Chicago Journal of International Law

Volume 20 | Number 1 Article 7

1-1-2019

Enforcement Through the Network: The Network Enforcement Act and Article 10 of the European Convention on Human Rights

Imara McMillan

Enforcement Through the Network: The Network Enforcement Act and Article 10 of the European Convention on Human Rights

Cover Page Footnote

I would like to thank Professor Lakier and the entire Chicago Journal of International Law staff for helping me develop this Comment from a casual question of “is this legal” to a thesis about the way social media companies should be regulated across borders. A particular shout-out goes to the team at Cloudflare, who introduced me to the idea that international law touches more than just trade and migration. This is a piece I am really proud of, and I hope everyone who helped me work on it understands exactly how important their role was.

Enforcement Through the Network: The Network Enforcement Act and Article 10 of the European Convention on Human Rights

Imara McMillan*

Abstract

This Comment explores the conflict between state-described freedom of expression and the autonomy of social media companies to regulate content on their platforms through the lens of the Network Enforcement Act, passed by Germany in 2017, and the freedom of expression clause of the European Convention on Human Rights. The Network Enforcement Act, which compels social media companies to monitor and remove content from their sites which violate certain other provisions of German law, has thrust the issues of intermediary autonomy and censorship-by-proxy into the spotlight. Proponents of the law support it as a way to ensure that what is illegal offline remains illegal online. Opponents argue that the law essentially amounts to censorship, and therefore violates freedom of expression under the German constitution and a host of international treaties. This Comment finds that while the law likely does not violate freedom of expression as enumerated under Article 5 of the Basic Laws of the Republic of Germany, it may violate freedom of expression under Article 10 of the European Convention of Human Rights, in part because the law incentivizes "overblocking" which could lead to the removal of lawful speech without due process. In order to promulgate such regulations, more than one country needs to band together in order to promote safety and international security without curtailing civil rights.

* I would like to thank Professor Lakier and the entire Chicago Journal of International Law staff for helping me develop this Comment from a casual question of "is this legal" to a thesis about the way social media companies should be regulated across borders. A particular shout-out goes to the team at Cloudflare, who introduced me to the idea that international law touches more than just trade and migration. This is a piece I am really proud of, and I hope everyone who helped me work on it understands exactly how important their role was.

Table of Contents

I. INTRODUCTION

In January 2018, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken[1] (hereinafter the Network Enforcement Act) came into effect.[2] Passed in late 2017 by the Bundestag, the German federal parliament, the Network Enforcement Act was designed to combat hate speech, radicalization, and fake news online.[3] The crux of the law provides that when a social media company receives a complaint about a piece of controversial content, if that company has more than two million German users[4] it must spring into action to determine whether the content is "manifestly unlawful" according to eighteen separate provisions of German criminal law.[5] If the company determines that the content is unlawful, access to it must be removed within twenty-four hours.[6] For borderline cases, companies have seven days to remove the content.[7] The consequences for noncompliance are fines of up to five million euros (5.8 million dollars in December 2018).[8] There are currently no consequences for over-policing speech and no mechanism to contest violations.

Since the law went into effect in January 2018, it has faced a bevy of complaints. This Comment focuses on one—whether the law violates the freedom of expression clause, Article 10, of the European Convention on Human Rights (ECHR).[9] Although Heiko Maas, Germany's current Minister of Foreign Affairs who helped introduce the bill, argued that the kind of content which the bill seeks to have removed "damages . . . our culture of debate, and ultimately freedom of expression,"[10] many, including Facebook, claim that the law does the

---

1 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Network Enforcement Act], Sept. 1, 2017, Bundesgesetzblatt, Teil I [BGBL I] at 3352 (Ger.).

Official English translation may be found here: http://perma.cc/72JK-3KNM.

The law is also referred to by its abbreviated German names, NetzDG or Netzkdurchsetzungsgesetz.

2 Philip Oltermann & Thomas Furmann, *Tough New German Law puts Tech Firms and Free Speech in Spotlight*, THE GUARDIAN (Jan. 5, 2018), http://perma.cc/ENU5-4FKZ.

3 Stefan Engels, *Network Enforcement Act in a Nutshell*, DLA PIPER BLOG: IPT GERMANY (Jan. 31, 2018), http://perma.cc/E6QT-VSEL.

4 Netzwerkdurchsetzungsgesetz, *supra* note 1, at §1(2).

5 *Id.* at § 1(3).

6 *Id.* at § 3(2)(2).

7 *Id.* at § 3(2)(3).

8 *Id.* at § 4(2).

9 European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature Nov. 4, 1950, Eur. T.S. No. 5, 213 U.N.T.S. 221, at art. 10.

10 DEUTSCHER BUNDESTAG: PLENARPROTOKOLL 18/235 at 23848, (statement of Heiko Maas, Bundesminister BMJV), http://perma.cc/WKU4-HSGJ (Ger.).

opposite and violates freedom of expression under not only the German constitution but a host of international treaties.[11]

Because of the punitive nature of the fines, social media companies are incentivized to err on the side of caution and remove any content that is reported. This includes unlawful content, but also clearly satirical tweets parodying actual illegal content[12] and heated, but ultimately harmless,[13] comments.[14]

Facebook has allegedly recruited "several hundred staff" to deal with complaints.[15] For some, such as Bernhard Rohleder, CEO of Bitkom, a digital industry association which represents more than 2,600 German tech companies,[16] it appears as though Germany is privatizing the administration of justice and outsourcing it to large U.S. companies.[17] On the other hand, the rise of "fake news" and the use of social media by foreign actors to influence people's thoughts and ideas are increasingly large national security and safety concerns.[18]

To say that the law is controversial is an understatement. However, whether the European Court of Human Rights (ECtHR) would find that it in fact violates freedom of expression is another story. While the law, and the way the lower courts are currently enforcing it, may harm individual freedom of expression, the legitimate national security and safety concerns could allow for the law to be upheld without further adjustments. This would alter the way these claims get handled. That is, rather than the government or another complaining individual having to bring their case to the courts to remove speech, the affected individuals

---

11 Linda Kinstler, *Can Germany Fix Facebook?*, THE ATLANTIC (Nov. 2, 2017), http://perma.cc/B7EF-UDS8.

12 Emma Thomasson, *Germany Looks to Revise Social Media Law as Europe Watches*, REUTERS (Mar. 8, 2018), http://perma.cc/ZM6T-76XU (explaining that Titanic, a satirical magazine, had its content removed for parodying the language of a tweet from a far-right German political party which was also removed).

13 "Harmless" varies from person to person. There are a number of online posts, some of which will be discussed in this Comment, which cause real emotional harm to users. However, harmless is used here to mean not tending to call for or incite immediate violence or threatening physical harm against a given user.

14 Christof Kerkmann, *German Court Overturns Facebook 'Censorship,'* HANDELSBLATT TODAY (Apr. 13, 2018), http://perma.cc/S4LZ-DRCE (including examples of comments, such as "the Germans are becoming more and more stupid. No wonder, as they are being clobbered daily by left-wing media with fake news about skilled workers, declining unemployment or Trump.").

15 *Germany Starts Enforcing Hate Speech Law*, BBC NEWS (Jan. 1, 2018), http://perma.cc/23QB-MXB7.

16 Bitkom is the German Association for IT, Telecommunications, and New Media. For more information see http://perma.cc/T56F-EGUT.

17 Guy Chazan, *Berlin Forced to Defend Hate Speech Law*, FIN. TIMES (Jan. 5, 2018), http://perma.cc/8GAN-72TF.

18 *See generally* Jarred Prier, *Commanding the Trend: Social Media as Information Warfare*, 11 STRATEGIC STUD. Q. 50 (2017).

will have to bring their cases to court to get their accounts and posts reinstated. This could create a severe enough chilling effect on speech to warrant the ECtHR overturning at least part of the law. However, as this Comment explains, it is debatable that the Network Enforcement Act is uniquely to blame for this issue, and it is unclear whether removing the law will solve these free expression claims.

Section II addresses the history of the Network Enforcement Act. Although current discourse relating to controlling online speech has been centered on fake news in the wake of the U.S. 2016 election, the passage of the Network Enforcement Act is the culmination of a decade of growing tension in Europe between lawmakers and social media companies as both attempt to combat terrorism. It also explains how the "Brussels Effect"[19] could now be applied to Germany's new law, and therefore why the ECtHR would be the proper body to adjudicate this issue.

Section III briefly examines the history of the ECHR's Article 10 and the role of freedom of expression in Europe. The ECHR's ratification in the shadow of World War II means that its goals are centered in a historical moment that is very different from one that the mostly U.S.-based social media companies are accustomed to. This means that, although the Network Enforcement Act's goals instinctually seem to violate the traditional definition of freedom of expression that many of the affected social media companies operate under, it is not necessarily antithetical to the historical goals of the treaty.

In Section IV, this Comment determines whether the Network Enforcement Act indeed violates freedom of expression under Article 10. Because the state has a positive obligation to not interfere with freedom of expression, and penalties are generally considered interferences, Article 10 is implicated. Despite the fact that the goals which the legislature is attempting to promote through its interference are rational, and the fact that the law is potentially necessary, the lack of oversight and disproportionate fines mean that the ECtHR should find that the law violates Article 10. However, this Comment concludes that some sort of regulation over social media companies is necessary on an international scale in order to maintain a unified digital environment. Finding the correct balance between maintaining freedom of expression and promoting other rights, such as the right to privacy or national security, is increasingly crucial and difficult as expression moves away from public, government-sponsored forums to private locations.

II. HISTORICAL BACKGROUND

In order to understand the Network Enforcement Act's interaction with free expression rights, it is necessary to examine the law itself, as well as the forces that

---

[19] The Brussels Effect is the term coined to describe the E.U.'s growing ability to control and affect international regulations without entering into formal international agreements. For more information see Section II(C).

led to its passage. As Section II(A) discusses, the Network Enforcement Act must be understood in the context of the recent intensification of xenophobia in Europe, as well as the advent of terrorist attacks—coordinated online—in major European cities. Yet, lawmakers' attempts to curtail this unlawful speech are arguably harming the free expression rights of their citizens when it goes beyond standard national security justifications. In Section II(B), this Comment examines what the Network Enforcement Act actually does. The law acknowledges that by the time a given piece of media makes its way through the court system, it may be too late. The effects of harmful speech or images can multiply in seconds because of the internet. By moving the adjudication process from the courts to social media companies and speeding up the timeline, lawmakers are responding to real problems with monitoring online content, but in a way that arguably causes more harm.

Indeed, as Section II(C) discusses, because of the way the Network Enforcement Act is being interpreted, the German Bundestag is arguably expanding domestic laws far outside Germany's borders. Because the internet has no boundaries when German courts ask for content to be "removed" they can, and have, asked companies to remove it anywhere a German citizen might view it. With current technology, this means that German law is superseding international law and infringing on other countries' citizens' rights. Thus, although this is a German law, the ECtHR should adjudicate it.

A. What Forces Led to the Network Enforcement Act's Passage?

In order to analyze the freedom of expression concerns, it is important to understand the context of the Network Enforcement Act. Discussed in more detail in Section IV, one defense to a violation of freedom of expression is a compelling state interest. Here, Germany has frequently asserted an interest in national security, namely blocking terrorist and extremist content on the internet.

While the Network Enforcement Act feels like a law rooted in fears about populism and foreign election tampering, in many ways the worries that led to the act's passage came to a head in the wake of the 2015 Charlie Hebdo attacks in Paris. On January 7, 2015, twelve people, including four cartoonists, were murdered because of the magazine's publication of a satirical "Prophet Mohammed" cartoon.[20] The attack, which demonstrated terrorism's global reach

[20] Agnes Callamard, *Religion, Terrorism, and Speech in a 'Post-Charlie Hebdo' World*, 10 RELIG. & HUM. RTS. 207 (2015).

in the middle of one of the most prominent cultural centers of Europe[21], became a two-fold attack on freedom of expression. First, journalists were murdered due to their reporting. Second, the attack ignited a push towards more stringent policies for removing content on social media sites, such as Facebook and YouTube.

March 2016 brought another terrorist attack, this time in Brussels, a city known to be the center of privacy regulation in Europe.[22] In response, European leaders made a fervent call for a code of conduct against online hate speech.[23] In mid-2016, Facebook, Microsoft, Twitter, and YouTube voluntarily signed the "Code of Conduct on Countering Illegal Hate Speech Online" propagated by the European Commission.[24] Under this code, these tech companies were tasked with reviewing valid notifications for removal of illegal hate speech in under twenty-four hours, "remov[ing] or disabl[ing] access to such content, if necessary."[25] One major difference between the Network Enforcement Act and this early prototype is that the removal was based primarily on the companies' Terms of Service, rather than substantive criminal law.[26] This is in line with the E.U.'s vision of a "digital single market," which extends the idea of a unified Europe to cyberspace.[27] Despite the compliance with the law, one official lamented the fact that Facebook *only* reviewed forty percent of reported cases within twenty-four hours.[28] E.U. Justice Commissioner Vera Jourova, warned that tech companies "will have to act quickly and make a strong effort in the coming months" if they wanted to show that a non-legislative approach was viable.[29]

---

21 *Id.* at 208. While this Comment attributes the Charlie Hebdo attacks to ISIS, they were actually claimed by Al-Qaeda in the Arabian Peninsula. *See* Catherine E. Schoichet & Josh Levs, *Al Qaeda Branch Claims Charlie Hebdo Attack was Years in the Making*, CNN (Jan. 21, 2015), http://perma.cc/F5BL-4PRK.

22 Brussels is home to the Brussels Privacy Hub, "an academic privacy research centre with a global focus . . . Brussels is where key decisions are taken on data protection in the European Union, and EU rules set the standard for data protection and privacy law around the world." *About the Brussels Privacy Hub,* BRUSSELS PRIVACY HUB, http://perma.cc/W9P6-AX89.

23 Council of the E.U. Press Release 158/16, Joint Statement of E.U. Ministers for Justice and Home Affairs and Representatives of E.U. Institutions on the Terrorist Attacks in Brussels on 22 March 2016 (Mar. 24, 2016), http://perma.cc/L8XJ-V59D.

24 Liat Clark, *Facebook and Twitter Must Tackle Hate Speech or Face New Laws*, WIRED (Dec. 5, 2016), http://perma.cc/YCN7-4AP6.

25 *Id. See also* European Commission Factsheet, Code of Conduct on Countering Illegal Hate Speech Online: First Results on Implementation (Dec. 2016).

26 Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035, 1038 (2018).

27 *See* EUR. COMM'N, *Priority: Digital Single Market*, http://perma.cc/74TV-9684.

28 Clark, *supra* note 24.

29 *Id.*

By passing the Network Enforcement Act, Germany showed that it felt Facebook and other social media companies' responses since Charlie Hebdo have been inadequate. They are not alone.[30] Since the Network Enforcement Act's passage, Russia (another ECHR signatory), Singapore, and the Philippines have all cited it as a "positive example."[31] The U.K. and France have both recently begun to crack down on speech online. The U.K. recently passed the Digital Economy Act, which requires pornographic websites to develop the technology to actively block users under the age of eighteen, something privacy and free speech experts worry could lead to further censorship.[32] French president Emmanuel Macron is pushing for a measure which would grant judges emergency powers to remove or block content determined to be "fake" during "sensitive election periods."[33] The E.U. has also recently moved closer to intermediary responsibility. It floated an agreement to force social media companies to remove unlawful terroristic content within an *hour* or face fines.[34]

B. What is *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*?

1. The Network Enforcement Act is a law designed to combat extremism and hate speech online.

The Network Enforcement Act is a deceptively simple law. It applies to "telemedia service providers" or "social networks," defined as entities with over two million registered users in Germany "which, for profit-making purposes, operate internet platforms which are designed to enable users to share any content with other users or to make such content available to the public."[35] There are exceptions for platforms which offer "journalistic or editorial content" and messaging services.[36] In short, professional networks, specialist portals, games with online messaging systems, sales platforms, and email are intended to be

---

30 *See generally* Giancarlo F. Frosio, *Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility*, 26 INT'L J. L. & INFO. TECH. 1 (2017).

31 *Germany: Flawed Social Media Law*, HUMAN RIGHTS WATCH (Feb. 14, 2018), http://perma.cc/B87K-YGLJ.

32 Billy Perrigo, *The U.K. Is About to Regulate Online Porn, and Free Speech Advocates Are Terrified*, TIME MAGAZINE (Aug. 20, 2018), http://perma.cc/JH4U-LMXY.

33 James McAuley, *France Weighs a Law to Rein in 'Fake News,' Raising Fears for Freedom of Speech*, WASHINGTON POST (Jan. 10, 2018), http://perma.cc/HW79-N7LE. It is important to note that while distasteful, printing fake news is usually not considered illegal in modern times.

34 Saqib Shah, *E.U. Will Fine Social Media Sites for Lingering Extremism*, ENGADGET (Sept. 12, 2018), http://perma.cc/NR2E-RVYJ.

35 Netzwekdurchsetzungsgesetz, *supra* note 1, at § 1.

36 *Id.*

excluded.[37] This leaves the big social media companies, such as Facebook, Instagram, YouTube, and Google+, in the law's reach.

The law then outlines these companies' reporting obligations. Companies which receive more than a hundred complaints per calendar year about unlawful content are mandated to produce biannual reports on how they handled said unlawful content.[38] As of July 2018, this number included Twitter (approximately 270,000 complaints);[39] YouTube (58,297 complaints);[40] Google+ (2,769 complaints);[41] Change.org (1,257 complaints);[42] and Facebook (886 complaints).[43] These reports, which can be found on the individual company websites as well as the German Federal Gazette, contain a nine-point list of requirements with which companies must comply, ranging from "general observations outlining the efforts undertaken by the provider . . . to eliminate criminally punishable activity on the platform,"[44] to a detailed breakdown of how many complaints they received, from where those complaints were obtained, and how quickly they were removed.[45]

Finally, and most controversially, the law dictates how social media companies should handle certain kinds of complaints about unlawful content. The law requires social media companies to address complaints related to eighteen provisions of the criminal code,[46] enumerated below:[47]

1. Dissemination of propaganda material of unconstitutional organizations (§ 86)
2. Using symbols of unconstitutional organizations (§ 86(a))
3. Preparation of a serious violent offense endangering the state (§ 89(a))

---

37 Engels & Fuhrmann, *supra* note 3.

38 Netzwekdurchsetzungsgesetz, *supra* note 1, at § 2(1).

39 *Twitter Netzwerkdurchsetzungsgesetzbericht: Januar–Juni 2018*, TWITTER (2018), http://perma.cc/JU7L-ND3U (Ger.).

40 *Removals under the Network Enforcement Law*, GOOGLE (2018), http://perma.cc/L8PY-RAQ4.

41 *Removals under the Network Enforcement Law*, GOOGLE (2018), http://perma.cc/Z98S-25V5.

42 Centre For European Policy Studies, Germany's NetzDG: A Key Test For Combatting Online Hate 9 (2018).

43 *NetzDG Transparency Report*, FACEBOOK (July 2018), http://perma.cc/99SR-E3T9.

44 Netzwekdurchsetzungsgesetz, *supra* note 1, at §2(2)(1).

45 *Id.* at § 2(2)(3).

46 *Id.* at § 1(3).

47 *See* Michael Bohlander, trans., Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 1 of the Law of 24 September 2013, Federal Law Gazette I p. 3671 and with the text of Article 6(18) of the Law of 10 October 2013, Federal Law Gazette I p 3799. Bundesgesetzblatt [Criminal Code], Nov. 13, 1998, BGBL II, last amended by Gesetz [G], Sept. 2013 BGBL II, *translation at* http://perma.cc/Y6DK-FAEQ.

4. Encouraging the commission of a serious violent offense endangering the state (§ 91)
5. Treasonous forgery (§ 100(a))
6. Public incitement to crime (§ 111)
7. Breach of the public peace by threatening to commit offenses (§ 126)
8. Forming criminal or terrorist organizations (§§ 129–129(b))
9. Incitement to hatred (§ 130)
10. Dissemination of depictions of violence (§ 131)
11. Rewarding and approving of offenses (§ 140)
12. Defamation of religions, religious and ideological associations (§ 166)
13. Insult (§ 185)
14. Defamation (§ 186)
15. Intentional defamation (§ 187)
16. Violation of intimate privacy by taking photographs (§ 201a)
17. Threatening the commission of a felony (§ 241)
18. Forgery of data intended to provide proof (§ 269)

Content which is determined to be "manifestly unlawful," because it violates one of the above criminal provisions, must be removed within twenty-four hours, although a company may work with law enforcement to receive an extension.[48] Content which is merely "unlawful" must be removed or have access blocked within seven days.[49] There is no guidance about how to determine whether something is manifestly unlawful under the law other than the related criminal statutes,[50] so companies must make their own determination or seek the outside assistance of an attorney.

---

48 Netzwerkdurchsetzungsgesetz, *supra* note 1, at § 3.

49 *Id.*

50 The statutes vary in effectiveness and clarity. For example, the definition for "insult" only reads "An insult shall be punished with imprisonment not exceeding one year or a fine and, if the insult is committed by means of an assault, with imprisonment not exceeding two years or a fine." Bohlander, *supra* note 47, at § 185. Whereas the definition of "[b]reach of the public peace by threatening to commit offences" states, in detail:

> (1) Whosoever, in a manner capable of disturbing the public peace, threatens to commit
>
> 1. an offence of rioting indicated in section 125a 2nd sentence Nos 1 to 4;
>
> 2. murder under specific aggravating circumstances (section 211), murder (section 212) or genocide (section 6 of the Code of International Criminal

If a user's content is removed, currently the only recourse they have is at the discretion of the social media company. If the decision depends on the falsity of a factual allegation or other factual circumstances, the network may give a user an opportunity to respond.[51] Unfortunately, this is not required, and the law contains no mandatory recourse for individuals whose content is removed at the initial "manifestly unlawful" stage. However, as is discussed throughout this Comment, affected individuals may appeal to the courts.

2. The three initial concerns about the interaction between freedom of expression and the Network Enforcement Act are censorship, overblocking, and removal of lawful content

The Network Enforcement Act raises three main concerns with regard to freedom of expression. First, there is the issue of censorship. Second, there is the problem of overblocking, which leads to to a chilling effect on speech. Finally, there is the issue of what "remove" really means and the exportation of censorship to other countries.

a) Censorship

Politicians from Germany's far-right party, Alternative for Deutschland (AfD), are among the law's staunchest opponents.[52] AfD members argue that the law permits state-sanctioned censorship based on their beliefs, rather than the

---

> Law) or a crime against humanity (section 7 of the Code of International Criminal Law) or a war crime (section 8, section 9, section 10, section11 or section 12 of the Code of International Criminal Law);
>
> 3. grievous bodily harm (section 226);
>
> 4. an offence against personal freedom under section 232(3), (4), or (5), section 233(3), each to the extent it involves a felony, section 234, section 234a, section 239a or section 239b;
>
> 5. robbery or blackmail with force or threats to life and limb (Sections 249 to 251 or section 255);
>
> 6. a felony endangering the public under sections 306 to 306c or section 307(1) to (3), section 308(1) to (3), section 309(1) to (4), section 313, section 314 or section 315(3), section 315b(3), section 316a(1) or (3), section 316c(1) or (3) or section 318(3) or (4); or
>
> 7. a misdemeanour endangering the public under section 309(6), section 311(1), section 316b(1), section 317(1) or section 318(1),
>
> shall be liable to imprisonment not exceeding three years or a fine.
>
> (2) Whosoever intentionally and knowingly and in a manner capable of disturbing the public peace pretends that the commission of one of the unlawful acts named in subsection (1) above is imminent, shall incur the same penalty.

Id. at § 126.

51 Netzwerkdurchsetzungsgesetz, *supra* note 1, at § 3(2)(3)(a).

52 AFD, FACEBOOK (Nov. 21, 2017), http://perma.cc/VM4Q-LFVH. A post where AfD says they "kept their word" and are requesting the cancellation of the Network Enforcement Act. It includes a link to a bill to repeal the act.

content of speech.[53] AfD ran afoul of the law almost immediately. AfD member Beatrix von Storch tweeted an incendiary response to the Cologne police department's New Year message, which was written in Arabic in addition to German, French, and English. Von Storch accused the department on Twitter of "appeas[ing] the barbaric, Muslim, rapist hordes of men."[54] Alice Weidel, the recently elected lead candidate of AfD, jumped to support her party member. She tweeted, "our authorities submit to imported, marauding, groping, beating, knife-stabbing migrant mobs."[55] Von Storch's account was suspended for twelve hours after her post,[56] while Weidel's tweet was blocked for German Twitter users.[57]

AfD is not alone in its objections to the law. The Left Party and the pro-business Free Democratic Party also have their own concerns about the law.[58] Germany has a difficult history with censorship that the Network Enforcement Act cannot help but echo. For example, during the Cold War, East Germany's feared Ministry for State Security, or Stasi, as well as the Ministry of Culture, had one of the most robust censorship programs in history.[59] Authors who wished to write a piece had to work with editors in a publishing house to ensure their manuscript did not contain any taboo topics prior to receiving authorization to print.[60] As time went on, it was not only the content of a piece that received scrutiny but the author's relationship to the State, as well as their commitment to socialism.[61] Internal and external reviewers, who could potentially be members of the State who wished to remove political enemies, potentially parallels the anonymous reporting of comments and posts online today.

While the Network Enforcement Act is not a prior restraint in the same way a license is, the similarities are difficult to ignore. The Network Enforcement Act is another law in a long line of attempts to censor content by proxy. Seth Kreimer illustrates several examples of proxy censorship through the internet perpetrated

---

53 Linda Kinstler, *Germany's Attempt to Fix Facebook Is Backfiring*, THE ATLANTIC (May 18, 2018), http://perma.cc/9A3P-DDRF.

54 Philip Oltermann & Pádraig Collins, *Two Members of Germany's Far-Right Party Investigated by State Prosecutor*, THE GUARDIAN (Jan. 2, 2018), http://perma.cc/R9U9-YC4U.

55 *Id.*

56 *Id.*

57 *Id.*

58 *Id.*

59 Carol Anee Costabile-Heming, *"Rezensur": A Case Study of Censorship and Programmatic Reception in the GDR*, 92 MONATSHEFTE 53, 54 (2000) ("[GDR's] structure [went] beyond censorship, a term that itself was taboo, and bec[ame] a type of systematic control.").

60 *Id.* at 56.

61 *Id.* at 58.

by France, Switzerland, Germany, and Britain.[62] As he explains, "[p]roxy censorship of the Internet is no passing fad; it is a growth industry of Internet regulation."[63]

The Council of Europe Commissioner of Human Rights has denounced such proxy censorship. As early as 2014 it stated "[r]ule of law obligations, including those flowing from Article[] . . . 10 . . . of the ECHR, may not be circumvented through ad hoc arrangements with private actors who control the internet and the wider digital environment."[64] The Council of Europe also recommended that "any restrictions on access to internet content affecting users under [member states'] jurisdiction [should be] based on a strict and predictable legal framework . . . and afford[] the guarantee of judicial oversight to prevent possible abuses."[65] The Network Enforcement Act has no such judicial oversight, except for when individuals march to the courthouse door on their own. While Germany is hardly encouraging Facebook to block unlawful content, it also is not discouraging the practice. The law looks very much like the German legislature is circumventing its Article 10 obligations by foisting them onto social media companies. However, the Council of Europe is merely an advisory body[66]—without a binding ruling from the ECtHR, there is little it could do legally to change Germany's policy.

b) Overblocking

Less maliciously, there is a concern of overblocking—the blocking of content which is not actually illegal. While the Bundestag assured companies that fines would only be levied against systematic actors, there are currently no checks on social media companies to determine whether the content they are blocking is actually unlawful. Determining the unlawfulness of content would "ordinarily take weeks in a German court," according to Mirko Hohmann, a project manager at the Global Public Policy Institute in Berlin.[67] Rather than allowing the speech to

---

62 Seth F. Kreimer, *Censorship by Proxy*, 155 U. PA. L. REV. 11, 19–20 (2006) (providing examples of: France attempting to impose liability on Yahoo! for making overseas Nazi messages, images, and paraphernalia available to French citizens; Swiss police inducing ISPs to block neo-Nazi sites; German courts requiring ISPs to block access to extraterritorial neo-Nazi websites; British telecom blocking access to sites on a child pornography blacklist).

63 *Id.* at 27.

64 COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, THE RULE OF LAW ON THE INTERNET AND IN THE WIDER DIGITAL WORLD (2014).

65 *Id.* at ¶ 16.

66 *Values*, COUNCIL OF EUROPE (2019), http://perma.cc/Q857-ZSA7 ("The Council of Europe promotes human rights through international conventions. . . It monitors member states' progress in these areas and makes recommendations through independent expert monitoring bodies.").

67 Kinstler, *supra* note 53.

propagate and potentially cause harm while waiting for the courts to adjudicate it, the Bundestag has decided to shift the cost of court adjudication to its citizens and tech companies. Now, without the guidance that years of judicial experience would provide, tech companies are sent out to sea to determine what content is manifestly unlawful, and citizens whose speech is removed bear the cost of their silence alone "with none of the due process guarantees that preserve accuracy in the public sector."[68] Additionally, because the fines for noncompliance are so high, private actors have a much greater incentive to protect themselves from sanctions, as opposed to maintaining the free expression rights of their customers.

Unfortunately, there is no way around this. Speed is among the primary reasons the law is considered necessary. Once content is placed on the web, it spreads like wildfire and becomes difficult to remove. The Bundestag was not thinking of fringe cases of people blowing off steam, or satire. Instead, it was thinking of imminent threats of violence that need to be removed immediately.[69] However, the chilling effect it could have on speech cannot be denied. Contesting removal of a post can take weeks,[70] and for the average user it may not be worth doing.

c) Removal

Finally, the lack of definition for "removal" brings the law into an international context. What the German Bundestag likely had in mind was that a post would be taken down for German users. However, Alice Weidel once again provides an example of why this is far more complicated than it sounds. In May, a court in Hamburg said that Facebook did not do enough to prevent German users from viewing a comment on a Huffington Post article about Weidel's opposition to gay marriage.[71] The comment referred to Weidel as "Nazi Drecksau" (filthy Nazi swine) and attacked her sexual orientation (Weidel identifies as a lesbian).[72] While Facebook immediately blocked the comment from German IP addresses, Weidel could still see it in Switzerland and other German-speaking countries.[73] Therefore, German users within Germany who used an IP address that makes them appear to be outside of Germany could still view the

---

68 Kreimer, *supra* note 62, at 28.

69 *Maas verteidigt Gesetz gegen Hass im Internet*, SPIEGEL ONLINE (Apr. 1, 2018), http://perma.cc/67DK-7X6K ("Calls for murder, threats and insults, sedition or Auschwitz lie [Holocaust denial] are not expressions of freedom of expression, but rather are attacks on the freedom of expression of others.").

70 *Id.*

71 *Id.*; *see also* Joachim Huber, *Alice Weidel gewinnt Rechtsstreit mit Facebook*, DER TAGESSPIEGEL (Jan. 5, 2018), http://perma.cc/HSS3-QNBC.

72 *Maas verteidigt Gesetz gegen Hass im Internet*, *supra* note 69.

73 *Id.*

post. The Hamburg court ruled that because it was viewable in Germany using a VPN[74] if Facebook did not rectify the issue it could face a fine of up to 250,000 Euros or imprisonment of up to two years.[75]

On the face of the law, this is a perfectly acceptable outcome. However, with respect to international norms, this is unprecedented. Of course, Facebook could just pay the fine and refuse to remove the content—Facebook's income for 2018 was 55.8 billion dollars, a figure which even the maximum fine would not scratch.[76] However, the lack of clarity in the law regarding what it means to remove a post could lead to other courts following Hamburg's example. This would result in the exportation of German criminal law across the globe in a way that is dangerously overbroad. It also leads to further questions—how *should* a company determine a user's location? Should unlawful content that is visible in Germany, but originates outside of it, be included? After all, if Weidel's commenter had posted from Austria, Switzerland, or another German-speaking country it is not clear whether the law requires that Facebook still honor her request to remove the content.

This is not a classroom hypothetical. The Court of Justice of the European Union recently heard a case on substantially similar grounds related to the General Data Protection Regulation (GDPR). GDPR is a regulation intended to "protect[] fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[77] Unlike the Network Enforcement Act, which is nominally German law, GDPR applies extraterritorially to all companies when processing the data of European consumers.[78] GDPR granted consumers new data rights, such as the right to data breach notification, right to access and receive information about data a given company collects on them, as well as the right to data erasure, or the right to be "forgotten."[79] A French privacy firm, CNIL, argued that its clients should be able to be "forgotten" online, as is their right under GDPR, not only within the boundaries of the E.U. but absolutely and internationally. CNIL argued that they were only asking for what the E.U. had

---

74 A VPN, or Virtual Private Network, allows users to create a secure connection to another network over the internet. VPNs can be used to access region-restricted websites, so a viewer in Germany can appear to be in France.

75 David Meyer, *Facebook's New Court Defeat: This Time it 'May Have Free Speech Implications'*, ZDNET (May 1, 2018), http://perma.cc/66DS-SRY2.

76 FACEBOOK, INC., Annual Report (Form 10-K) 59 (Feb. 1, 2018).

77 Regulation (EU) 2016/679 of the European Parliament and 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 [hereinafter GDPR], at art. 1(2), http://perma.cc/W56Q-AKZW.

78 *Id.* at art. 3(1).

79 *Id.*

already granted. Google's lawyers, supported by legal counsel from other tech companies, pushed back. Not only would the system be "untenable," but it would potentially affect access to information and freedom of expression in countries across the globe.[80]

The Network Enforcement Act could lead to even bigger conflicts. Unlike GDPR's data erasure provision, where a given consumer is requesting that information about themselves be removed, the Network Enforcement Act forces the removal of content that the consumer explicitly does not want to be removed. This could potentially lead to novel and impossible to solve conflict-of-laws issues. If an American college student visits a German news site for a class and is moved to insult the person in the article, the First Amendment and the Network Enforcement Act could have the ultimate legal showdown, with social media companies trapped in the middle.

C. The Brussels Effect, and Why the European Court of Human Rights Should Adjudicate This Law

What happens in Germany and the E.U. on the internet has an outsized effect on global internet culture. Anu Bradford has coined this phenomenon "The Brussels Effect" in order to describe the "deeply underestimated aspect of European power that the discussion on globalization and power politics overlooks: Europe's unilateral power to regulate global markets."[81] The simplest example of this is privacy. As discussed in Section II(B), depending on how the European Court of Justice interprets GDPR, the right to be forgotten could change legal rights for people all over the world.

For social media companies, this influence is often exerted without utilizing legal channels. For instance, the code of conduct to counteract hate speech mentioned previously is not binding law. These "voluntary" measures have their own advantages and disadvantages because they allow "[the circumvention of] the E.U. charter on restrictions to fundamental rights, avoiding the threat of legal challenges, and taking a quicker reform route."[82] Thus, while appearing to be all stick and no carrot, the Network Enforcement Act at least has the benefit of being justiciable in open court.

Nevertheless, depending on how courts interpret the law, German criminal law might easily be moved far outside its borders. Weidel's case is a good example of this. A rude comment, such as the one she fought, would likely not have

---

80 Mark Scott, *In Google Privacy Case, Europe's Highest Court to Decide on Future of the Web*, POLITICO (Sept. 12, 2018), http://perma.cc/TU2F-FPZB.

81 Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 3. (2012).

82 Frosio, *supra* note 30, at 13–14.

implicated removal in other portions of Europe. The German criminal code's particular sensitivity to references to the Nazi Party, as well as their unusual *Beleidigunggesetz*, or law protecting people against insults, goes well beyond standard defamation law—particularly how U.S.-based tech companies would understand it.[83] "The decentralized, global nature of the internet means that almost anyone can present an idea, make an assertion, post a photograph or push to the world numerous other types of content, some of which may be illegal in some jurisdictions or offensive in some cultures."[84] It is the fact that regulations concerning the internet are so porous that makes it especially important that this law is adjudicated by an international court, so as to avoid the German legislature making decisions on behalf of seven billion people, rather than the eighty million they were elected to represent.

III. THE EUROPEAN COURT OF HUMAN RIGHTS AND ARTICLE 10

This Section discusses the history of Article 10 of the ECHR, as well as the history of the ECtHR generally. Because Germany is a signatory country to this treaty, the ECtHR can have jurisdiction over a case brought to it, provided that the petitioner exhausts their opportunity for relief within their own country. Section III(B) explains why Germany's highest court will likely find that the Network Enforcement Act is constitutional under Germany's Basic Law for the Federal Republic of Germany, which acts as the country's constitution. The final section explains how Article 10 cases have been reviewed generally, in order to provide context for how those rights may apply to the Network Enforcement Act. It explains that the two principles of necessity and proportionality are key to examining Article 10 cases.

A. History of Article 10 of the ECHR and the European Court of Human Rights

The ECHR was opened for signature in Rome in November 1950 and entered into force three years later.[85] The Convention was a response to the human rights atrocities committed before and during the European theater of

---

83 Erik Kirschbaum, *In Germany It Can be a Crime to Insult Someone in Public*, L.A. TIMES (Sept. 6, 2016), http://perma.cc/7JTF-45KP.

84 Frosio, *supra* note 30, at 2.

85 COUNCIL OF EUROPE, THE CONSCIENCE OF EUROPE: 50 YEARS OF THE EUROPEAN COURT OF HUMAN RIGHTS 22 (Egbert Myjer et al. eds., 1st ed. 2010).

WWII, as well as the rise of communism in the Eastern Bloc.[86] The drafters of the Convention, the Council of Europe, intended to provide an institutional framework based on liberal democratic values to overcome the extremism of fascism and to set a counterbalance against a looming threat of Stalinist communism.[87] The ECHR is only applicable to member states, which currently includes Germany as well as forty-six other European countries.[88] The ECHR is enforced by the ECtHR, also referred to as "the Strasbourg Court" due to its location in Strasbourg, France.

Like most post-war international human rights treaties, the ECHR establishes a set of enumerated rights. Article 10 instituted freedom of expression as one of those rights.[89] The landmark case, *Handyside v. United Kingdom,*[90] established the importance of freedom of expression to the ECtHR. There, the court stated: "freedom of expression is 'one of the essential foundations' of a democratic society."[91] Although it is only two paragraphs, Article 10 is complicated. It articulates multiple freedoms of expression, including the freedom to express one's opinion, receive information, and communicate information.[92] Freedom of expression also applies not only to ideas that are "favorably received or regarded as inoffensive. . . but also to those that offend, shock or disturb."[93] What constitutes expression is also incredibly broad. Paintings, books, cartoons, films, video-recordings, statements in radio interviews, and pamphlets are all included.[94] Most importantly for this Comment's purposes, the internet is also considered a valid place of expression.[95]

While the historical background of Article 10 provides a mandate of sorts to the ECtHR to protect freedom of expression, that same history has allowed the court to curtail freedom of expression that is seen to violate historical norms. This leads to biased jurisprudence when it comes to freedom of expression claims. The

---

86 *See generally* BERNADETTE RAINEY ET AL., JACOBS, WHITE, AND OVEY: THE EUROPEAN CONVENTION ON HUMAN RIGHTS (7th ed. 2017).

87 DAVID HARRIS ET AL., HARRIS, O'BOYLE & WARBRICK: LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 621 (3rd ed. 2014).

88 *47 Member States*, COUNCIL OF EUROPE, http://perma.cc/G23F-TGVR.

89 European Convention on Human Rights, *supra* note 9, at art. 10.

90 Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A) 49 (1976).

91 Mario Oetheimer, *Protecting Freedom of Expression: The Challenge of Hate Speech in the European Court of Human Rights Case Law*, 17 CARDOZO J. INT'L & COMP. L. 427, 427 (2009), *citing* Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A) 49 (1976).

92 European Convention on Human Rights, *supra* note 9, at art.10.

93 Handyside v. United Kingdom, *supra* note 90, at 18.

94 RAINEY ET. AL., *supra* note 86, at 484.

95 *Id.*

case law has evolved such that there is a presumption in favor of national authorities where they justify their laws based on "their fight against . . . anti-Convention values."[96] Anything related to the National Socialist Party or the Holocaust receives stricter scrutiny than other equivalent claims.[97] For example, while Germany may bar Holocaust denial and similarly anti-Semitic sentiments, the same prior restraints are not allowed for the Armenian genocide.[98]

B. How Article 10 is Applied Generally

The ECtHR follows a four-part test in determining whether an action violates Article 10. First, the ECtHR must determine whether the state action actually interferes with free expression. The court has found that a wide variety of activities, from run-of-the-mill censorship and confiscation to prohibitions on wearing symbols that communicate resistance, constitute interference with expression.[99] The important part of this analysis is whether the state is *directly* interfering with a person's expressive rights. Where the impact on speech is indirect—that is, "collateral to the exercise by the state of its authority for other purposes"—the ECtHR rarely finds that the matter breaches Article 10.[100]

Article 10 explicitly outlines ways in which states may abridge expression.[101] Of course, states abridge expression all the time in ways that are not enumerated by the ECHR—this Comment has already discussed a few. Article 10(2) explains that states are free to place formalities, conditions, restrictions, or penalties on speech provided they are "prescribed by law and are necessary in a democratic society."[102] Those two conditions provide the next two steps by which the ECtHR must analyze a freedom of expression claim. The second step, whether something is "prescribed by law," is usually the shortest. The "law" in the phrase "prescribed by law" means that a law must be foreseeable—that is, precise enough to allow applicants to reasonably predict that their actions would violate the law.[103] Precision does not only include the content of a law but also "the field it is designed to cover and the number and status of those to whom it is

---

96 DAVID HARRIS ET AL., HARRIS, O'BOYLE, & WARBRICK: LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 601 (4th ed. 2018).

97 Aleksandra Gliszczynska-Grabias & Grazyna Baranowska, *The European Court of Human Rights on Nazi and Soviet Past in Central and Eastern Europe*, 45 POLISH POL. SCI. Y.B. 117, 119 (2016).

98 RAINEY ET. AL., *supra* note 86, at 490.

99 *Id.* at 485.

100 HARRIS ET AL. (3rd ed. 2014), *supra* note 87, at 616.

101 ECHR, *supra* note 9, at art. 10 (states are allowed to license television).

102 *Id.*

103 *See generally* Open Door Counselling Ltd. v. Ireland, 246 Eur. Ct. H.R. (ser. A) (1992); Delfi AS v. Estonia, App. No. 64569/09, 2015-II Eur. Ct. H.R. 319.

address[ed]."[104] The court gives broad latitude to state legislatures in this step and rarely spends any time on this issue.

Instead, the bulk of the analysis lies in the third and fourth steps that make up the necessity test. The ECtHR must determine whether the free speech limitation is *necessary* in a democratic society, and, if it is necessary, whether it is *proportionate* to the legitimate aim pursued.[105] The court has stated: "'[N]ecessary', within the meaning of Article 10 § 2, implies the existence of a 'pressing social need'."[106] The court has also stated that "necessary" lies between "indispensable" and words like "'admissible', 'ordinary', 'useful', 'reasonable', [and] 'desirable'."[107] Article 10(2) outlines nine reasons a state might be allowed to interfere with speech due to necessity: national security interests; disorder or crime prevention; territorial integrity or public safety; protection of health or morals; protection of the reputation or rights of others; prevention of the disclosure of information received in confidence; or, maintaining the authority and impartiality of the judiciary.[108]

Even if necessity is found, an interference can be a violation of Article 10 if it is not proportionate. Proportionality is the fuzziest portion of this test. It is unclear who has the burden of proving or disproving proportionality.[109] Furthermore, what constitutes proportionality varies from case to case. The necessity for a restriction must be "convincingly established" and narrowly construed to be proportional.[110] Examples of interferences in Articles 8–11, which have violated the proportionality test include: the firing of a primary school teacher for being a member of the German communist party;[111] house searches and seizures without appropriate legislative or judicial safeguards;[112] criminal sanctions for homosexual activities between consenting men over the age of

---

104 Delfi v. Estonia, *supra* note 103, at ¶ 122.

105 *See generally* Handyside v. United Kingdom, *supra* note 90, at 16; European Convention on Human Rights, *supra* note 9, at art. 10.; Oetheimer, *supra* note 91, at 434.

106 Delfi v. Estonia, *supra* note 103, at ¶ 131.

107 Sunday Times v. United Kingdom, App. No. 6538/74, 30 Eur. Ct. H.R. (ser. A) ¶ 59 (1979).

108 ECHR, *supra* note 9, at art. 10.

109 STEVEN GREER, THE EXCEPTIONS TO ARTICLE 8 TO 11 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 15 (1997).

110 *Id.*

111 Vogt v. Germany, 323 Eur. Ct. H.R. (ser. A) (1995).

112 Greece v. United Kingdom, App. No. 176/56, 1959 Y.B. Eur. Conv. On H.R. (Eur. Comm'n on H.R.) (1958-59).

twenty-one;[113] as well as the conviction of a journalist who interviewed, and then reported on, three men who said racist remarks.[114]

In order to understand the Court's approach to proportionality, it is important to briefly discuss the margin of appreciation doctrine. According to Professor Yutaka Arai, "the 'margin of appreciation' refers to the latitude a government enjoys in evaluating factual situations and in applying the provisions enumerated in international human rights treaties."[115] Because of the importance of freedom of expression to a democratic society, the court is generally strict when assessing whether something is "proportional" under Article 10.[116] However, the content and kind of speech addressed may widen or narrow the margin of appreciation the court prescribes to states. Like most courts, the ECtHR acknowledges the fact that expression by the press gets wide protection,[117] as does political expression which criticizes the government.[118] However, artistic expression is in a less privileged position in the Court's eyes.[119] This balancing act between a state's needs and desires and the motivations of the ECtHR can make Article 10 claims particularly difficult to decide.

Outside of this test, Article 10 claims must also be analyzed in the context of other rights within the ECHR. This is mandated by Article 17, the prohibition on the abuse of rights. That provision states:

> Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein, or at their limitation to a greater extent than is provided for in the convention.[120]

In light of the historical context for the adoption of the ECHR, the ECtHR and Europe, in general, are "s[k]eptical of the ability of the democracy to resist the danger of racist propaganda leading to totalitarian dictatorships and massive abuses."[121] As such, Article 10 is not applicable where Article 17 applies.[122] This is

---

113 Norris v. Ireland, App. No. 10581/83, 13 Eur. H.R. Rep. 186 (1988).

114 Jersild v Denmark, App. No. 15890/89, 298 Eur. Ct. H.R. (ser. A) (1994).

115 YUTAKA ARAI-TAKAHASHI, THE MARGIN OF APPRECIATION DOCTRINE AND THE PRINCIPLE OF PROPORTIONALITY IN THE JURISPRUDENCE OF THE ECHR 2 (2002).

116 *Id.* at 136.

117 *Id.* at 127.

118 HARRIS (4th ed. 2018), *supra* note 96, at 608.

119 *Id.* at 612.

120 ECHR, *supra* note 9, at art. 17.

121 HARRIS (3rd ed.), *supra* note 87, at 621.

122 Oetheimer, *supra* note 91, at 429.

why German laws that ban speech denying the Holocaust and other forms of odious speech can be excluded from the scope of Article 10.[123]

Similarly, individual instances of speech may implicate other aspects of the ECHR. For example, defamation claims can be found to interfere with a person's Article 8 rights. Article 8 of the ECHR protects the right to "respect for private and family life, home, and correspondence."[124] Courts have found that an individual's reputation is included in their Article 8 rights.[125] Naturally, there are instances where one person's freedom of expression will conflict with another's right to personal integrity. Likewise, Article 9—freedom of religion[126]—and Article 10 will occasionally interact. Where this occurs, the court performs a balancing test between the rights as a part of the proportionality test.

C. Bringing a Network Enforcement Act Claim to the ECtHR

Only individuals, groups of individuals, and other member states may bring claims to the ECtHR.[127] Inter-state claims are relatively rare, with individual grievances making up the bulk of the court's 50,000 cases.[128] The ECtHR is a court of last resort. Before a claim may make its way to Strasbourg, France, it must first go through the entirety of the judicial system within the claimant's country.[129] As such, either an affected social media company or someone from within Germany will need to first raise a constitutional claim at the German Supreme Court to gain access to the ECtHR.

Article 5 of the Basic Law of the Federal Government of Germany is the German constitutional provision which governs freedom of expression. It merely states: "[e]very person shall have the right to freely express and disseminate his opinion in speech, writing and picture . . . There shall be no censorship."[130] The following section provides that "[t]hese rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honor."[131]

---

123 *Id.*

124 ECHR, *supra* note 9, at. art. 8.

125 HARRIS, (4th ed. 2018), *supra* note 96, at 608.

126 ECHR, *supra* note 9, at art. 9.

127 *Id.* at art. 33.

128 EUROPEAN COURT OF HUMAN RIGHTS, THE ECHR IN 50 QUESTIONS, at Question 19 (Feb., 2014).

129 European Convention on Human Rights, *supra* note 9, at art. 35(1).

130 Grundgesetz für die Bundesrepublik Deutschland, at art. 5(1), translated in BASIC LAW FOR THE FEDERAL REPUBLIC OF GERMANY (Christian Tomuschat & David P. Currie trans., 2008).

131 *Id.*

Operating under the assumption that every individual law the Network Enforcement Act is supposed to enforce has been found constitutional in Germany, recent scholarship suggests that the Act will also be found constitutional.[132] It is not censorship in the traditional sense because the state is not the one affecting content, and the content is being taken down post-publication, as opposed to a prepublication licensing scheme.[133] Further, overzealous enforcement by individual private actors is arguably not covered under a constitutional provision that is intended to monitor governmental actions. For example, Germany has long been known to require video game companies to censor Nazi symbols in their games in order to receive a license to sell the game.[134] Since 1998, when the *Wolfenstein 3D* case,[135] which solidified this policy, was decided, and until very recently video game manufacturers would remove Hitler's mustache, replace or block swastikas, or not release games in Germany at all in order to comply with the practice.[136] This censorship, which ended officially in August 2018,[137] never ended up in court after *Wolfenstein 3D*. Therefore, the premise of the law is still good. Germany can still force companies to comply with a law that violates freedom of art and arguably a consumer's freedom to receive information. In fact, in the Network Enforcement Act's case, the argument is even stronger because the statements are neither in a historical nor fantastical context—these are statements made by real people with real harms that the government seeks to prevent.

Additionally, none of the problems that the Network Enforcement Act arguably creates are new to social media companies nor unique to law. Companies have always had the ability to regulate speech according to their own terms of service. Neither the Council of Europe's anti-hate speech code nor the Network Enforcement Act changed the fact that the final step of review lies with the courts. Although the Network Enforcement Act acknowledges this fact wholeheartedly and moves even further towards private regulation, it is not clear that the Act itself

---

132 *See generally* Thomas Wischmeyer, *'What is Illegal Offline is Also Illegal Online' – The German Network Enforcement Act 2017*, *in* FUNDAMENTAL RIGHTS PROTECTION ONLINE: THE FUTURE REGULATION OF INTERMEDIARIES (Bilyana Petkova & Tuomas Ojanen eds., 2019).

133 *Id.* at 15.

134 Sebastien Schwiddesen, *German Attorney General: Video Game with Swastika Does Not Violate the Law; Constitutes Art*, LEXOLOGY (May 8, 2018), http://perma.cc/E3F4-W3CV.

135 *Id.* (Wolfenstein is a series of games set in Third Reich era Germany. Wolfenstein 3D has players kill members of the National Socialist Party, and they even go on to kill Hitler in the end. Naturally, Nazi imagery is pervasive throughout the game.)

136 *Id.*

137 Judith Vonberg, *Germany Lifts Ban on Nazi Symbols in Computer Games*, CNN (Aug. 10, 2018), http://perma.cc/LVL9-C6SV.

is the problem.[138] There are examples globally of social media companies blocking accounts and removing legal content because it violates their personal terms of service. The fact that they are not doing so at the behest of the government arguably does not make this any more or less problematic.

Once the Network Enforcement Act is found constitutional within Germany, the ECHR is implicated. Article 1 states: "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."[139] The ECtHR has found that there is a positive obligation to ensure freedom to receive information in certain contexts.[140] The court has also found that among the positive obligations a contracting party has is providing a legal framework that protects expression.[141] Given that the Network Enforcement Act is a German law, the court would have jurisdiction to hear it, despite the fact that private actors are making the final decisions.

IV. THE NETWORK ENFORCEMENT ACT AND THE EUROPEAN COURT OF HUMAN RIGHTS

This section analyzes whether the Network Enforcement Act is permissible under Article 10 of the ECHR by walking through the ECtHR's four-part test. Sections IV(B) and IV(C) argue that, for some of the criminal provisions, the law is neither necessary nor proportional to the needs Germany expressed a desire to protect when the law passed. For comparatively minor comments, which do not express imminent threats or acts of violence, the lack of due process afforded to those who have their comments removed is not proportional to the fines that social media companies may face for hosting those comments. Additionally, because social media companies already enforce their own terms of service as private platforms, it is not necessary for comments which fall under less severe categories. As such, these provisions of the law should be found to violate Article 10 of the ECHR.

However, this is a much closer issue than it might initially seem and highlights some of the problems the ECtHR will have to deal with when it comes to regulating social media companies in the future. As long as undesirable content is posted online, social media companies and global leaders will need to work together to keep the internet safe for everyone, while still providing a unified network.

---

138 Wischmeyer, *supra* note 132, at 16.

139 ECHR, *supra* note 9, at art. 1.

140 RAINEY ET. AL., *supra* note 86, at 515.

141 *Id.*

A. Important Precedent and Case Law

When examining the legality of the Network Enforcement Act, there are a few cases and terms that will be used extensively. Therefore, it is important to outline them at the forefront of the argument. While, as Section III(C) discussed, the court has a robust history of dealing with Article 10 claims generally, the internet and intermediaries have illuminated some of the weaknesses in that procedure. Most modern communication takes place over networks owned by private companies, which the court acknowledges "provides an unprecedented platform for the exercise of freedom of expression."[142] However, the court's Article 10 jurisprudence to date has addressed the historical fears of direct government censorship, and individual liability for infringing content. These fears have in some ways been overtaken by "censorship-by-proxy" fears,[143] which have not yet been extensively addressed.

As such, the court is in the process of developing new methodology when it comes to these internet intermediary liability cases. According to Robert Spano, a judge on the ECtHR, the court appears to be trying to strike a balance between two competing viewpoints. The first is net neutrality, described generally as the proposition that internet service providers should treat all traffic equally, regardless of origin.[144] The second is the viewpoint promoted by the European Commission: "what is illegal offline is also illegal online."[145] To date, the court has not staked out a full position on the role of intermediaries in general circumstances. However, their analysis with respect to certain kinds of claims is useful for predicting how the court would address a Network Enforcement Act claim.

One of the first cases to help establish the contours of this emerging methodology is *Delfi v. Estonia*.[146] *Delfi* is a landmark case, where the court for the first time laid out a framework for dealing with internet intermediaries in the context of news sites and Article 10. Delfi is an internet news portal that publishes

---

142 Delfi AS v. Estonia, *supra* note 103.

143 *Intermediary Liability*, THE CENTER FOR INTERNET AND SOCIETY AT STANFORD LAW SCHOOL, http://perma.cc/27LM-5SZG.

144 Robert Spano, *Intermediary Liability for Online User Comments under the European Convention on Human Rights*, 17 HUM. RTS. L. REV. 665, 667 n. 5 (2017).

145 *Id.* at 667. *See also* Communication from the Commission to the European Parliament COM 555, the Council the European Economic and Social Committee, and the Committee of the Regions, Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms (Sep. 28, 2017), at 2. ("*what is illegal online is also illegal offline* . . . addressing the detection and removal of illegal content online represents an urgent challenge for the digital society today.")

146 Delfi v. Estonia, *supra* note 103.

up to 330 news articles per day in Estonian and Russian.[147] It is historically one of the most visited websites in Estonia and Lithuania.[148] Like most modern online news sites, Delfi had a comment box at the bottom of its articles.[149] The articles received about 10,000 comments per day, which were monitored through reader complaints and submissions, as well as an algorithm which automatically removed comments that contained obscene words.[150] Delfi published an article about a ferry company, which implicated the company's majority shareholder (referred to only as L) in a plan to destroy an ice road.[151] This article generated 185 comments, of which twenty were personal threats or attacks directed to L.[152] L sued Delfi to force them to remove the comments, as well as for 32,000 Euros in non-pecuniary damages.[153] Delfi removed the comments, six weeks after they had been posted, but protested the damages.[154] The court held that Delfi was the discloser of the defamatory comments, and therefore they could be sued for defamation.[155] It also found that there was a legitimate interest in protecting the rights of others under Article 10, and that the fine was necessary and proportionate to protect that interest.[156]

A Network Enforcement Act claim would not simply be a repeat of *Delfi*. First, the Network Enforcement Act explicitly excludes news sites.[157] Conversely, as *Delfi* was a case of first impression for intermediary liability in this sphere, the court chose to narrow its ruling to the kind of company and the kind of speech at issue (a news site, and defamation, respectively).[158] The court explicitly refused to make judgments on the liability of social media platforms.[159] However, the court did establish the proposition that "certain intermediaries should play an active role in minimizing the spread of particularly harmful content."[160] A Network

147 *Id.* at ¶ 11.

148 GEMIUS RATING, *Domains*, http://perma.cc/4MSC-XHEZ.

149 Delfi v. Estonia, *supra* note 103, at ¶ 12.

150 *Id.* at ¶ 13.

151 *Id.* at ¶ 16.

152 *Id.*

153 *Id.* at ¶ 18.

154 *Id.* at ¶ 19.

155 *Delfi AS v. Estonia*, COLUMBIA GLOBAL FREEDOM OF EXPRESSION, http://perma.cc/5BPM-K6NG.

156 *See generally id.*; Spano, *supra* note 144, at 669-72; Delfi AS v. Estonia, *supra* note 103.

157 Netzwerkdurchsetzungsdesetz, *supra* note 1, at § 1(1).

158 Spano, *supra* note 144, at 670.

159 Delfi v. Estonia, *supra* note 103, at ¶ 116.

160 Lisl Brunner, *The Liability of an Online Intermediary for Third Party Content - The Watchdog Becomes the Monitor: Intermediary Liability after Delfi v. Estonia*, 16 HUM. RTS. L. REV. 163, 173 (2016).

Enforcement Act claim would force the court to address the tenuous issues left out of *Delfi* and establish exactly which intermediaries need to play an active role.

Second, *Delfi* concerned a series of comments, rather than an overarching notice and takedown regime like the one the Network Enforcement Act promotes. Nevertheless, the general scenario is very similar. In both cases, an intermediary, who does not have control over the content posted, is requested to remove unlawful content and faced with a fine for not doing so in a timely manner. The intermediary in *Delfi* was also a big name—Delfi is prominent in Estonia,[161] and the kinds of social media providers who the Network Enforcement Act targets are also likely to be prominent, based on their size.[162] This is in contrast to cases such as *Pihl v. Sweden,*[163] in which the insignificance of the website led the court to believe that the Article 8 harms the applicant suffered were outweighed by the chilling effect that third-party liability for the anonymous comments would have.[164]

A similar, but contrary, intermediary liability case is *Magyar Tartalomszolgáltatók Egyesülete and Index.hu v. Hungary*.[165] Once again, the Court addressed an intermediary's liability for comments on a news site. Magyar Tartalomszolgáltatók Egyesülete (MTE) is the self-regulatory body of Hungarian internet content providers, while Index is the owner of a major news portal in Hungary.[166] In this case, the site posted an article arguing that the business practices of two real estate management companies were unethical.[167] These included comments such as "[p]eople like this should go and shit a hedgehog and spend all their money on their mothers' tombs until they drop dead." ("Azért az ilyenek szarjanak sünt és költsék az összes bevételüket anyjuk sírjára, amíg meg nem dögölnek.")[168] Here, however, the comments were not found to be illegal, and therefore liability would be improper.[169] As the court described it, "Although offensive and vulgar . . . the incriminated comments did not constitute clearly

---

161 *See* GEMIUS RATING, *supra* note 148.

162 Recall that the Network Enforcement Act only affects social media companies with more than two million registered German users. *See* Netzwerkdurchsetzungsdesetz, *supra* note 1, at § 1.

163 Pihl v. Sweden, App. No. 74742/14, Eur. Ct. H.R. (2017).

164 *Phil v. Sweden*, COLUMBIA GLOBAL FREEDOM OF EXPRESSION, http://perma.cc/645V-R4H5. *See also* Pihl v. Sweden, *supra* note 163, at ¶ 35 ("However, the Court has previously found that liability for third-party comments may have negative consequences on the comment-related environment of an internet portal and thus a chilling effect on the freedom of expression via internet.").

165 Magyar Tartalomszolàltatòk Egyesülete and Index.hu v. Hungary, App. No. 22947/13 (Eur. Ct. H.R. 2016).

166 *Id.* at para. 5.

167 *Id.* at para. 11.

168 *Id.* at para. 12.

169 HARRIS ET AL., *supra* note 87, at 623.

unlawful speech; and they certainly did not amount to hate speech or incitement to violence."[170] They also found that because the domestic courts failed to address the liability of the commenters in addition to the liability of the website, the website could not be held liable.[171]

Magyar is important because it acknowledges that having a law that holds a "large Internet news portal" liable for third-party commenters is enough to meet the "prescribed by law" portion of the Article 10 analysis.[172] Additionally, by implementing fines for those comments, the state was clearly interfering with MTE and Index's freedom of expression.[173] This simplifies the Network Enforcement Act claim analysis considerably.

The final applicable case is *Tamiz v. United Kingdom,*[174] which was decided in late 2017. A short piece about Mr. Tamiz, alongside a photograph of him, was uploaded to a Blogger-hosted website "London Muslim."[175] Mr. Tamiz used the "report abuse" feature in late April to complain that the comments were defamatory.[176] In July, after clarification that the comments were false as well as defamatory, Google refused to remove the post or comments itself but did forward the complaints to the blog's author, who subsequently removed the comments and the post.[177] There, the court held that the domestic courts had adequately balanced an anonymous Google Blogger commenter's Article 10 rights with the applicant's Article 8 rights.

The court distinguished the case from *Delfi* by pointing out that here the Court was finally dealing with a social media platform "where the platform provider[] does not offer any content and where the content provider may be a private person running a website or blog as a hobby."[178] The court also pointed out that wide latitude in a case like this was important because platform providers, such as Google here, perform an important role in "facilitating access to information and debate on a wide range of political, social, and cultural topics."[179] Importantly, although this case was about individual comments rather than procedure generally, this is the first case that the court decided about a social media company.

---

170 Magyar Tartalomszolàltatòk Egyesülete and Index.hu v. Hungary , *supra* note 165, at para. 64.

171 *Id.*

172 *Id.* at para. 51.

173 Spano, *supra* note 144, at 673.

174 Tamiz v. United Kingdom, App. no. 3877/14 (Eur. Ct. H.R. 2017).

175 *Id.* at para. 7.

176 *Id.* at para. 17

177 *Id.* at para. 18-21.

178 *Id.* at para. 85 (citing Delfi v. Estonia, *supra* note 103, at ¶ 115-116).

179 *Id.* at para. 90.

B. The Network Enforcement Act is an Interference with Expression Prescribed by Law

The threshold questions of the ECtHR's freedom of expression analysis—whether a state action is an interference with expression and whether that interference was prescribed by law—are relatively simple to answer in light of the aforementioned case law. The Network Enforcement Act was a widely publicized law, passed by the national legislature, therefore it is certainly foreseeable enough to be "prescribed by law." As far as interference goes, the ECtHR in *Delfi*, *Pihl*, and *Tamiz* frequently referred to the Article 10 rights of providers as a given. That the social media companies who are tasked with removing comments have Article 10 rights has not been the subject of in-depth analysis by the court, but it is something that they recognize. For example, in *Tamiz*, the court consistently refers not only to the Article 10 rights of readers but also of Google and information society service providers ("ISSPs").[180] Since we are in the context of removing content at the direction of the state, with sanctions for noncompliance, it is clear that there is an interference with their rights.

C. Is Interference through NetzDG Necessary?

Given the nature of policy developments regarding the internet, while intermediary liability is not required by the ECHR, it does not go against the treaty. Therefore, the ECtHR will likely find that Germany's interference with freedom of expression through the Network Enforcement Act is necessary for many of the eighteen criminal provisions companies are asked to enforce. For example, the Act falls within the sweet spot of "desirable" and "indispensable" that the court described in *Sunday Times*[181] for dissemination of depictions of violence, public incitement to crime, and preparation of a serious violent offense endangering the state. Yet for other provisions, such as incitement to hatred, insult, or defamation, the line between desirable and necessary is much more permeable. There, because the harm is less, and because affected individuals may still go after the original commenters, liability for these companies is arguably not necessary.

It has never been a question that the internet, and by extension social media, needs to be regulated. The problem that courts have grappled with for the better part of two decades is *how*. If social media is like the press, then the ECtHR will more closely examine the necessity of regulations which restrict it. The ECtHR has emphasized on numerous occasions that the press is the "public watchdog in

---

180 *See generally id.*

181 Sunday Times v. United Kingdom, *supra* note 107, at para. 59

a democratic society."[182] However, as the court has recently encountered in cases like *Delfi*, the internet's speed and reach means that there is an increased likelihood that unchecked speech can infringe on other people's rights, such as their rights under Article 8.[183] Additionally, due to the potentially anonymous nature of comments, there may be limited means for an affected individual to respond to attacks on their reputation or private life. As such, there is a greater impulse to place pressure on "points of control" such as Facebook and Twitter in order to curb undesirable content.[184] There is growing support for the idea that social media companies should be seen as "gatekeepers" to information. Therefore, as gatekeepers, they "must assume an obligation as trustees of the greater good."[185]

The ECtHR has stated that due to the important role that ISSPs play in facilitating access to information and public debate, the state has a wide margin of appreciation in cases similar to *Tamiz*.[186] Even without that, Germany has strong arguments that the Network Enforcement Act is necessary for the interests of national security, public safety, the prevention of disorder or crime, and for the protection of the reputation or the rights of others. All of these are valid reasons to restrict speech under Article 10.[187] The Network Enforcement Act requests that social media providers remove only content which has already been determined to be unlawful within one day to one week. This request that social media companies remove content that is arguably unprotected under Article 10[188] seems reasonable.

Heiko Maas, Germany's Federal Minister of Justice and Consumer Protection, described NetzDG as *promoting*, rather than chilling, freedom of expression because it removes violent and unlawful content online.[189] Arguably, without something like the Network Enforcement Act, countries are creating a

---

182 RAINEY ET. AL., *supra* note 86, at 496.

183 *See id.* at 487; ECHR, *supra* note 9, at art. 8 (outlining the right to respect for private and family life).

184 *See, generally* Tamiz v. United Kingdom, *supra* note 174, at para. 75 (noting that while many user comments are likely defamatory, the majority of comments are likely to be too trivial or limited in publication to cause any significant damages to a person's reputation.); *See also* Kreimer, *supra* note 62, at 17.

185 Frosio, *supra* note 30, at 7 (citing ANDREW SHAPIRO, THE CONTROL REVOLUTION: HOW THE INTERNET IS PUTTING INDIVIDUALS IN CHARGE AND CHANGING THE WORLD WE KNOW 225 (2000)).

186 Tamiz v. United Kingdom, *supra* note 174, at para. 90.

187 ECHR, *supra* note 9, at art. 10(2)

188 Delfi v. Estonia, *supra* note 103, at para. 136 ("Moreover, the Court has held that speech that is incompatible with the values proclaimed and guaranteed by the Convention is not protected by Article 10 by virtue of Article 17 of the Convention.").

189 Deutscher Bundestag, *supra* note 10.

tiered system—speech which is okay online is "verboten" (forbidden) offline.[190] Additionally, Maas notes, speech which incites violence or abuses others has its own chilling effect.[191] This is a powerful argument. In 2016, a survey of German daily newspapers found that over half of the editorial teams did not allow comments on their own websites or on Facebook, in part due to how difficult it is to moderate right-wing and radical content.[192] As was described previously, none of the German provisions which social media companies have been tasked with enforcing has been declared to be in violation of any treaty or constitution. Therefore, the content which is correctly removed is arguably not violating anyone's expression.

Nevertheless, there is a strong argument that the Network Enforcement Act is not necessary for the more nuanced criminal provisions like defamation or insult. In those circumstances, the law certainly is not indispensable. Even assuming that, as the court presumed in *Delfi*, there is a tendency for platform providers to drag their feet when it comes to the removal of content, whether that is due to lack of knowledge, manpower, or actual bad faith varies from instance to instance. One reading of the *Delfi* judgment is that the fine was necessary to deter a notoriously bad actor from failing to remove content. After all, Delfi took six weeks and a lawsuit to remove the twenty comments against the applicant.[193] The companies affected by the Network Enforcement Act do not seem to have this issue. For example, Twitter, the company which received by far the most user (*Nutzern*) and trusted reporter (*Beschwerdestellen*) complaints in the first reports, only removed ten percent of those complaints.[194] The number seems large, but in the context of the sheer amount of content posted to the site[195] it is a drop in the bucket. In addition, the companies the law affects have already signed the Code of Conduct on Countering Illegal Hate Speech Online as discussed in Section II(A). There is therefore already an international framework that the Network Enforcement Act duplicates and narrows. Between a company's own terms of service and other international agreements, the Network Enforcement Act's fines merely provide another stick where one is not necessary.

---

190 *Id.*

191 *Id.*

192 Markus Reuter, *Umfrage: Zeitungsredaktionen Schränken Kommentarfunktionen 2015 Weiter ein*, NETZPOLITIK (Apr. 3, 2016), http://perma.cc/V5E2-7YXJ (translated "Survey: Newspaper editors continue to restrict commentary features in 2015.").

193 Delfi v. Estonia, *supra* note 103.

194 Twitter Netzwerkdurchsetzungsgesetzbericht, *supra* note 39.

195 According to Internet Live Stats, 6,000 tweets are sent per second. *Twitter Usage Statistics*, INTERNET LIVE STATS, http://perma.cc/AAY7-6MKH. That means it would take fewer than 5 seconds to reach the amount of content removed over those six months, and 45 seconds to reach the number of complaints lodged.

Moreover, the law might introduce further confusion. In the case of Twitter, Facebook, and Google, content subject to complaints was first screened using the company's own terms of service, which allows for the removal of legal and illegal content.[196] Whether companies are able internally screen content has come under scrutiny after the law's passage. In April 2018, a court in Berlin told Facebook that it could not block a user and delete their anti-immigrant comment because although it may have violated Facebook's community standards, it did not violate Germany's hate speech laws.[197] Yet, in late August 2018, a court in Munich ruled that Facebook may regulate speech on its own terms because freedom of expression exists only between citizen and state. However, the court also echoed Jürgen Habermas's idea of the "public sphere"[198] by commenting that Facebook must keep freedom of expression in mind because it is a "public marketplace for information and exchange of views (öffentlichen Marktplatz für Informationen und Meinungsaustausch)" despite the fact that it is a private company. [199]

This highlights the Left Party's initial hesitation with the Network Enforcement Act. In response to Heiko Maas's impassioned speech about promoting freedom of expression, a party member stated "*[d]as ist keine Durchsetzung gegenüber den Netzwerken, sondern durch die Netzwerke*"—"The Network Enforcement Act is not enforced against the networks but through the networks."[200] The Network Enforcement Act does not penalize companies for not removing content that was found in court to be unlawful. Instead, it asks social media companies to become the court and to enforce German law, in some cases as a substitute to their own terms of service. In a sense, the court in Berlin was acting as an appellate court to the court of Facebook, and in so doing overturned their institutional sovereignty.

This is a new direction for intermediaries, and the desirability of said direction is up for debate. Historically, anti-censorship laws and their enforcement have only applied to state actors. As Judge Spano points out, "Article 10 of the convention does not . . . mandate any particular form of intermediary liability."[201] Therefore, it is not apparent that Facebook must be held liable for third-party

---

196 *The Network Enforcement Act Apparently Leads to Excessive Blocking of Content*, REPORTERS WITHOUT BORDERS (Aug. 3, 2018), http://perma.cc/H3D9-T7ND.

197 David Meyer, *Facebook Can Block Hate Speech, Even If It's Not Illegal, Court Rules*, ZDNET (Sept. 18, 2018), http://perma.cc/D6YD-7ABK.

198 Franklin Foer, *The Death of the Public Square*, THE ATLANTIC (July 6, 2018), http://perma.cc/AXM5-8C5S.

199 Von Constantin Van Lijnden, *Facebook, Geben Sie Redefreiheit!,* FRANKFURTER ALLGEMEINE ZEITUNG (Sep. 6, 2018), http://www.faz.net/aktuell/feuilleton/medien/facebook-darf-nicht-eigenhaendig-beitraege-loeschen-15773244.html.

200 *Id.*

201 Spano, *supra* note 144, at 668.

content, or that it has any responsibility to monitor its content at all. As discussed previously, norms appear to be moving in that direction, but legally, the Network Enforcement Act is not desirable precisely because social media companies are private entities. As an example, all of the companies who were required to write transparency reports removed more content because it violated their own community standards rather than because it violated German law.[202]

However, if not social media companies, it is unclear who could handle these complaints. The traditional justice system seems currently unable to deal with the sheer mass and speed of the dissemination of unlawful content on the internet in a timely manner. Thus, there are few alternatives to social media providers defining and enforcing the ground rules for online speech through private community standards.[203] After all, these companies are the ones who may most quickly and effectively remove content on their platforms.

Therefore, while the ECtHR could find that the Network Enforcement Act is necessary in its entirety, the best approach that the court could take is to find the law necessary for some of the eighteen criminal provisions, but not for others. For example, encouraging the commission of a serious violent offense endangering the state, as well as public incitement to crime, have imminence that surrounds their offenses such that real harm could come from allowing the content to remain online. Therefore, fines and criminal sanctions levied against a negligent intermediary may seem necessary to induce a speedy takedown of that content. Conversely, with crimes like "insult" it is not clear that the law is doing anything more than what a company's own terms of service are doing. Additionally, as all of the court cases discussed have shown, whether something is insulting or defamatory to an individual is hard enough to determine. Whether it is insulting or defamatory enough to fine an intermediary is another question altogether. In those cases, without the immediate harm, it may be enough for Germany to do what it already has the ability to do—retrieve the information about the perpetrator and go after them through the normal court system.[204] Here, the duplicative nature and alternative method of dispute resolution mean that the law borders on merely desirable—not enough to warrant a finding of necessity.

D. Is the Interference Proportional?

There is no one standard for determining the proportionality of a law. As discussed in Section III(B), the ECtHR requires laws to be convincingly established and narrowly construed in order to be proportional. This analysis takes

---

202 Dorothée Baumann-Pauly, *German Companies Report on the Implementation of New Hate Speech Law*, COMMENTARY: NYU STERN CENTER FOR BUSINESS AND HUMAN RIGHTS (Aug. 7, 2018), http://perma.cc/VB89-6AR7.

203 Wischmeyer, *supra* note 132, at 16.

204 Kirschbaum, *supra* note 83.

into consideration the kind of speech affected and the state's margin of appreciation. Following these guidelines, there is a strong argument that the Network Enforcement Act is not proportional for most of the eighteen criminal provisions it covers. Because the harm inflicted by most of the affected content is not comparable to the potential chilling effect that fines and government intervention have on speech, there is an imbalance between "the interests served by the measure and the interests that are harmed by introducing it."[205] There are three reasons for this imbalance. First, there is no due process or transparency for those whose speech is targeted. Second, there is no legal check on the legislature with regard to whom they fine. Finally, although the court rarely applies a least restrictive means analysis, it should do so here. It would find that this is not the least restrictive means of achieving Germany's goals for most of the criminal provisions in place, and therefore that the Network Enforcement Act is not proportional with respect to those provisions.

Before addressing the reasons the law is not proportional, it is important to note one reason which does not come into play—extraterritorial removal. The court has previously found that, following the margin of appreciation, states have the ability to choose the measures by which they deal with issues of obscenity.[206] Therefore, in *Perrin v. UK*[207] the court declined to review the conviction of an individual who ran a website which displayed pornographic images on a preview page, despite the fact that the images were legal both in the U.S., where the company was based, and other states in Europe. As such, there is no reason to believe that the court would be persuaded by the argument that the Network Enforcement Act would violate the Article 10 rights of citizens of other states, either because they posted in German or because they have a right to access the contested information.

Currently, the law has no guarantee of due process rights. Tech companies are not required to allow people to explain their comments or content before removing them. Such a requirement is something which the European Commission has recommended.[208] There is no official channel, other than the court system, for undoing tech companies' conduct. Even if one were to go

---

205 Janneke Gerards, *How to Improve the Necessity Test of the European Court of Human Rights*, 11 INT'L J. OF CONST. L. 466, 469 (2013).

206 HARRIS ET AL., *supra* note 87, at 637.

207 Perrin v. United Kingdom, App. No. 5446/03 (Eur. Ct. H.R. 2005). ("The fact that dissemination of the images in question may have been legal in other States, including non-Parties to the Convention such as the United States, does not mean that in proscribing such dissemination within its own territory and in prosecuting and convicting the applicant, the respondent State exceeded the margin of appreciation afforded to it.")

208 European Commission, C(2018) 1177, Commission Recommendation of 1.3.2018 on Measures to Effectively Tackle Illegal Content Online (Mar. 1, 2018).

through the courts, there is no requirement that the social media company keep a record of what it removed.[209] Therefore, the one piece of evidence a user has to vindicate their response may not be available. Whether this actually has a chilling effect on speech needs further study. Nevertheless, it is certainly a troubling aspect of the law, especially considering the fact that the law, unlike a judicial opinion, does not require companies to explain why they removed particular content.[210] This hardly balances the interests concerned with the free expression rights of individuals.

Likewise, companies cannot explain why a given piece of content was reported in the first place. This creates an environment conducive to discrimination. This is particularly true with regard to the categories, such as "insult," that are more open to interpretation. It would not be hard to imagine a scenario where potentially insulting comments are written, but only those relating to or posted by certain political parties or ethnic groups are targeted for reporting. There is a reason that many of the comments behind the challenged cases this Comment has discussed are authored by AfD members, beyond the party's anti-immigrant sentiment and Neo-Nazi ties.[211] AfD has been testing the limits of the law and using it to amplify its voice and message since the law has been passed.[212] The law could be weaponized by political parties to remove comments which target them at a disproportionate rate to other parties. Unlike the first example of the law's lack of transparency, this issue has no fix—it is nearly impossible to get data on what is *not* reported. Unless German law evolves to develop a disproportionate impact claim for free expression online, there is no way to guarantee an individual's due process rights in this regard.

The implications of this are particularly worrisome when it comes to administrative agencies. While the reports state whether the complaints came from governmental entities or users, there is nothing to stop government agencies from tracking individuals and reporting their content, regardless of whether they are in an "unconstitutional organization" or not. When Facebook or Twitter then refuses to remove it, the companies could be fined. Although it is unlikely to happen, the fraught history the West has with authoritarianism means that the court should find this argument persuasive.

The lack of transparency when it comes to fines is another issue in its own right. Although Heiko Maas emphasized the fact that fines of any size will only be

---

209 Human Rights Watch, *supra* note 31.

210 Baumann-Pauly, *supra* note 202.

211 Kate Connolly, *Chemnitz Riots Spark Calls for AfD to Be Put under Surveillance*, THE GUARDIAN (Sept. 4, 2018), http://perma.cc/TB39-XHPV.

212 Kinstler, *supra* note 53.

levied on "systematic" actors,[213] the text of the law does not include that guarantee. An additional reason a check on power is necessary is so that fines are not limited to one provider. There is nothing to stop the legislature from targeting one or two companies as opposed to all companies in violation of the law. The fact that the law is colloquially referred to as "the Facebook Law" does not assuage this concern.[214] Without this particular safeguard, the law as applied to certain companies could be disproportionate to the rights that the government seeks to protect. This is an argument which needs to develop with time—to date, no company has faced fines from the law.

To the second point, placing a burden this heavy on tech companies is disproportionate to the harm caused by these posts. As Google's lawyers in *Tamiz v. United Kingdom* argued,

> [H]olding ISSPs liable from the moment the first letter of complaint was received, without allowing a reasonable period of time to investigate the merits of a complaint, to contact the author of the blog or comment, and take the necessary technical and practical steps to facilitate removal, would [] result in a disproportionate interference with the ISSP's Article 10 rights. In order to strike a fair balance between the interests of the aggrieved person and the provider of the blogging platform, an ISSP must be afforded a reasonable period of time to investigate and evaluate a request to remove a comment and, where appropriate, to implement removal. To find otherwise would effectively compel ISSPs to remove comments immediately following a complaint, without first considering its merits, and this would likely stifle legitimate speech and suppress the publication of information on important matters of public interest.[215]

Although the court did not directly address the proportionality of the response, Google's point still stands. The Network Enforcement Act is not proportionate because it provides every incentive to over-police content with no oversight, and no equivalent incentive to ensure that lawful content is not deleted. There is no case of the Court finding disproportionality on these grounds because the recent cases like *Tamiz* and *Delfi* have not addressed the issue. Nevertheless, the argument is persuasive. Unlike individuals posting, governments assume that companies are rational actors who will do the bare minimum to maintain the culture of their platforms and avoid legal costs. This is the way that fines are expected to work—by increasing the cost of unlawful behavior, such that it is no longer in a company's best interest to behave in that way.[216] Although no evidence of over-blocking has yet been found, there is a real concern that it may occur. When it does occur, it is unclear that it will be detectable or enforceable. In order to demonstrate over-blocking, users will have to go to the courts or the press to

---

213 Deutscher Bundestag, *supra* note 10.

214 Kinstler, *supra* note 11.

215 Tamiz v. United Kingdom, *supra* note 174, at para. 71.

216 *Fine and Punishment*, THE ECONOMIST (July 21, 2012), http://perma.cc/4TTY-RG67.

show that their content was improperly removed. Without the possibility of some individual benefit, users are unlikely to do so.

Finally, the Network Enforcement Act is not the least restrictive means by which Germany can target the harm caused by this content. There are rare examples where the court has found that the benefits a law provides are outweighed by the harms it causes under a least restrictive means analysis.[217] The Network Enforcement Act provides an example of why such an analysis should be applied to intermediary liability cases. Here, social media companies are ostensibly being sanctioned for their omissions. However, in practice, they are indirectly being used to sanction the true wrongful agents—the people who post unlawful content. In *Tamiz* and in *Delfi*, the ECtHR examined alternatives to suing the intermediary before determining whether the action was valid or not. Part of the reason the ECtHR decided *Tamiz* the way it did was because the applicant could have found the actual commenters and sued them or sued the individual who placed the article on Blogspot, before suing Google.[218] *Tamiz* was not a case "in which no measures were in place to enable the applicant to protect this Article 8 rights."[219]

The Network Enforcement Act, by design, creates circumstances where no measures are in place to enable applicants to protect their Article 10 rights. In many ways, it prioritizes the Article 8 rights of the complainers over the Article 10 rights of the commenters. As the divided lower court decisions discussed earlier show, there is a chance that social media companies could get their decisions wrong. With no formal mechanism other than the courts to help individuals adjudicate their rights, chilling of speech is inevitable.

On balance, it is arguable that the court should find in favor of the Network Enforcement Act for content which incites violence or promotes terrorism. But for all other content, no matter how insulting or demeaning, it is not proportional. By drawing this line, the court could help clarify its own jurisprudence and strike the balance that it desires. Rather than helping facilitate obstacles to a unified internet and encouraging a fragmented digital economy, the court could find that although some content is internationally undesirable, the harm to the free expression rights of intermediaries outweighs the harm to individuals for other content. This would pave the way for international cooperation on goals relating to regulations for the internet—something which, as a policy matter outside the scope of this Comment, is desirable.

---

217 Gerards, *supra* note 205, at 483.

218 Tamiz v. United Kingdom, *supra* 174, at para. 82.

219 *Id.*

V. CONCLUSION

The Network Enforcement Act suffers from the issues all laws passed with short notice and out of fear suffer from: it is vague, overbroad, and pins the moral blame for very real issues on the wrong individuals. By laying the blame at the feet of social media intermediaries rather than at the actual perpetrators of hate speech and violent actions, it effectively shoots the messenger. The ECtHR should find that this law violates Article 10 for all criminal provisions other than those which implicate imminent violence or threats to government agencies. Even then, the law is arguably not necessary because of the fact that the European Union is working towards its own version of regulating speech and conduct online, on top of regulations that already exist. Still, at least with regard to the worst conduct, the fines that companies could potentially receive for not monitoring their content are more proportional to the harms which they seek to prevent.

This is not to say that the impetus behind the law is misguided—social media companies do need to be regulated. We are beyond the times where such companies could be viewed as paper and pens that radical and violent individuals use to write posters. Instead, they look more and more like billboards on the side of the highway who choose to sell their space and turn a blind eye to the consequences of who posts. Also, speed matters when regulating the internet.[220] Mobilizing thousands of people with nothing more than a computer is the reality of our society today. Fighting the people who would use the internet to support their ill will is as difficult as fighting the mythic Hydra. If governments are Hercules, social media companies are Iolaus.[221] While governments are free to cut off all the heads they please, without social media companies to cauterize the wounds, the problems of hate speech and extremism will remain unsolvable.

This leads to the most important question, which is far outside the bounds of this Comment: the question of what the scope of social media regulation should be. The Network Enforcement Act is a proxy war in the ultimate battle over how to tame the internet. Companies censor legal content outside the scope of the Network Enforcement Act all the time. For example, Facebook's algorithms blocked and removed posts with variations on the phrase "men are scum,"[222] a

---

220 Take, for example, the case of Cody Wilson. Mr. Wilson wished to publish blueprints for 3-D-printed guns online in summer of 2018. The last time he posted blueprints for a handgun, they were downloaded 100,000 times from his site before the State Department ordered it to be taken down. *See generally* Kurtis Lee, *Want to Make a Gun with a 3-D Printer? Here Is Why Gun Control Groups Oppose the Practice*, LA TIMES (July 31, 2018), http://perma.cc/DP8A-KXLN.

221 While Hercules would cut off the heads of the Hydra, Iolaus would cauterize the necks to prevent them from growing back.

222 Samuel Gibbs, *Facebook Bans Women for Posting 'Men Are Scum' after Harassment Scandals*, THE GUARDIAN (Dec. 5, 2017), http://perma.cc/XV7F-8YUP.

phrase which might violate their community guidelines but would be difficult to find illegal in most Western jurisdictions. In the first quarter of 2018, YouTube deleted nearly 9.8 million videos, many of which were flagged before anyone could view them.[223] At the same time, there is evidence to suggest that companies are still not doing enough to curb extremist speech on their platforms. If companies actively monitor content, they move further away from being the passive platforms most safe-harbor exceptions require. If companies ignore extremist and violent content, they become complicit in harassment at best or terrorism at worst. The Network Enforcement Act does not cause nor solve any of these issues.

What Germany's law does show is the problems with regulating the internet on a nation-by-nation basis. Social media combines all of the trickiest portions of free expression jurisprudence and forces it across borders. If courts hold that content must be globally removed, it will be impossible to uphold the Network Enforcement Act and respect the margin of appreciation other states have for monitoring content within their borders. As such the ECtHR will be hard pressed to find that any domestic law like the Network Enforcement Act is necessary or proportional as Article 10 requires. Such laws need to be propagated by large, international bodies such as the E.U. or the U.N. in order to ensure a plurality of countries agree upon what content needs to be regulated when.

Given the variety of free expression regimes across borders, the best solution is to focus on the content when there is an international consensus on its egregiousness and unlawfulness. For example, the E.U. has already decided that "propaganda that prepares, incites or glorifies acts of terrorism" should be removed from the internet.[224] Categories of speech like this, which are more clearly defined and at the core of undesirable online content, can avoid the controversy and balancing that other categories of speech, such as defamation, invite. They are also the categories of speech for which speed is of the utmost importance, and therefore where intermediary liability is an adequate deterrent. Narrowing the Network Enforcement Act to those categories would help Germany curb undesirable content online while giving Europe and the world a chance to create a single digital environment. Finding otherwise could lead to the end of the unified internet as we know it.

---

223 Wischmeyer, *supra* note 132, at 20.

224 *EU to Give Internet Firms 1 Hour to Remove Extremist Content*, ASSOCIATED PRESS (Sept. 12, 2018), http://perma.cc/U8KV-Z93T.