "Fake News Sites" Liable for Deceiving Consumers, 2nd Circuit Says, 34 WESTLAW JOURNAL COMPUTER AND INTERNET 2 (2016).
[21] See id.
[22] Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 162-63 (2d Cir. 2016).
[23] See id. at 162-64
[24] See id. at 164.
[25] See id. at 164.
[26] See id. at 162.
[27] See id. at 167.
[28] Id. at 168; *FTC v. Verity Int'l, Ltd.*, 443 F.3d 48, 63 (2d Cir. 2006) (quoting *In re Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 165 (1984)).
[29] Fed. Trade Comm'n v. LeadClick Media, LLC, 838 F.3d 158, 168 (2d Cir. 2016).
[30] See id. at 172.
[31] Callum Borchers, How The Federal Trade Commission Could (Maybe) Crack Down On Fake News, THE WASHINGTON POST (Jan. 30, 2017), https://www.washingtonpost.com/news/the-fix/wp/2017/01/30/how-the-federal-trade-commission-could-maybe-crack-down-on-fake-news/?utm_term=.323c10c21683; Internet Marketers of Dietary Supplement and Skincare Products Banned from Deceptive Advertising and Billing Practices, FEDERAL TRADE COMMISSION (NOV. 15, 2017),

are established to purposefully create fabricated news and share it on social media this could violate the deceptive prong of Section 5.[32] So far, the FTC has only cracked down on fake news sites that sell products.[33] However, there is interest in expanding its reach to examine the type of fake news most prevalent in current events.[34]

Another potential option for the FTC could be in the form of enforcement actions against social media companies that are the platforms for the spread of fake news. However, this is much less likely to occur than the FTC going after the producers of fake news. In the end, it will remain interesting to see if the FTC tests its enforcement ability in the coming months as the fake news phenomena remains prevalent.

ii. Defamation

Suing the producer of fake news for defamation is another option for those who have suffered from fake news.[35] The most relevant type of defamation originating from fake news on social media would be libel.[36] Libel is a written or published defamatory statement.[37] The elements of defamation vary across the country, but a standard example includes: "(1) the publication of a false statement of fact to a third party, (2) that was defamatory concerning the plaintiff, (3) with the requisite degree of fault, and (4) damages, in some cases."[38] Noting these simple requirements, with a few caveats, it is clear that fake news aimed at a private and even public official could lead to success for plaintiffs.[39]

Despite some of these cases seeming relatively straightforward for plaintiffs there are a few roadblocks. The first is the constitutional protection for free speech that the First Amendment provides.[40] Facebook and others are facing criticism about proposed restrictions for this very reason.[41] In addition

---

https://www.ftc.gov/news-events/press-releases/2017/11/internet-marketers-dietary-supplement-skincare-products-banned.

[32] Id.

[33] Id.

[34] Id.

[35] Klein & Wueller, supra note 1, at 6.

[36] §1:10.Common-law libel/slander distinction, 1 Law of Defamation § 1:10 (2d ed.).

[37] §1:11.Common-law libel/slander distinction—In general, 1 Law of Defamation § 1:11 (2d ed.).

[38] §1:34.Elements of the modern cause of action, 1 Law of Defamation § 1:34 (2d ed.); Tipping v. Martin, 2016 WL 397088, *3 (N.D. Tex. 2016) (quoting In re Lipsky, 460 S.W.3d 579, 593, 43 Media L. Rep. (BNA) 1793 (Tex. 2015), citing WFAA-TV, Inc. v. McLemore, 978 S.W.2d 568, 571, 26 Media L. Rep. (BNA) 2385 (Tex. 1998).

[39] The Lipsky case lays out some of the caveats to succeeding in defamation case. It states:

> "The status of the person allegedly defamed determines the requisite degree of fault. A private individual need only prove negligence, whereas a public figure or official must prove actual malice. WFAA–TV, Inc., 978 S.W.2d at 571. "Actual malice" in this context means that the statement was made with knowledge of its falsity or with reckless disregard for its truth. Huckabee v. Time Warner Entm't Co., 19 S.W.3d 413, 420 (Tex.2000). Finally, the plaintiff must plead and prove damages, unless the defamatory statements are defamatory per se. Waste Mgmt. of Tex., 434 S.W.3d at 162 n.7."

In re Lipsky, 460 S.W.3d 579, 593 (Tex. 2015).

[40] §1:34.Elements of the modern cause of action, 1 Law of Defamation § 1:34 (2d ed.)

[41] Brook Masters, Social Media Encounters Maelstrom Over Free Speech, FINANCIAL TIMES (Apr. 7, 2017), https://www.ft.com/content/eebbbc08-1b8c-11e7-a266-12672483791a.

to the strong protection the First Amendment brings, another tool for defendants is known as an anti-SLAPP law.[42] This law allows defendants to dismiss lawsuits that may infringe on a defendant's rights to free speech if used to focus on matters of public concern.[43] Yet another defense that could protect companies spreading fake news is Section 230 of the Communication Decency Act of 1996.[44] This particular law protects platforms like Facebook and Twitter from the actions of their users.[45] Regardless of these protective measures for defendants some of the fake news defamation cases are likely to be quite favorable for plaintiffs.

There are quite a few recent examples relevant to defamation and fake news that have taken place. Two of them include Alex Jones and the fake news that is frequently passed along by his media organization Infowars.[46] The first is related to none other than Comet Ping Pong and its owner James Alefantis.[47] Alex Jones recently apologized to Alefantis regarding the Pizzagate story and some say this is because he was fearful of facing a defamation lawsuit.[48] In the other example, Alex Jones is facing a lawsuit over his spread of fake news attacking the yogurt company Chobani on Twitter and YouTube.[49] The fake news accused Chobani of importing migrant rapists.[50] In the complaint, Chobani accused Jones and Infowars of defamatory reports on social media and the Internet.[51] Jones and Chobani ultimately settled this case, but it is likely not to be the last party to accuse fake news creators of defamation.[52]

iii. Proposed California Fake News Laws

States are also positioned to take action in their own legislatures to address the problem of fake news. California is the first one to attempt to address fake news through its very own Assembly Bill 1104

[42] SLAPP lawsuits are "strategic lawsuits against public participation" and can frequently limit free speech and frequently place defendants in strong positions against defamation suits. See Klein & Wueller, supra note 1, at 7.
[43] See id.
[44] See id.; 47 U.S.C. § 230.
[45] See id.; 47 U.S.C. § 230.
[46] Christine Hauser, Chobani Yogurt Sues Alex Jones Over Sexual Assault Report, THE NEW YORK TIMES (Apr. 25, 2017), https://www.nytimes.com/2017/04/25/business/chobani-alex-jones.html; Jonathan Tilove, Now That's Real News. On Alex Jones' Pizzagate Apology And The Perils Of Subbing One Conspiracy For Another., THE AUSTIN AMERICAN-STATESMAN (Mar. 27, 2017), http://politics.blog.mystatesman.com/2017/03/27/now-thats-real-news-on-alex-jones-pizzagate-apology-and-the-perils-of-subbing-one-conspiracy-for-another/.
[47] Tilove, supra note 46.
[48] See id.
[49] Hauser, supra note 46.
[50] See id.
[51] See id.
[52] Christine Hauser, Alex Jones Retracts Chobani Claims to Resolve Lawsuit, NEW YORK TIMES (May 17, 2017), https://www.nytimes.com/2017/05/17/us/alex-jones-chobani-lawsuit.html.

introduced in February of 2017.[53] This particular bill was initially introduced to make it illegal to publish and spread fake news concerning politics.[54]

The final version that was signed into law on October 12, 2017 makes it "unlawful for a person, with intent to mislead, deceive, or defraud, to commit an act of political cyberfraud."[55] The law now defines political cyberfraud as a:

knowing and willful act concerning a political Web site that is committed with the intent to deny a person access to a political Web site, deny a person the opportunity to register a domain name for a political Web site, or cause a person reasonably to believe that a political Web site has been posted by a person other than the person who posted the Internet Web site, and would cause a reasonable person, after reading the Internet Web site, to believe the site actually represents the views of the proponent or opponent of a ballot measure or of a candidate for public office.[56]

This definition most likely encompasses some politically focused fake news on websites that can be spread on social media. However, the original bill was far more aggressive in restrictions aimed at those creating and circulating fake news.[57] The original language from the bill before it was pulled and amended, made it illegal to publish or circulate "a false or deceptive statement designed to influence" decision-making on issues or candidates by citizens at the voting booth.[58] The more pointed language was removed after criticism from numerous groups including the ACLU and the Electronic Frontier Foundation.[59] The Electronic Frontier Foundation was concerned that it would threaten free speech and would be ineffective in battling fake news.[60]

Another pending piece of California legislation aims to use education as a tool to help combat fake news.[61] Senator Bill Dodd is attempting to add media literacy to California's school curriculum.[62] He hopes that this will allow students to identify and combat fake news on a variety of different platforms including social media.[63] Dodd's bill cites a Stanford University study that found "82 percent of middle school students struggled to distinguish advertisements from news stories."[64] This statistic exemplifies

---

[53] Cyber Fraud Bill Would Make Political 'Fake News' Against The Law, CBS Los Angeles (Mar. 31, 2017), http://losangeles.cbslocal.com/2017/03/31/cyber-fraud-bill-would-make-political-fake-news-against-the-law/.
[54] See id.
[55] Cal. Elec. Code § 18320 (West).
[56] Id.
[57] Cyber Fraud Bill Would Make Political 'Fake News' Against The Law, supra note 53.
[58] Id.
[59] Susan Seager, 'Disastrous for Free Speech': Lawmaker Pulls Bill to Ban Fake News, THE WRAP (Mar. 28, 2017), http://www.thewrap.com/lawmaker-ed-chau-pulls-bill-to-ban-fake-news/.
[60] See id.
[61] Jordan Ball, California Bill Pushing To Teach Curriculum On Media Literacy, How To Spot Fake News, ABC (Apr. 27, 2017), http://www.abc10.com/news/local/california/california-bill-pushing-to-teach-curriculum-on-media-literacy-how-to-spot-fake-news/434107406.
[62] See id.
[63] See id.
[64] See id.

the need for such changes in school curriculums. This bill also represents the other side of the fake news fight, which focuses on users themselves combatting fake news. The combination of this education and effective changes by social media companies, as discussed below, could lead to productive and more constructive media consumption.

**International Fake News Social Media Laws**

With the growth of fake news on social media affecting more than just American society, some countries have started to investigate potential solutions. One country that has yet to pass legislation but is considering it is the United Kingdom.[65] In March of 2017 there was the beginning of a parliamentary inquiry by the digital, culture, media and sport committee into fake news and its effects.[66] The investigation specifically focused on methods Facebook utilizes to handle complaints and protect the Facebook community.[67] The chair of this committee, Damian Collins, is steadfast in his criticisms of Facebook's fake news and is convinced that people will leave Facebook if it continues.[68] He also believes that democracy is generally threatened by disinformation and that his committee should address the issue.[69]

As recently as February 8, 2018 the committee questioned senior officials of Facebook, Twitter and Google. [70] During these hearings it seemed as if the committee grew further frustrated with the inaction of these technology companies.[71] There has been even the threat of sanctions for such inaction by Collins after Russian bots were found to have been posting during the United Kingdom's EU referendum in 2016.[72]

Australia is another country that has discussed investigating fake news and the social networks it spreads through.[73] At least one Australian senator believed that the government should potentially address the issue through legislation.[74] However, there is some concern that such a debate would take

[65] Jane Martinson & Jasper Jackson, Fake News Inquiry To Review Social Networks' Complaints Procedures, THE GUARDIAN (Mar. 8, 2017), https://www.theguardian.com/media/2017/mar/08/fake-news-inquiry-social-networks-complaints-policy-facebook.
[66] See id.
[67] See id.
[68] See id.
[69] See id.
[70] Annabelle Dickson, UK 'fake news' committee says patience is running out, POLITICO (FEB. 9,2018), https://www.politico.eu/article/uk-fake-news-committee-says-patience-is-running-out/.
[71] See id.
[72] See id.
[73] Amy Remeikis, Parliament To Launch Inquiry Into "Fake News' In Australia, THE SYDNEY MORNING HERALD (Mar. 30, 2017), http://www.smh.com.au/federal-politics/political-news/parliament-to-launch-inquiry-into-fake-news-in-australia-20170330-gv9xwz.html.
[74] See id.

away the focus from other issues in the country.[75] It will be interesting to see how both the Australians and the British draft legislation in a time where fake news remains highly relevant.

Germany, however, has done more than just have a simple investigation or conversation on the topic. On April 5th Chancellor Angela Merkel's cabinet approved legislation that would fine social media companies for failing to remove fake news.[76] This approval was followed by the German parliament also passing the law in late June of 2017.[77] The law could lead to social networks facing fines of up to $53 million for failing to follow the strict requirements of the law.[78] One condition includes that social networking companies must remove violating content within 24 hours.[79] This requirement is clearly stringent and would also force social media companies to work with fact-checkers in Germany to abide by the law.[80]

This German legislation is the most concrete example of where the law is trending overseas. Because of its novelty and severity it has received criticism.[81] There are also concerns about limiting free speech and actual compliance with the law if finalized.[82] Finding a balance between free speech and such a law will be a difficult task according to writer Paul Crookston.[83] He claims that too many resources from these companies will be spent on policing user content and that this could lead to unnecessary control of opinionated posts.[84] This debate will likely continue as other countries attempt to address the issue of fake news on social media.

Also relevant to this legislation is a lawsuit that may have contributed to the momentum behind proposing the law.[85] The suit revolved around Anas Modamani, a Syrian refugee, who took a "selfie" with Angela Merkel.[86] This picture and others capturing the moment ended up becoming widely used to positively define Germany's commitment to helping refugees.[87] Unfortunately, some of these pictures were also used by a variety of people to spread fake news accusing him of being one of the

---

[75] See id.
[76] Germany Approves Bill Curbing Online Hate Crime, Fake News, CNBC (Apr. 6, 2017), http://www.cnbc.com/2017/04/06/germany-fake-news-fines-facebook-twitter.html.
[77] Germany approves plans to fine social media firms up to €50m, THE GUARDIAN (Jun. 30, 2017), https://www.theguardian.com/media/2017/jun/30/germany-approves-plans-to-fine-social-media-firms-up-to-50m.
[78] Paul Crookston, German Official Seek To Control 'Fake News' online – and Hope The EU Will Follow Suit, NATIONAL REVIEW (Apr. 7, 2017), http://www.nationalreview.com/corner/446542/fake-news-hate-speech-law-germany-targets-facebook-twitter.
[79] See id.
[80] See id.
[81] Crookston, supra note 78.
[82] See id.
[83] See id.
[84] See id.
[85] Philip Oltermann, Syrian Who Took Merkel Selfie Sues Facebook Over 'Defamatory' Posts, THE GUARDIAN (Jan. 12, 2017), https://www.theguardian.com/world/2017/jan/12/syrian-who-took-merkel-selfie-sues-facebook-over-defamatory-posts.
[86] See id.
[87] See id.

Brussels bombers amongst other false allegations.[88] Eventually, Modamani sued Facebook for failing to remove the posts defaming him.[89] He ended up losing the lawsuit because the district court decided Facebook was not sufficiently involved in the process.[90] Instead the court blamed users for defamatory material and this absolved Facebook from any liability.[91] Regardless of the outcome his lawsuit likely contributed to the discussion that led to the German law passing..

**Policy Changes by Social Media Companies to Address Fake News**

Noting the issues and concerns about fake news, Facebook even without fake news specific laws, has started addressing the issue. The criticisms aimed at Facebook after the 2016 U.S. election led Facebook CEO and founder Mark Zuckerburg to take action.[92] Facebook initially addressed some of the issues surrounding fake news by labeling certain posts as "disputed" with links to a variety of websites that measure the validity of the questionable article.[93] It also altered its formula for trending news stories in its response to the issues surrounding the 2016 election to "consist of topics covered by several publishers."[94] Previously it was focused on subjects that had the most comments and shares.[95] However, these initial attempts have been replaced by two major changes announced in December of 2017.[96] The first is that the disputed flags will be replaced by links to content from "more reputable publishers."[97] The second will be a new study by Facebook to learn how people analyze the news consumed on the site.[98]

Despite these attempts some changes in the news feed have led to even more criticism.[99] Recent changes by Facebook to its news feed have started prioritizing friends and family posts over posts from publishers.[100] Some believe that this has actually exacerbated the fake news problem.[101] In the end, these actions are likely necessary in order to preempt strong government action. A former Facebook

---

[88] See id.
[89] See id.
[90] German Court Rejects Injunction For Facebook In Syrian Selfie Case, FORTUNE (Mar. 7, 2017), http://fortune.com/2017/03/07/german-court-rejects-injunction-for-facebook-in-syrian-selfie-case/.
[91] See id.
[92] Jordan Crook, Fake Times, TECHCRUNCH (Mar. 19, 2017), https://techcrunch.com/2017/03/19/facebook-will-never-take-responsibility-for-fake-news/.
[93] Steven Rosenbaum, Facebook Takes On Fake News, FORBES (Mar. 8, 2017), https://www.forbes.com/sites/stevenrosenbaum/2017/03/08/facebook-takes-on-fake-news/#7a1cfd512220.
[94] Facebook Takes Aim at 'Fake News' With New 'Trending' Formula, THE TELEGRAPH (Jan. 26, 2017), http://www.telegraph.co.uk/technology/2017/01/26/facebook-takes-aim-fake-news-new-trending-formula/.
[95] See id.
[96] Catherine Shu, Facebook will ditch Disputed Flags on fake news and display links to trustworthy articles instead, TECHCRUNCH (Dec. 20, 2017), https://techcrunch.com/2017/12/20/facebook-will-ditch-disputed-flags-on-fake-news-and-display-links-to-trustworthy-articles-instead/.
[97] Id.
[98] See id.
[99] Swapna Krishna, Facebook's News Feed change may amplify fake news, ENGADGET (Jan.16, 2018), https://www.engadget.com/2018/01/16/facebook-news-feed-tweak-could-make-fake-news-worse/
[100] Id.
[101] See id.

executive Adam D'Angelo substantiated this thought by mentioning that if efforts fail in combatting fake news the U.S. government will likely take a larger role in the fight.[102]

**Recommendations for New Laws and Social Media Policies Addressing Fake News**

There are a multitude of potential solutions that can remedy the fake news problem. One modification that could positively impact social networks is more stringent restrictions on bots. This change would come in the form of a law or regulation requiring social media companies to implement stricter standards regarding the elimination and prevention of bots that have peddled fake news across social media.[103] Ridding social media of these fake accounts spreading disinformation could prevent fake news from going viral.[104] Twitter for example states that it strictly enforces its restrictive policy against such automated accounts.[105] Despite its best efforts there are still hundreds of thousands of bots spamming Twitter.[106]

This hypothetical law would also likely have a larger effect on Twitter than on Facebook.[107] Recent studies have found that bots are more actively posting fake news than humans on Twitter and the opposite is the case on Facebook.[108] The law would also not be unprecedented, as Facebook has already eliminated 30,000 fake accounts for their roles in fake news in France.[109]

This suggested law does a good job of hypothetically balancing free speech concerns while addressing the negative impacts of fake news. Finding equilibrium between these competing interests is the most difficult part of finding any remedy. A solution that could also succeed at finding this equilibrium is legislation aimed at increasing media literacy like that of California's bill. Social media platforms could also have modules they produce to help users identify fake news in conjunction with this legislation. Federalizing a law like California's is always difficult, but if the apprehension continues regarding foreign governments conducting "information operations" there should be broad action combatting it.[110]

---

[102] Mathew Ingram, Former Facebook Exec Says Government Action On Fake News Is a Real Possibility, FORTUNE (Apr. 25, 2017), http://fortune.com/2017/04/25/facebook-government-fake-news/.
[103] Gabe O'Connor & Avie Schneider, How Russian Twitter Bots Pumped Out Fake News During The 2016 Election, NPR (Apr. 3, 2017), http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election.
[104] Faye Flam, Fighting Fake News With Science, BLOOMBERG (Mar. 27, 2017), https://www.bloomberg.com/view/articles/2017-03-27/fighting-fake-news-with-science.
[105] Massive Networks Of Fake Accounts Found On Twitter, BBC (Jan. 24 2017), http://www.bbc.com/news/technology-38724082.
[106] See id.
[107] Joon Ian Wong, Bots Aren't Spreading Fake News on Facebook; Humans Are, QUARTZ (Apr. 28, 2017), https://qz.com/971465/facebook-research-paper-bots-arent-spreading-fake-news-on-facebook-humans-are-fb/.
[108] See id.
[109] See id.
[110] Information Operations and Facebook, FACEBOOK (Apr. 27, 2017), https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

**Conclusion**

Fake news and its presence on social media has become one of the most important issues of our time. Its ability to alter elections and even drive people to cause physical harm is unprecedented. Countries have faced a variety of propaganda before, but no propaganda of the past can match its latest iteration. The ability to traverse social media in seconds and be consumed by millions makes fake news more dangerous than any government sanctioned propaganda campaign from the Cold War.

Combatting this issue on social media will be especially complex. As mentioned previously, there are legitimate concerns about limiting free speech if social media companies were to act too stringently. Conversely, will the tagging of posts as "disputed" really provide a solution? It will be difficult for Facebook and others to find this balance. Additionally, working with stakeholders like Facebook and Twitter should be at the crux of any law moving forward. Establishing such a working relationship between governments and the private sector will be necessary for success.

In the end, social media's change from primarily a social networking platform to one that provides people with their news will require a drastic shift from social media companies. This shift will require a solution to the nuanced issue of fake news. Despite the difficulty this is the industry that gave us unprecedented tools that completely changed the way humans interact. With this pedigree, there is no industry better positioned to solve such a challenging problem. Finally, they are also not alone in this fight, as it is also up to every citizen to become more aware of their media consumption in order to combat one of the most complicated issues facing our society.

***Kornel "Kori" Rady*** *is a 3L at SMU Dedman School of Law and graduate of the University of Texas at Austin. He plans to practice commercial litigation after graduating.*

***Dustin Mauck*** *is a shareholder at intellectual property boutique RegitzMauck in Dallas. He provides legal representation in intellectual property, cybersecurity, and data privacy matters and disputes. Dustin is a graduate of the SMU Dedman School of Law, a Certified Information Privacy Professional (CIPP/US), and a registered patent attorney.*

## States Come Out Fighting as the Battle Over the Repeal of Net Neutrality Continues On

***By Sherri Marie Carr***

"*It shall be the policy of the United States to encourage the provision of new technologies and services to the public*."[1]

**The Repeal of Net Neutrality Regulations**

*On December 14, 2017, the Federal Communications Commission (FCC) voted down party lines, with the Restoring Internet Freedom Declaratory Ruling, Report and Order, and Order, to repeal the net neutrality regulations put in place in 2015;*[2] *Title 47 U.S. Code Section 161 (b) may have provided the FCC* with the ability to do so: "The Commission shall repeal or modify any regulation it determines to be no longer necessary in the public interest."[3] FCC Chairman Pai's statement detailed reasons for the repeal of the 2015 net neutrality regulations, including but not limited to,

> The main complaint consumers have about the Internet is not and has never been that their Internet service provider is blocking access to content. It's that they don't have access at all or enough competition. These regulations have taken us in the opposite direction from these consumer preferences. Under Title II [net neutrality], investment in high-speed networks has declined by billions of dollars.[4]

The FCC's news release dated December 14, 2017, states, "the FCC's action today has restored the jurisdiction of the Federal Trade Commission (FTC) to act when broadband providers engage in anticompetitive, unfair, or deceptive acts or practices."[5] However, many fear without the net neutrality regulations in place, internet service providers (ISPs) will be able to impede an end user's internet experience negatively by 1) slowing access and/or providing faster access to sites based on the ISP's discretion or whether you have paid more money for applicable sites and services, and 2) potentially blocking access altogether, among other things.[6] In response, some states are

---

[1] 47 US Code 157(a) available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapI-sec156.pdf (last visited Feb. 3, 2018)(emphasis added).
[2] FCC Restoring Internet Freedom Declaratory Ruling, Order, and Statements, available at https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order (last visited Feb. 3, 2018).
[3] U.S. Government Publishing Office, Title 47 US Code Section 161(b) Effect of Determination, available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapI-sec160.pdf (last visited Feb. 4, 2018).
[4] FCC Chairman Ajit Pai's Statement, Dec. 14, 2017, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A2.pdf (last visited Feb. 4, 2018).
[5] FCC New Release, dated December 14, 2017, available at https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order (last visited Feb. 3, 2018).
[6] Cecilia Kang, What's Next After the Repeal of Net Neutrality, The New York Times, Dec. 15, 2017, available at https://www.nytimes.com/2017/12/15/technology/net-neutrality-repeal.html (last visited Feb. 4, 2018).

implementing state level net neutrality laws; states are utilizing a variety of approaches, in doing so. Net neutrality regulation by the states, though, could cause federal preemption issues to emerge.

**Federal Preemption Explained**

Article VI of the United States Constitution (Constitution) states,

> This Constitution, and the laws of the United States which shall be made in pursuance thereof, and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land; and the judges in every State shall be found thereby, anything in the Constitution or laws of any State to the contrary notwithstanding.[7]

This portion of the Constitution has been interpreted to mean that Congress - and those agencies with powers delegated by Congress - have the ability to preempt state laws, as long as it is within the Constitutional parameters given to the federal government.[8]

Federal preemption is based on Article VI of the Constitution and deprives states of their power to legislate in particular areas, regardless of if there is a conflict existing between a federal law and a state law.[9] Since states lose their abilities to create laws in applicable areas through preemption, any challenges by states of federal laws governing a preempted area is almost futile, as the merits of substantive issues between federal and state laws are not addressed.[10] The federal law simply controls over particular areas through preemption, even if states want to legislate differently.

**FCC and FTC Memorandum of Understanding[11]**

The FCC and FTC shared a draft Memorandum of Understanding (MOU) on December 11, 2017 – three days before the FCC's vote.[12] The MOU outlined how both agencies would collaboratively address "online consumer protection efforts following the adoption of the Restoring Internet Freedom Order."[13] That order is also known as the repeal of net neutrality.[14] The order designates the FTC as the

---

[7] Edward S. Corwin's, The Constitution and What It Means Today, Revised by Harold W. Chase and Craig R. Ducat, Princeton University Press, 1978, p. 272.
[8] James C. Sturdevant and F. Paul Bland, Jr., Federal Preemption Cases: Reflections On The U.S. Supreme Court's Busy Docket, February 2008, available at http://www.plaintiffmagazine.com/item/federal-preemption-cases-reflections-on-the-u-s-supreme-court-s-busy-docket (last visited Feb. 3, 2018).
[9] Stephen A. Gardbaum, Nature of Preemption , 79 Cornell L. Rev. 767, 771 (1994) available at http://scholarship.law.cornell.edu/clr/vol79/iss4/1 (last visited Feb. 3, 2018).
[10] *Id*.
[11] This section originally appeared in the American Business Law Today's Month-in-Brief Internet Law and Cybersecurity section for the month of January 2018 available at https://businesslawtoday.org/month-in-brief/january-brief-internet-law-cyber-security-2018/ (last visited Feb. 4, 2018).
[12] FTC, FCC Outline Agreement to Coordinate Online Consumer Protection Efforts Following Adoption of The Restoring Internet Freedom Order, Dec. 11, 2017, available at https://www.ftc.gov/news-events/press-releases/2017/12/ftc-fcc-outline-agreement-coordinate-online-consumer-protection?utm_source=govdelivery (last visited Feb. 3, 2018).
[13] *Id*.

appropriate policing agency over ISP conduct, which includes ensuring that providers abide by promises they give to consumers, and requires "broadband Internet access service providers" to disclose their commercial terms of service, performance, and network management practices.[15]

**States Fight Back Against Repeal of Net Neutrality Regulations**

Despite assurances from the FCC and FTC, Montana Governor Steve Bullock signed Executive Order 3-2018, on January 22, 2018, which became effective immediately.[16] This Executive Order is an attempt to fight back against the FCC vote to repeal net neutrality.[17] According to Executive Order 3-2018, after July 1, 2018, service providers seeking a contract with the State of Montana must not engage in paid prioritization, block lawful content, unreasonably interfere with an end user's internet experience, or impair lawful internet use, among other things.[18]

In addition, New York Governor Andrew M. Cuomo followed Governor Bullock's lead and signed Executive Order 175 into law on January 24, 2018, to address the repeal of net neutrality, as well.[19] According to the New York Executive Order, "Affected State Entities [will] only enter into contracts with ISPs that adhere to net neutrality principles and [the purpose of the Executive Order is] to ensure that internet services provided to Affected State Entities, include net neutrality protections, and specifically state that ISPs may not block lawful content, applications, services, non-harmful devices, or applications that compete with other services provided by the ISP."[20] This applies to any contract or renewal dated March 1, 2018, or thereafter.[21]

Although not law, yet, the California Senate voted on January 29, 2018, to approve SB-460: "Communications: broadband Internet access service";[22] this bill will move next to the California State Assembly for a vote, which is expected to be approved, as well[23]. The Consumers Legal Remedies Act would be revised under this bill: "to prohibit specified actions by an Internet service provider . . . that

---

[14] *Id*.
[15] *Id*.
[16] State of Montana Executive Order 3-2018, available at http://governor.mt.gov/Portals/16/docs/2018EOs/EO-03-2018_Net%20Freedom.pdf?ver=2018-01-22-122048-023 (last visited Feb. 3, 2018).
[17] GOVERNOR BULLOCK PROTECTS NET NEUTRALITY IN MONTANA: BULLOCK FIRST GOVERNOR IN THE NATION TO IMPLEMENT ACTION TO SAFEGUARD INTERNET FREEDOM, Office of Steve Bullock, available at http://governor.mt.gov/Newsroom/governor-bullock-protects-net-neutrality-in-montana (last visited Feb. 3, 2018).
[18] State of Montana Executive Order, *supra*.
[19] Governor Andrew M. Cuomo Pressroom, Governor Cuomo Signs Executive Order to Protect and Strengthen Net Neutrality in New York, Jan. 24, 2018, available at https://www.governor.ny.gov/news/governor-cuomo-signs-executive-order-protect-and-strengthen-net-neutrality-new-york (last visited Feb. 4, 2018).
[20] New York Executive Order 175, Jan. 24, 2018, available at https://www.governor.ny.gov/sites/governor.ny.gov/files/atoms/files/EO_175.pdf (last visited Feb. 4, 2018).
[21] *Id*.
[22] California Legislature, Senate Bill No. 460, available at http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB460 (last visited Feb. 4, 2018).
[23] Jon Brodkin, California Senate defies FCC, approves net neutrality law, ARS TECHNICA, Jan. 30, 2018, available at https://arstechnica.com/tech-policy/2018/01/california-senate-approves-net-neutrality-law-in-defiance-of-fcc/ (last visited Feb. 4, 2018).

provides broadband Internet access service . . . and make a violation of those prohibitions subject to the remedies available pursuant to the act."[24] The bill further would not allow state agencies to contract with ISPs unless that provider of broadband Internet access service would attest subject to the penalty of perjury that it will "not engage in specified activities."[25]

Furthermore, over twenty states have united in the fight against the net neutrality repeal by filing a "protective petition for review" in the United States Court of Appeals for the District of Columbia Circuit;[26] the District of Columbia joined 21 states (collectively referred to as "State Petitioners") that include: Virginia, California, Mississippi, Connecticut, Minnesota, Delaware, New Mexico, Hawaii, Washington, New York, Vermont, Kentucky, Rhode Island, Maryland, Illinois, Pennsylvania, Oregon, Maine, North Carolina, Iowa, and Massachusetts.[27]

> State Petitioners seek a determination by this Court that the [Restoring Internet Freedom] Order is arbitrary, capricious, and an abuse of discretion within the meaning of the Administrative Procedure Act, 5 U.S.C. § 701 *et seq*.; violates federal law, including, but not limited to, the Constitution, the Communications act of 1934, as amended, and FCC regulations promulgated thereunder; conflicts with the notice-and-comment rulemaking requirements of 5 U.S.C. § 553; and is otherwise contrary to law.[28]

The State Petitioners, led by New York Attorney General Eric Schneiderman,[29] are asking for the Court "to hold as unlawful, vacate, enjoin, and set aside the Order, and that it provide such additional relief as may be appropriate."[30] Attorney General Shneiderman argues, repealing net neutrality regulations put in place in 2015 will have "dire" ramifications impacting business and consumers throughout the United States, including but not limited to New York – since these entities and people "rely on a free and open internet." Schneiderman further elaborates on the "dire" results by emphasizing things that he says would be allowed to happen with the repeal of net neutrality regulations including "allowing internet service providers to block certain content, charg[ing] consumers more to access certain sites, and throttle[ing] or slow[ing] the quality of content from content providers that don't pay more."[31]

---

[24] California Senate Bill No. 460, *supra*.
[25] *Id*.
[26] Petition for Review by 21 states and the District of Columbia available at https://ag.ny.gov/sites/default/files/petition_-_filed.pdf (last visited Feb. 4, 2018).
[27] *Id*.
[28] *Id*.
[29] New York State Office of the Attorney General, A.G. Schneiderman Files Suit To Stop Illegal Rollback Of Net Neutrality, available at https://ag.ny.gov/press-release/ag-schneiderman-files-suit-stop-illegal-rollback-net-neutrality (last visited Feb. 4, 2018).
[30] Petition for Review, *supra*.
[31] New York State Office of the Attorney General, *supra*.

On February 5, 2018, New Jersey Governor Philip Murphy signed Executive Order Number 9 into law.[32] This Executive Order specifically addresses the repeal of Net Neutrality policies by the FCC mandating,

> The Division of Purchase and Property, within the Department of the Treasury, and all other contracting units or officials of any State entity, shall require that all future contracts for Internet, data, and telecommunications ("Internet and broadband") be awarded only to ISPs that adhere to "net neutrality" principles.[33]

In a landmark move, the Washington State Legislature passed, with bipartisan support, legislation addressing the repeal of Net Neutrality policies on February 27, 2018.[34] Washington Governor Jay Inslee signed the legislation, HB 2282 - 2017-18 Protecting an open internet in Washington state, into law on March 5, 2018.[35] Washington is now "the first state in the nation to pass a law to protect net neutrality."[36] This new law protects, at a state level, net neutrality principles, which will ensure internet providers are not allowed to unfairly manipulate access to content or internet.[37]

**Has the Issue of Net Neutrality Been Preempted by the Federal Government?**

The above actions by the states after the FCC repealed net neutrality last December raises this question: has Congress successfully acquired federal preemption over the states in this area? According to Title 47 U.S. Code section 253 it arguably has,

> If, after notice and an opportunity for public comment, the Commission determines that a State or local government has permitted or imposed any statute, regulation, or legal requirement that violates subsection (a) or (b) of this section, the Commission shall preempt the enforcement of such statute, regulation, or legal requirement to the extent necessary to correct such violation or inconsistency.[38]

But only time will tell what the courts, who have the obligation to determine Congress's intent to preempt or not, will do. If the courts find Congress has not preempted this area and there are conflicting federal and state laws,

---

[32] New Jersey Executive Order Number 9 dated Fe. 5, 2018, available at http://nj.gov/infobank/eo/056murphy/pdf/EO-9.pdf (last visited Feb. 28, 2018).
[33] *Id.*
[34] Washington State Legislature, progress of HB 2282 - 2017-18 available at http://app.leg.wa.gov/billsummary?BillNumber=2282&Year=2017 (last visited Feb. 28, 2018).
[35] Office of Washington Governor Jay Inslee, Washington becomes first state to pass net neutrality protections into law, Mar. 5, 2018, available at https://www.governor.wa.gov/news-media/washington-becomes-first-state-pass-net-neutrality-protections-law (last visited Mar. 6, 2018).
[36] *Id*.
[37] *Id*.
[38] U.S. Government Publishing Office 47 U.S.C. 253 (d), available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapII-partII-sec253.pdf (last visited Feb. 5, 2018).

> Chief Justice Warren in 1956 provided the criteria used by the Court to decide such cases: 'Where . . . Congress has not stated specifically whether a federal statute has occupied a field in which States are otherwise free to legislate, different criteria have furnished touchstones for decision. . . . "*First*, [t]he scheme of federal regulation is so pervasive as to make reasonable the inference that Congress left no room for the States to supplement it. . . . "*Second*, the federal statutes 'touch a field in which the federal interest is so dominant that the federal system [must] be assumed to preclude enforcement of state laws on the same subject.' . . . "*Third*, enforcement of state sedition acts present a serious danger of conflict with the administration of the federal program.[39]

"Congress can delegate to a federal agency the power to preempt state requirements when Congress adopts enabling legislation in a particular field."[40] Congress delegated authority to the FCC through Title 47 of US Code;[41] this chapter applies to "all interstate and foreign communication by wire or radio . . . ."[42] It is noteworthy to mention that in section 157 it states, "Any person or party (other than the Commission) who opposes a new technology or service proposed to be permitted under this chapter shall have the burden to demonstrate that such proposal is inconsistent with the public interest."[43] Maybe The New Yorker's cartoon with a internet page spinning indefinitely waiting for the content to appear is not what Congress and the FCC had in mind;[44] however, the public comments to the FCC - making this issue one of the most active on the FCC website within the last thirty days - could be, but the FCC only shows the public comments for a thirty day time period on the internet.[45]

It is important for all of us to remember that the FCC was created

> [f]or the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex, a *rapid*, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at *reasonable charges*, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications, and for the

---

[39] Corwin at 273.
[40] American Bar Association, The Basics of Preemption, p.8, available at http://apps.americanbar.org/abastore/products/books/abstracts/5010047samplechp_abs.pdf (last visited Feb. 5, 2018).
[41] U.S. Government Publishing Office, 47 U.S.C. 151 - PURPOSES OF CHAPTER; FEDERAL COMMUNICATIONS COMMISSION CREATED, available at https://www.gpo.gov/fdsys/granule/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapI-sec151 (last visited Feb. 3, 2018).
[42] U.S. Government Publishing Office, Title 47 US Code section 152 (a) available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapI-sec152.pdf (last visited Feb. 4, 2018).
[43] Title 47 US Code section 157 (a) *supra*.
[44] The New Yorker, I Can't Believe They Repealed Net Neutrality, Dec. 15, 2017, available at https://www.newyorker.com/tag/net-neutrality.
[45] ECFS Most Active Proceedings available at https://www.fcc.gov/rulemaking/most-active-proceedings (last visited Feb. 3, 2018).

> purpose of securing a more effective execution of this policy by centralizing authority heretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication, there is created a commission to be known as the ‘‘Federal Communications Commission’’, which shall be constituted as hereinafter provided, and which shall execute and enforce the provisions of this chapter.[46]

***Sherri Marie Carr*** *is the S. M. Carr Law Firm, Ltd. Co. Founding Member, is based in South Carolina and focuses on cyberspace issues involving business law and the professional responsibility and ethical implications for lawyers and law firms regarding cyber security and other cyberspace issues. Attorney Carr is admitted to practice law in South Carolina, Georgia, Minnesota, Washington D.C., the Eastern and Western Districts for the United States District Courts of Michigan, the Northern and Middle Districts for the United States District Courts in Georgia, the Court of Appeals for Veterans Claims, and the Supreme Court of the United States.*

[46] U.S. Government Publishing Office, Title 47 US Code Section 151, available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapI-sec151.pdf (last visited Feb. 4, 2018) (emphasis added).

# The Cyber Cold War: How Stockpiling Malware Moves the World Closer to a Technological Armageddon

***By Justin Evans***

## Introduction: Blind Reliance

*The world is currently experiencing a digital revolution, where access to the internet and technology has increased significantly in all age groups. Technology has improved the quality of life for everyone,* for example, it has made the world borderless by allowing individuals to connect with each other throughout the world for personal and professional reasons. With the increased utility of the technology, has come a false sense of security. Individuals, governments, and corporations have all grown comfortable with the storage and use of technology without giving security a second thought. Lack of preparation has created a problem of security for personal and confidential information for individuals and corporations.

Corporations have become repositories of gold for hackers, who employ tools such as viruses, worms, and Trojans, and malware to gain access to this information. One of the most utilized techniques by hackers to gain access to corporations' information is malware. Ransomware is a type of malware that hackers employ to gain access to the corporations' information. In fact, the summer of 2017 saw the largest global ransomware cyber-attack, which lead to the hacking of over 300,000 computers in 150 countries. WannaCry is one of the more dangerous types of ransomware because of its ability to infect the victim's computer. Once in the victim's computer, it can automatically spread itself across the victim's network by exploiting vulnerabilities in the Microsoft software. The vulnerability was first discovered by the National Security Agency (NSA), which generated a stockpile of malware to exploit it. The NSA is not the only organization that is stockpiling malware, and this has a number leaders and citizens afraid of a potential cyber cold war.

## This is a Stick Up: Ransomware?

Ransomware is a type of malware that is used by cyber criminals to conduct cyberattacks on various computer systems.[1] Hackers use ransomware to take control of computer systems or mobile devices, blocking the owners from accessing their files until a ransom is paid.[2] Cyber criminals access victims' computer systems using tools of social engineering, convincing the victim to click on a malicious link or mistakenly download malicious software onto their device.[3] The software is often attached to an email

[1]Kim Zetter, *What is Ransomware? A Guide to the Global Cyberattack's Scary Method*. Wired (May 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise.
[2]Josh Fruhlinger, What is ransomware? How it works and how to remove it. CSO from IDG (Nov. 2017), https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html.
[3] Zetter Supra, note 1.

that masquerades as something innocent, like a coupon. Once the software is downloaded on the device, the virus can access the networking system.[4] Once the software has been given access to the victim's network, the hackers can lock all of the files on the computer and network. Files are encrypted one after another.[5]

**WannaCry: The Sleeper Agent?**

WannaCry is a specific type of computer malware, belonging to the family called Ransomware.[6] WannaCry allows the hackers to lock all of the data on a victim's computer and network system until a ransom is paid.[7] WannaCry is similar to other ransomware in that it infects and encrypts files when it gains access to the victims' computers.[8] However, WannaCry varies from other ransomware in that it also includes a worm that allows it to spread autonomously to other systems using the Ethernal Blue exploit.[9] The WannaCry virus does not require user interaction once it has gained access to the network, meaning it works autonomously.[10] This allows for the virus to corrupt computers that have locked away in storage rooms with only access to the network and a power source.[11] This unique feature allows for a hacker to hold an entire computer network system hostage from corporations and governments, which forces them to pay the ransom.[12]

Infected victims' are left with only two files: instructions on the next steps and the WannaCry software itself.[13] Once the software is opened, it tells the victim that their files have been encrypted, and instructs the victim that they have a few days to pay the ransom, and if the fee isn't paid the files will be deleted.[14] The hackers demand the ransom to be paid in the form of Bitcoin, instructing victims on how to purchase the Bitcoin and an address where to send the payment.[15] The hackers promise that upon verification of the payment, that the hackers would send a key to the victim allowing them to unlock their files.[16] Experts urge against paying the ransom because there are no guarantees, by paying

---

[4] *Id.*
[5] *Id.*
[6] Josh Fruhlinger, What is WannaCry ransomware, how does it infect, and who was responsible?, CSO from IDG (Sep. 2017), https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.
[7] *Id.*
[8] *Id.*
[9] *All about ransomware*, Malwarebytes (2017), https://www.malwarebytes.com/ransomware.
[10] Josh Fruhlinger, 2017, The 5 biggest ransomware attacks of the last 5 years. CSO from IDG (Aug. 2017), https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html.
[11] *Id.*
[12] Malwarebytes Supra, note 9.
[13] Josh Supra, note 10.
[14] Malwarebytes Supra, note 9.
[15] *Id.*
[16] *Id.*

the ransom that you will receive your files back intact.[17] Cyber criminals require payment in Bitcoin because the currency is decentralized, unregulated in most countries, and almost impossible to trace.[18]

**The Drafter of the WannaCry?**

The WannaCry software was created by the United States of America's NSA when it discovered a vulnerability within the Microsoft's software known as Eternal Blue.[19] The NSA has stockpiled several malware programs that exploit the Eternal Blue vulnerability.[20] After the completion of this malware, the exploit was leaked to the hacker group Shadow Brokers, who later released the software publicly at the beginning of the year.[21] It is believed that the WannaCry was stolen by an NSA insider but has not been verified.[22] Soon after the release of the software, Microsoft created a patch in an update to prevent the vulnerability.[23] Though Microsoft released the patch in an update, many consumers who did not update their systems or could not because they were operating legacy or pirated systems, were left vulnerable.[24] India and Russia were two of the countries most affected by the hack, because of their use of the Microsoft's Windows XP legacy or pirated operating systems, which are widely used throughout both countries.[25]

**The Mechanistic of the WannaCry Virus?**

The WannaCry virus targets the victim's pictures, documents, files, and data that are personally invaluable.[26] Hackers gain access to the victim's computer networks through the deployment of social engineering.[27] One of the most popular social engineering is the phishing emails.[28] Once the victim has opened the email attachment or clicked on the link, the virus quickly infiltrates the network and locks the files up.[29] The virus then targets the backed up files and folders, which prevents the user from being able to backup corrupted files; preventing replacement or restoration.[30] Once the attack has

---

[17] *Id.*
[18] Josh Supra, note 10.
[19] Alfred NG, *Hackers behind stolen NSA tool for WannaCry: More leaks coming*, CNET (May 2017), https://www.cnet.com/news/hackers-behind-stolen-nsa-tool-for-wannacry-more-leaks-coming.
[20] *Id.*
[21] Bruce Schneier, *Who Are the Shadow Brokers?,* The Atlantic (May 2017), https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778.
[22] Alfred Supra, note 19.
[23] Bruce Supra, note 21.
[24] Alfred Supra, note 19.
[25] Bruce Supra, note 21.
[26] Sam Jones, What is WannaCry and how can it be stopped?, Fin. Times (May 2017), https://www.ft.com/content/af74e3f4-373d-11e7-99bd-13beb0903fa3.
[27] *Id.*
[28] Andy Greenberg, The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes, Wired (May 2017), https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes.
[29] *Id.*
[30] *Id.*

begun, the victim can expect to see any of the following: ransomware note, encrypted files, renamed files, locked browser, and/or a locked screen.[31]

**The Attack: What Does the News say Happened**

The first appearance of the WannaCry was reported on April 29th by Golan Ben-Oni, the global chief information officer for IDT corporation.[32] Ben-Oni reported the attack to the White House, the Federal Bureau of Investigation, the New Jersey Attorney General's Office, and other top cybersecurity firms.[33] Two weeks later, on Friday, May 12, during the early morning hours, the second major company to report being affected by the malware attack was Telefonica, which is a Spain-based telecommunications company.[34] By mid-morning, employees of Telefonica found themselves locked out of their computers.[35] Once the WannaCry virus accessed the Telefonica's computer network, it not only restricted access for the employees but also affected its subsidiaries.[36] Within 3 hours there were already victims in 11 countries, including some European health institutions, which began to report that they were also experiencing symptoms from the attack.[37] Soon the virus had spread across computers and network systems in 70+ countries, utilizing technology that had been released by the Shadow Brokers.[38] Included in the list of entities affected by the attacks that Friday, were universities in China, rail systems in Germany, FedEx, oil companies, and several auto plants in Japan.[39]

A cybersecurity researcher, who worked for Proofpoint, discovered an unregistered domain that was buried in the code of the WannaCry virus and posted it online.[40] Hours later, a UK cyber security researcher, known online by the name MalwareTech, found the findings online and activated a kill switch for the attack, thereby slowing the spread of the attack.[41] MalwareTech was able to activate the kill switch after he noticed that during the first stage of the infection process that the virus was trying to access a web address.[42] MalwareTech noticed that the site was unregistered and decided to buy the website domain for 11 dollars.[43] The developers of the virus built in a kill switch, which was

---

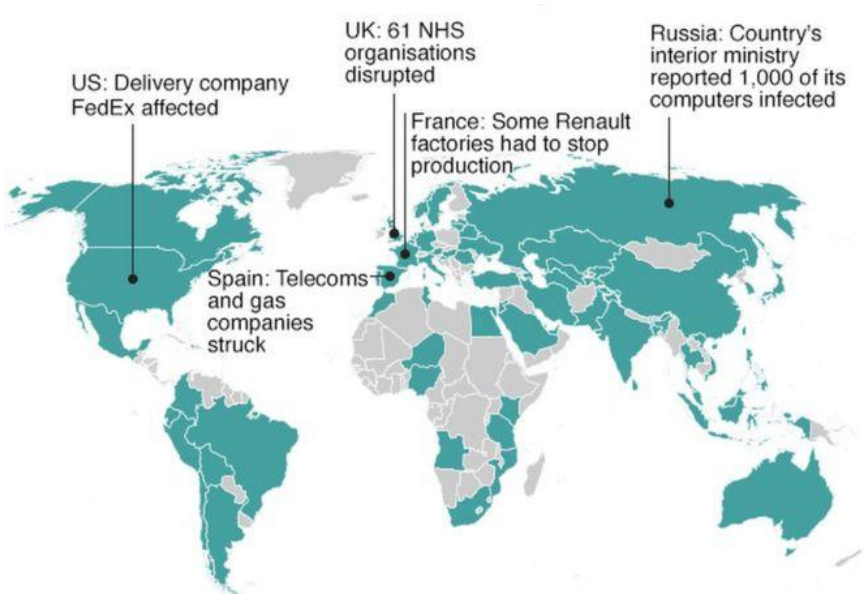
[31] Sam Supra, note at 26.
[32] Nicole Perlroth, A Cyberattack 'the World Isn't Ready For, The NY. Times (Jun. 2017), https://www.nbc.com/dateline/video/a-cold-december-morning/3641846.
[33] *Id.*
[34] Sam Jones, Timeline: How the WannaCry cyber attack spread, Fin. Times (May 2017), https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23.
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] James Hayes, Wannacry and ransomware impact on patient care could "cause fatalities", E and T (May 2017), https://eandt.theiet.org/content/articles/2017/05/wannacry-and-ransomware-impact-on-patient-care-could-cause-fatalities.
[39] *Id.*
[40] Sam Supra, note at 34.
[41] Michael Hayden, A timeline of the WannaCry cyberattack, ABC News (May 2017), http://abcnews.go.com/US/timeline-wannacry-cyberattack/story?id=47416785.
[42] Sam Supra, note at 34.
[43] *Id.*

activated when the domain was activated. Activation of the domain signaled to the virus to halt its infection of the system.[44]

**Lighting the Fuse: How the Global Attack Started**

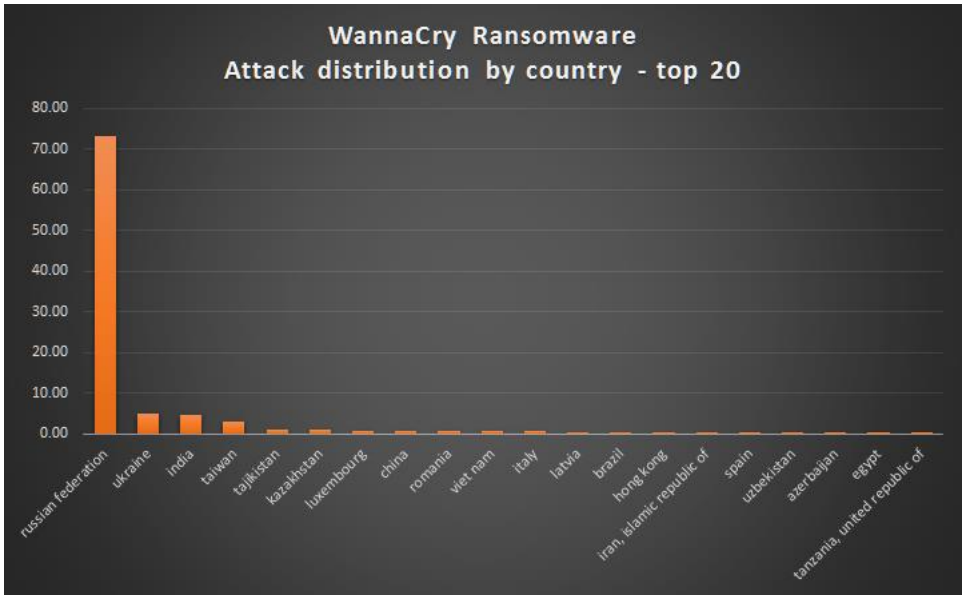
Top lawyers for Microsoft have blamed the largest global hack on the NSA, due to its habit of creating and stockpiling malware.[45] It is believed that an insider accessed the malware and released it to the Shadow Brokers.[46] The attack was felt global, leading many leaders to call for a new "Digital Geneva Convention," to force governmental entities to take greater responsibility for the malware that it has been creating, stockpiling, and selling. Hackers were able to use the WannaCry virus to take advantage of the Microsoft exploit Eternal Blue.[47] Upon discovery of the exploit, Microsoft created a patch for the vulnerability. However, users who were using Windows 7 and Windows Server 2008 (or earlier OS) system, were left unpatched and therefore vulnerable.[48] Microsoft users who were using Windows 10, were not susceptible to the attack. Once one computer on the network is infected, the ransomware moves laterally to spread to additional computers.[49] To raise the sense of urgency, the hackers included a specific countdown till when the payment cost will be raised, as well as a threat of the complete loss of the data.[50]

**Touched by an Angel: Countries Affected by the Global Malware Attack**




[44] *Id.*
[45] Andy Patrizio, Microsoft to NSA: WannaCry is your fault, Net. World (May 2017), https://www.networkworld.com/article/3196222/security/microsoft-to-nsa-wannacry-is-your-fault.html.
[46] *Id.*
[47] *Id.*
[48] Sam Supra, note at 34.
[49] *Id.*
[50] Andy Supra, note 45.

While ransomware has always been global, this particular attack has affected over 300,000 victims worldwide, in over 150 countries according to the Kaspersky Lab, a Moscow-based Internet security firm.[51] Among those initially affected by the attack was the Telecommunication and gas companies in Spain; sixty-one (61) British hospitals in the National Health Services network; over 1,000 computers in the Russian interior ministry; Brazilian government agencies; the German transit system; Chinese Universities; and the Renault factories in France.[52] Analysts believe that the British hospitals were susceptible to the attacks because hospitals are generally behind other industries when it comes to upgrading and updating its security and software systems.[53] Hospitals are also at a disadvantage because of the limited number of resources that it assigns to its information technology.[54] The financial sector allots around 25% to 35% of its operating budget to information technology, whereas hospitals only allot 2% to 4%.[55] Kaspersky Lab reported that Russia was the most affected country, because of outdated and pirated software that is used by government agencies.[56]




**The Casino Heist: Nation States that Sponsored the Global Malware Attack**

It is believed that the WannaCry virus was created by the NSA and stolen by an insider. The insider subsequently released the virus to hackers known as the Shadow Brokers in April of 2017.[57] The Kaspersky Lab and the NSA have uncovered new evidence linking the WannaCry ransomware code to

[51] Michael Supra, note 41.
[52] Sam Supra, note at 34.
[53] *Id.*
[54] *Id.*
[55] James Supra, note 38.
[56] *Id.*
[57] *Id.*

North Korea's spy agency, the Reconnaissance General Bureau.[58] The WannaCry virus ultimately affected more than 300,000 victims worldwide, in over 150 countries, according to U.S. intelligence officials. The NSA has attributed the attack to cyber actors who have are suspected to be "sponsored by" the Reconnaissance General Bureau.[59]

Analysts believe that that the attacks were released by the state sponsored cyber actors to help generate another avenue for potential revenue for the country.[60] Analysts have reported that the cyber actors were able to generate over 140,000 in bitcoins but were unable to claim the funds due to an operational error, which made the transactions traceable.[61] Analysts believe that North Korea was responsible for the attacks because the attacks traced back to several computer internet protocols addresses in china, which has been used by the RGB in the past.[62] This has since been confirmed by other agencies. Agencies believe that the cyber actors are members of the Lazarus Group.[63]

Other agencies have also been able to link North Korea to a series of other cyber-enabled bank heists throughout Asia, which generated over 81 million dollars in that single heist.[64] North Korea also hacked Sony Pictures, when it was planning to release a movie that mocked its current leader.[65] These examples demonstrate that even though North Korea was thought to have a limited computer infrastructure, it can launch cyber attacks.[66] Though North Korea may have a limited infrastructure, it was able to carry out such a large cyberattack by employing sophisticated cyberweapons developed by the NSA.[67] The deployment of the virus itself is not as complex because once the victim clicks on the link or downloads malicious content, the attack becomes automated. [68]

**The Culprits: The Hackers Who Organized the Global Heist**

This attack was unique in that it involved various types of hackers for the attack to become the biggest attack to date.[69] The first hacker that contributed to the world's largest hack was the individual who was able to access the malware stockpile at the NSA.[70] A person who works for an entity and uses their

---

[58] Ellen Nakashima, The NSA has linked the WannaCry computer worm to North Korea, The Was. Post (Jun 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.c43dcbefb814.
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] Symantec Security Response, WannaCry: Ransomware attacks show strong links to Lazarus group, Symantec Connect (May 2017), https://www.nbc.com/dateline/video/the-carrollton-plot/3638493.
[64] Ellen Supra, note at 58.
[65] SSR Supra, note at 63.
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Andy Greenberg, Hold North Korea Accountable for Wannacry- and NSA, too, Wired (Dec. 2017), https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue.
[70] *Id.*

position to obtain and exploit secret information or launch an attack is an internal perpetrator.[71] The insider was responsible for the leaking of the virus from multiple divisions throughout the NSA and provided these items to the hacktivist group Shadow Brokers.[72] I believe that Shadow Brokers would be labeled as a hacktivist because its motivation was not for a financial gain but rather a political purpose.[73] Shadow Brokers are not cyber criminals because the group housed the stolen data for over three years and did not use it to its advantage.[74] Analysts believe that Shadow Brokers work for a nation state such as China or Russia. It would make sense if the group were members of Russia when considering the recent hacks of the DNC and the 2017 elections. Shadow Brokers seemed to be in the game for collecting state secrets from the US and releasing them to either embarrass the US or facilitate cyberattacks on the US. This could lead us to the second cold war (Cyber Cold War), either between the US/China and US/Russia.

Finally, the group of hackers that used the information released by Shadow Brokers to target various corporations, governments, and citizens in rivalry countries, which they are seeking revenge on which would classify them as blue hat script kiddies.[75] The group of hackers that released the WannaCry were likely the Lazarus Group, which were likely sponsored by North Korea as defined above.[76] The Lazarus Group would be classified as script kiddies because they are simply copying the code provided by the Shadow Brokers and using it to attack corporations, in the effort to fund their country.[77] Because the Lazarus Group established a required ransom but never cashed in on the funds, it leads me to believe that they are not only script kiddies but also blue hats.[78] Blue hat hackers are script kiddies that are seeking revenge on those that have angered the US. I believe that these state sponsored hackers were instructed to take US secrets and use them to embarrass them.[79] I believe this to be the case because now corporations like Microsoft have pointed their finger at the NSA demanding answers for its practices. The actions of The Lazarus Group have now placed US's largest security organization on the hot seat for stockpiling weapons, rather than focusing on the Lazarus Group or the Shadow Brokers.[80]

The Lazarus Group could also be hacktivist who are pointing out how stockpiling malware can be as bad as stockpiling nuclear weapons.[81] How? The ransomware attacked several hospitals in England, which required a number of them to turn away patients.[82] The attack could have been deadly, affecting not only patients seeking help but also the lives of those that rely on machines, which are connected to

---

[71] Grey Hat 4 Life, 7 Types of Hackers You Should Know, Cybrary (Sep. 2015), https://www.cybrary.it/0p3n/types-of-hackers.
[72] Andy Supra, note at 69.
[73] Grey Supra, note at 71.
[74] *Id.*
[75] Grey Supra, note at 71.
[76] SSR Supra, note at 63.
[77] *Id.*
[78] *Id.*
[79] Grey Supra, note 71.
[80] SSR Supra, note at 63.
[81] *Id.*
[82] James Supra, note 38.

the internet, for life.[83] If patients had died because of the WannaCry attacks, citizens would have held the US responsible and demanded an explanation for the casualties.

**Conclusion: Can We Halt the Cyber Cold War?**

The world is rapidly progressing into the digital age, but with the progression comes vulnerabilities that hackers are exploiting. In 2017 alone, the US has seen the hacking of law firms like DLA Piper, Credit Bureaus such as Equifax, and tech transportation like Uber. As hacks become weekly news, citizens throughout the world have become victims to tools that their countries have generated and stockpiled. If countries do not start to take ownership of their role in the cyber war, there is a chance that their citizens will continue to pay the price. What if hackers use these tools and shut down power grids, hospital computers and tools, and defense systems?

***Justin Evans*** *is an Innovation Assistant, Patent Division LSAG Liaison in the ABA Section of Intellectual Property Law 2017, E-Privacy Law Vice-Chair in the ABA Section of Science & Technology Law 2017, Sidney B. Williams, Jr. Scholar and Blockchain and Smart Contracts Scholar. Justin has degrees in chemistry and biology and works both as a patent strategy intern and as a judicial legal intern.*

[83] *Id.*

## How Belgium is preparing for life under the GDPR

***By Maarten Stassen***

*May 25 is marked in red in the agendas of privacy professionals around the globe. The day on which the General Data Protection Regulation (GDPR) becomes applicable will also be the birthdate of the new Belgian data protection regulator.*

**What's in a name?**

*Belgium already has a data protection regulator, but its structure,* roles and responsibilities are not fit for GDPR purposes. But a new law that was enacted on December 3, 2017 (Act) created a new regulator that provides broader authority.

The first change that catches the eye is the name of the regulator: "Data Protection Authority" (Authority) instead of the current "Commission for the Protection of Privacy" (Commission). While it might just be a matter of semantics, the change in wording does align with the significant change in powers. The most debated one is the new power to impose administrative fines. And these fines can be huge: up to 4% of an organization's total worldwide annual revenue or € 20 million, whichever is higher.

The case against Facebook shows that the Commission has not awaited the name change or new powers to show its teeth. In June 2015, it started a judicial fight with Facebook before the Brussels courts over the social media group's cookies practices. On February 16, 2018, the court ruled in favor of the Commission and required Facebook to amend its online tracking practices and to delete the data collected via these files.

**A new structure, adapted to the GDPR**

The Belgian Data Protection Authority will consist of 6 bodies:

1. Executive Committee
2. General Secretariat
3. First Line Service
4. Knowledge Center
5. Inspection Service
6. Dispute Chamber

An independent advisory board will assist the Executive Committee and the Knowledge Center with non-binding advice.

**Executive Committee**

The Executive Committee, which chaired by the president and composed of the heads of the other five abovementioned bodies, will be in charge of determining and evaluating budget, reporting, strategy and management plans, including the Authority's yearly priorities.

It is not known yet when the Authority's will issue its first strategic plan, but when it does it will be made available for public consultation during at least two weeks, will shed light on the approach of this new body.

**General Secretariat**

The General Secretariat will be an important sparring partner for controllers as it will provide advice in cases where, for example, a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken to mitigate the risk and that, thus, prior consultation with the Authority is required. Furthermore, it will, for example, approve binding corporate rules and codes of conduct.

**First Line Service**

An important task of the First Line Service is enhancing awareness around the protection of personal data. Furthermore, is plays an important role in the context of complaints and requests, as it assessed their admissibility.

Admissible complaints are sent to the Dispute Chamber. Requests, on the other hand, are firstly handled by the First Line Service. Only if no amicable settlement is reached, the request takes the form of a complaint and then follows the same route.

**Knowledge Center**

In line with the Commission's current practices, the Knowledge Center will provide advice regarding any matter related to the processing of personal data, as well as recommendations related to social, economic and technological developments that could affect the processing of personal data. It will provide these advices and recommendations, whether spontaneously or if requested by federal or regional authorities.

**Inspectorate**

The biggest game changer seems to the new Inspectorate, the body that will conduct investigations on the application of the GDPR. In line with the GDPR's accountability requirement, controllers must demonstrate compliance in case of an inspection. Duly documenting compliance efforts are therefore one of the main focus points of controllers in these months leading up to May 25.

The Inspectorate, which has broad investigative powers, can autonomously initiate investigations, or can be requested to do so by the Executive Committee or the Dispute Chamber. As part of its investigation, the Inspectorate can go on-site, look into IT systems, take copies of data stored on them, and seize or seal them. If required for the avoidance of a serious, immediate harm that would be difficult to repair, provisional measures can be taken, such as the suspension, restriction or ban on the corresponding processing operations. The operational impact of such measures can obviously not be underestimated.

**Dispute Chamber**

The body that will handle the administrative procedure is called the Dispute Chamber. While it is a written procedure, the Dispute Chamber can invite parties for a hearing. Such procedure can be initiated by the First Line Service, as explained above, by a party appealing measure taken by the Inspectorate, or by the Inspectorate itself once it has finalized its investigation.

**The Advisory Board**

The Advisory Board will provide non-binding advice related to any matter related to the protection of personal data, whether spontaneously or if requested by the Executive Committee or the Knowledge Center. The advice to the Executive Committee can also be related to the strategic plan and KPIs as well as on evolutions in technological, commercial and other domains which could affect the protection of personal data.

**Removing language barriers**

It is interesting to see that at least one member of the Executive Committee should talk German, and that all its members should not only speak both Dutch and French, but also English. This requirement makes much sense, given the international context in which the Authority will operate.

The Act does further states that the language of the procedures will be chosen "depending on the needs of the case".

Nothing but good news for international companies, as it is another door that remains open to a procedure in their business language.

**Adapting the Belgian legal framework**

While the GDPR will directly apply, member states can maintain or introduce national provisions to further specify the application of the GDPR. Important decisions can be taken on, for example, the use of the national identification number, the processing personal data in the context of employment, the processing of sensitive data, the minimum age for children's online consent, etc.

Regarding the last, Belgian State Secretary for Privacy Philippe De Backer recently announced that he suggest to lower the age for offering information society services directly to a child from 16, as currently foreseen in the GDPR, to 13 years.

Needless to say, these legislative changes should be closely monitored by controllers and processor who will be subject to Belgian law.

***Maarten Stassen*** *is a senior counsel in the Brussels office of Crowell & Moring, where he is a member of the firm's Privacy & Cybersecurity Group. His practice focuses on privacy and data protection, including the General Data Protection Regulation (GDPR) and cross-border data transfers solutions, as well as on the legal and operational aspects of the digital ecosystem, including Internet of Things (IoT), MedTech, and upcoming technologies such as Distributed Ledger Technology (e.g. Blockchain).*

*Before joining Crowell & Moring, Maarten was a director in Deloitte's Cyber practice, as well as the Faculty Leader of the European Privacy Academy. He has been focusing on privacy and data protection law for many years, first as a lawyer in both Spain and Belgium, and later as European Privacy Officer of an international health insurance company.*