THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOLUME 22 STLR.ORG NUMBER 2

ARTICLE

HOW THE POOR DATA PRIVACY REGIME CONTRIBUTES TO MISINFORMATION SPREAD AND DEMOCRATIC EROSION

Wayne Unger[1*]

Disinformation campaigns reduce trust in democracy, harm democratic institutions, and endanger public health and safety. While disinformation and misinformation are not new, their rapid and widespread dissemination has only recently been made possible by technological developments that enable never-before-seen levels of mass communication and persuasion.

Today, a mix of social media, algorithms, personal profiling, and psychology enable a new dimension of political messaging—a dimension that disinformers exploit for their political gain. These enablers share a root cause—the poor data privacy and security regime in the U.S.

At its core, democracy requires independent thought, personal autonomy, and trust in democratic institutions. A public that thinks critically and acts independently can check the government's power and authority. However, when

[1*] Visiting Assistant Professor, Gonzaga University School of Law. Founding Attorney & CEO, The Unger Firm LLC. CEO, (Stealth Enterprise SaaS Startup). Researcher, Disinformation Working Group, Global Security Initiative, Ariz. St. Univ. Prior to his current work, Unger worked in Silicon Valley where he managed multimillion dollar corporate transformation initiatives for Cisco Systems; directed sales for the banking, finance, and technology industry segments for a SaaS startup (acquired by LexisNexis Risk Solutions for $480M in 2020); and led strategic partnerships and account management for a second startup. Unger holds a J.D. from the Sandra Day O'Connor College of Law, ASU and a B.S. in Supply Chain Management from W.P. Carey School of Business, ASU. I thank Dr. Diana Bowman and Logan Clark for their support and guidance on this Article; Scott Ruston and the Disinformation Working Group for their contributions; and the editorial team at Columbia's STLR for their suggestions, improvements, and edits. All ideas, arguments, and errors are my own. (e) wayne@ungerfirm.com.

the public is misinformed, it lacks the autonomy to freely elect and check its representatives and the fundamental basis for democracy erodes.

This Article addresses a root cause of misinformation dissemination —the absence of strong data privacy protections in the U.S.—and its effects on democracy. This Article explains, from a technological perspective, how personal information is used for personal profiling, and how personal profiling contributes to the mass interpersonal persuasion that disinformation campaigns exploit to advance their political goals.

I. INTRODUCTION

Since 2014, there has been a wave of disinformation by which foreign and domestic actors have launched information operations against democracies. These operations aim to influence, disrupt, corrupt, or usurp the decision-making of a targeted audience.[2] From Russian election interference to COVID-19 conspiracies and election fraud, disinformation and misinformation harm citizens' presumptive trust in democracy and democratic institutions. While misinformation is not new,[3]

---

[2] Marek N. Posard, et al., *From Consensus to Conflict*, RAND CORP. 3 (2020), https://www.rand.org/pubs/research_reports/RRA704-1.html (last visited / modified Oct. 15, 2020) [hereinafter "Rand Report"] (quoting Gen. Martin Dempsey, Chairman of the Joint Chiefs of Staff).

[3] *See generally* Jayson Harsin, *Post-Truth and Critical Communication Studies*, OXFORD RES. ENCYCLOPEDIA, COMM. 6 (June 24, 2020), https://edisciplinas.usp.br/pluginfile.php/5433790/mod_resource/content/1/Post-truth%20and%20critical%20communication%20studies.pdf (noting that scholars began discussing post-truth (legitimate vs. illegitimate knowledges) in the 1990s).

rapid and widespread dissemination of misinformation has only recently been made possible by technological developments that enable mass communication and persuasion never seen before.[4] While misinformation spreads through traditional or mass media (e.g., NBC, ABC, CNN, Fox News, etc.) and online channels, this Article focuses on the internet-enabled dissemination channels because these channels have a broader reach and allow for more mass interpersonal persuasion.[5]

Today, a mix of social media, algorithms, personal profiling, and psychology enable a new form of political messaging.[6] These enablers share a root cause—the absence of a strong data privacy and security regime in the U.S.

At its core, democracy requires independent thought, personal autonomy, and trust in democratic institutions.[7] A public that thinks critically and acts independently can check the government's power and authority.[8] Civil liberties, such as the freedoms of speech and press, enable the "unfettered interchange of ideas for the bringing about of political and social changes desired *by the people*," who ultimately hold the supreme power in a democracy.[9] However, when the public is misinformed, it lacks the autonomy to freely elect and check its representatives, and the fundamental basis for democracy erodes. When citizens believe the misinformation, they are no longer informed of the truth, and are consequently unable to think independently or autonomously. Thus, once elected representatives are in office, citizens risk the inability to hold those elected representatives accountable.

This Article focuses on the absence of strong data privacy protections as a root cause of misinformation dissemination and the subsequent effects on American democracy.[10] This Article explains, from a technological perspective, how personal

---

[4] *See generally* B.J. Fogg, *Mass Interpersonal Persuasion: An Early View of a New Phenomenon*, PERSUASIVE TECH. (2008), https://link.springer.com/chapter/10.1007/978-3-540-68504-3_3#citeas (discussing how social media platforms enable the six necessary components of mass interpersonal persuasion).

[5] *See infra* Part II.B; s*ee generally* B.J. Fogg, *supra* note 4; Yochai Benkler, et al., *Mail-In Voter Fraud: Anatomy of a Disinformation Campaign*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y AT HARV. UNIV., Oct. 2, 2020, at 3-4, https://ssrn.com/abstract=3703701 (proposing three dissemination models: (i) social media dominant, (ii) social media led, and (iii) mass media led).

[6] *Id*.

[7] *See generally* U.N. Secretary General, *Guidance Note of the Secretary General on Democracy*, 5 (discussing general requirements and principles of democracies); Russell Weaver, *Fake News (& Deep Fakes) and Democratic Discourse*, 24 J. OF TECH. L. & POL'Y 35, 45 (2020) (discussing how free speech, thought, and discourse are foundational to freedom); Tal Zarssuky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRES IN L. 157 (2019) (discussing how manipulative actions interfere with an individual's autonomy).

[8] *See* Saxbe v. Wash. Post Co., 417 U.S. 843, 862-63 (1974) (Powell, J., dissenting) ("the societal function of the First Amendment [is to preserve] free public discussion of governmental affairs . . . public debate must only be unfettered; it must also be informed.").

[9] Roth v. United States, 354 U.S. 476, 484 (1957) (emphasis added).

[10] *See generally* Debra Cassens Weiss, *Sotomayor and Gorsuch Warn That Misinformation and Intolerance Can Threaten Democracy*, A.B.A. J. (Apr. 15, 2021), https://www.abajournal.com/news/article/gorsuch-and-sotomayor-warn-that-misinformation-and-intolerance-can-threaten-democracy (U.S. Supreme Court Justices Sotomayor and Gorsuch "warned of misinformation that

information is used for personal profiling, and how profiling contributes to the interpersonal persuasion that disinformation campaigns exploit to advance their political goals. While I provide various examples of disinformation campaigns and narratives, this Article is not a comprehensive analysis or summary.[11] Rather, this Article concentrates on the enablers of disinformation campaigns by foreign and domestic actors and the effect of the disinformation; it argues that Congress needs to strengthen trust and faith in our democracy and public institutions by enacting stronger data privacy and security protections.

Part II of this Article discusses disinformation campaigns. Part III details the enablers of disinformation campaigns. Part IV uses a case study to show that disinformation campaigns benefit from the current data privacy and security regime because the current regime is insufficient, causing societal polarization, and contributing to an erosion of democracy. Part IV also proposes reforms to the data privacy and security regime that, if enacted, could work to substantially curb disinformation spread online, and subsequently, preserve our democracy.

Before beginning, some definitions and caveats are in order. Disinformation is the *purposeful* dissemination of false information intended to mislead, deceive, or harm.[12] Related but different, misinformation is the *inadvertent* dissemination of false information.[13] Disinformers may produce misinformers, and shared misinformation typically originates from a disinformer.[14] While disinformation is closely linked to and often confused with misinformation, the two are notably different. However, this Article uses the terms interchangeably because it is more concerned about the spread of false information, without much regard to whether the false information is disseminated purposefully or inadvertently, and the enablers of this spread.

Even though disinformation campaigns have targeted countries around the world, this Article focuses on the U.S. for two reasons. First, there are well-documented and publicly available investigations, research, and examples related to misinformation and its effects on the U.S.[15] Second, the enablers of misinformation dissemination are prevalent in the U.S.[16] While it is important to recognize that the U.S. is both a disseminator and recipient of disinformation

---

spreads on social media," and how "[i]t is no surprise that a lot of the false misinformation spread on social media is deliberately spread by our enemies to sow disagreement internally in the country."); The exploitation of the poor data privacy and security regime by disinformation campaigns is not the sole cause of democratic erosion.

[11] While misinformation exists in various subject matters (e.g., anti-vaccine misinformation), this Article primarily focuses on political misinformation.

[12] *See* Harsin, *supra* note 3, at 8 (disinformation is a broad term that encompasses content commonly known as fake news, propaganda, parody, satire, manipulated content, false content, etc. This Article focuses on fabricated, misleading, or manipulated content).

[13] *Id.*

[14] *Id.*

[15] *See, e.g.*, Robert Mueller, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, DEPT. OF JUST. 14-35 (Mar. 2019), https://www.justice.gov/storage/report.pdf (hereinafter "Mueller Report").

[16] *See infra* Part I.

campaigns, and has deployed disinformation campaigns against foreign states to advance its own national interests, this Article focuses specifically on the American people as recipients of misinformation.

II. DISINFORMATION CAMPAIGNS

Coordinated disinformation campaigns, which have the goal of persuading, influencing, and manipulating people, are more prevalent today because the world is more interconnected than ever before.[17] Foreign and domestic actors can use these disinformation campaigns to achieve political goals.[18] In the 2016 Presidential Election, for example, Russia engaged in a targeted disinformation campaign intended to erode trust in democracy and assist Trump's campaign.[19] And in the 2020 election cycle, disinformation campaigns rapidly spread false information about in-person and mail-in voting.[20]

This Part explains how disinformation campaigns work, and how they result in the further spread of misinformation downstream. Section A discusses the rise of disinformation online. Section B explains the structure of disinformation campaigns. Section C turns to research to explain why and how disinformation spreads. This Part does not analyze why actors produce and distribute disinformation, but rather presumes these motivations and interests exist and are political in nature.

A. The Rise of Disinformation Online

Coordinated disinformation campaigns are not new.[21] Foreign and domestic actors have spread false news and propaganda to Americans for decades.[22] Similarly, the U.S. government and affiliates have launched information operations

---

[17] *See generally* Soroush Vosoughi, et al., *The Spread of True and False News Online*, SCI. MAG. 1146 (Mar. 9, 2018), https://www.doi.org/10.1126/science.aap9559 (analyzing the spread of false information on Twitter from 2006 to 2017) (for the study's methodology, *see* https://science.sciencemag.org/content/sci/suppl/2018/03/07/359.6380.1146.DC1/aap9559_Vosoughi_SM.pdf).

[18] *See generally* Mueller Report, *supra* note 15 and accompanying text.

[19] *Id.*

[20] *See* Ryan McCarthy, *"Outright Lies": Voting Misinformation Flourishes on Facebook*, PROPUBLICA (July 16, 2020), https://www.propublica.org/article/outright-lies-voting-misinformation-flourishes-on-facebook ("Facebook is rife with false or misleading claims about voting . . . these falsehoods appear to violate Facebook's standards yet have not been taken down or labeled as inaccurate.").

[21] *See* Matthew Hindman & Vlad Barash, *Disinformation, 'Fake News' and Influence Campaigns on Twitter*, KNIGHT FOUND. 9-12 (Oct. 2018), https://knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter/ (describing the history of disinformation, fake news, and propaganda. This study covered more than 10 million tweets from 700,000 Twitter accounts that linked to more than 600 fake and conspiracy news outlets. For more information regarding the study's methodology, *see* pages 19-22 of the report) [hereinafter "Knight Foundation"].

[22] *See id.*

against foreign states.[23] The dissemination of disinformation, however, changed with the advent of the internet and social media. This Section discusses the evolution of disinformation and its growth in the digital landscape.

There is a long history of disinformation campaigns in the United States. In the 19th century, the Associated Press spread false news stories that led to the Rutherford B. Hayes presidency and the end of the post-Civil War Reconstruction.[24] Britain led a fake news campaign to draw the U.S. into World War II.[25] During the Cold War, the Soviet Union targeted the West with disinformation run out of Department A—the nerve center for the global network of disinformation efforts run by the KGB.[26] One example of the false narratives they pushed was when the Soviet Union tried to blame the U.S. for the HIV/AIDS epidemic, by attempting to persuade the world the U.S. released HIV as a biological weapon.[27]

Domestic concern about foreign influence in elections has a similarly long history.[28] George Washington and Alexander Hamilton warned that foreign powers would seek to influence election outcomes to advance their own political interests.[29] Over two centuries later, these concerns regarding foreign interference are still valid. In 2018, for example, the Department of Justice indicted the Internet Research Agency LLC, a Russian entity with ties to Russian President Putin, for interfering in U.S. elections as far back as 2014.[30]

Yet despite their long history, disinformation campaigns are markedly different today. Over the last decade, disinformation mutated and metastasized as technology and social media have created new channels for dissemination.[31] The Russian interference in the 2016 U.S. presidential election illustrates this evolution.[32]

---

[23] *See* Roberto Garcia Ferreira, *The CIA and Jacobo Arbenz: History of a Disinformation Campaign*, 25 J. OF THIRD WORLD STUD. 59, no. 2 (2008), https://www.jstor.org/stable/45194479 (discussing the declassified documents related to the CIA's covert operation to overthrow Guatemalan president Jacobo Arbenz) (a discussion about the U.S. government or its affiliates disseminating disinformation campaigns is out of scope for this Article).

[24] Knight Foundation, *supra* note 21, at 9.

[25] *Id.*

[26] *Id.*; Nicholas J. Cull, et al., *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against It*, LONDON SCH. OF ECON. & POL. SCI. INST. OF GLOBAL AFF. 20 (Oct. 2017), https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.

[27] *See* Cull, et al., *supra* note 26, at 27; *see also* Christina Nemr & William Gangware, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, PARK ADVISORS 14-15 (2019), https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf [hereinafter "Mass Distraction"].

[28] Rand Report, *supra* note 2, at 1.

[29] *See id.*

[30] *Id.* at 2 (Hereinafter, the general references to Russia refer to the Internet Research Agency LLC and related organizations within the control of or controlled by the Kremlin—either directly or indirectly).

[31] *See* Knight Foundation, *supra* note 21, at 9.

[32] *See* Mass Distraction, *supra* note 27, at 14.

Russia's campaign created more than one million tweets, hundreds of Facebook posts, and thousands of YouTube videos to manipulate American voters.[33] Much of Russia's disinformation sought to promote then-candidate Donald Trump and attack the Democratic nominee, Hillary Clinton.[34] Similarly, in the 2020 U.S. presidential campaign, Russia continued its disinformation campaign by fabricating defamatory allegations against Hunter Biden in order to attack his father, then-candidate Joe Biden.[35]

Other foreign actors, such as Iran, built disinformation campaigns that resembled the Russian efforts.[36] Iran sought to manipulate the political discourse in the U.S. by promoting Iranian-friendly policy positions, such as anti-Israeli and pro-Palestinian narratives.[37] Using stolen voter information, Iran also targeted voters with threatening emails appearing to originate from the Proud Boys (a neo-fascist all-male right-wing group), which instructed recipients to "[v]ote for Donald Trump or else."[38]

Domestic actors have also launched disinformation campaigns against Americans to advance their own political goals. For example, following the death of George Floyd, far-right websites portrayed the Black Lives Matter protests as violent riots instigated by "[A]ntifa terrorists."[39] In addition, some conservatives shared false claims that rioters who attacked the U.S. Capitol on January 6, 2021, were members of Antifa and Black Lives Matter.[40]

There is evidence such campaigns are coordinated because the disinformation often originates from only a handful of sources. A Knight Foundation study revealed, for example, that 65% of false information on Twitter originated from ten disinformation websites.[41] One of the largest disinformation disseminators is the website Infowars.[42] Alex Jones leads it.

---

[33] *See id.* at 14-15.

[34] Mueller Report, *supra* note 15, at 19-31.

[35] Julian Barnes, *Russian Interference in 2020 Included Influencing Trump Associates, Report Says*, N.Y. TIMES (Mar. 16, 2021), https://int.nyt.com/data/documenttools/2021-intelligence-community-election-interference-assessment/abd0346ebdd93e1e/full.pdf

[36] *See* Mass Distraction, *supra* note 27, at 23.

[37] *Id.*

[38] Christopher Bing & Jack Stubbs, *Exclusive: 'Dumb Mistake' Exposed Iranian Hand Behind Fake Proud Boys U.S. Election Emails*, REUTERS (Oct. 22, 2020), https://www.reuters.com/article/us-usa-election-cyber-iran-exclusive/exclusive-dumb-mistake-exposed-iranian-hand-behind-fake-proud-boys-u-s-election-emails-sources-idUSKBN2772YL [hereinafter "Iranian Emails"].

[39] Richard Stengel, *We Should Be as Worried About Domestic Disinformation as We Are About International Campaigns*, TIME MAG. (June 26, 2020), https://time.com/5860215/domestic-disinformation-growing-menace-america/.

[40] *See* Michael Grynbaum, et al., *How Pro-Trump Forces Pushed a Lie About Antifa at the Capitol Riot*, N.Y. TIMES (Mar. 1, 2021), https://www.nytimes.com/2021/03/01/us/politics/antifa-conspiracy-capitol-riot.html.

[41] Knight Foundation, *supra* note 21, at 3 and accompanying text.

[42] *See, e.g.*, Tucker Higgins, *Alex Jones' 5 Most Disturbing and Ridiculous Conspiracy Theories*, CNBC (Sept. 14, 2018), https://www.cnbc.com/2018/09/14/alex-jones-5-most-

Alex Jones, a conservative personality who disseminates his messages via various online platforms and pushes countless conspiracy theories and falsehoods.[43] In defending himself against defamation claims, Jones stated in court filings that his comments were "opinion, not statements of fact," and that his website, Infowars, is a "freewheeling" website that publishes content loaded with hyperbole.[44] In other words, rather than defending himself by trying to show he believed in the truth of his claims, Jones merely argued they were opinions and not fact. Such admissions highlight the fact that Alex Jones *knowingly* and *deliberately* disseminates and perpetuates disinformation, and his listeners believe it.[45]

The pervasiveness of misinformation is a serious concern. Misinformation does not just undermine democracy and democratic institutions by perpetuating falsehoods;[46] it can also jeopardize public health and safety. For example, nefarious actors spread disinformation during the COVID-19 pandemic, including falsehoods about how the virus is transmitted and about the origins of the virus.[47] False and misleading information regarding the pandemic led to unnecessary transmissions, hospitalizations, and deaths.[48]

The pervasiveness of misinformation also prompts the question of how and why it spreads, especially when some are apt to dismiss the misinformation as a falsity. Before turning to how and why misinformation spreads, it is important to explain the anatomy of disinformation and disinformation campaigns.

B. The Anatomy of Disinformation and Disinformation Campaigns

Disinformation and disinformation campaigns are frequently structured in a common manner. To understand this structure, this Section explores what do disinformers do, and how they do it. The common structure of disinformation

---

disturbing-ridiculous-conspiracy-theories.html (listing examples of the conspiracy theories disseminated by Alex Jones).

[43] *Id.*; Alan Feuer, *Free Speech Scholars to Alex Jones: You're Not Protected*, N.Y. TIMES (Aug. 7, 2018), https://www.nytimes.com/2018/08/07/business/media/alex-jones-free-speech-not-protected.html.

[44] *Id.*

[45] *See, e.g.*, David Tarrant, *Why Do People Listen to Infowars' Alex Jones at all? We Asked Them*, DALLAS MORNING NEWS (Aug. 10, 2018) (containing interviews with Infowars listeners).

[46] *See infra* Part III.B.

[47] *See* J. Scott Brennen, et al., *Types, Sources, and Claims of COVID-19 Misinformation*, REUTERS INST. AT UNIV. OF OXFORD 6 (Apr. 7, 2020), https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation (finding the main types, sources, and claims of COVID-19 misinformation) (This study analyzed a sample of 225 pieces of misinformation rated false or misleading by fact-checkers and published between January and March 2020. For more information regarding its methodology, *see* Methodological Appendix).

[48] *See, e.g.*, Theresa Waldrop, et al., *Fearing Coronavirus, Arizona Man Dies After Taking a Form of Chloroquine Used to Treat Aquariums*, CNN (Mar. 25, 2020) https://www.cnn.com/2020/03/23/health/arizona-coronavirus-chloroquine-death/index.html (describing an Arizonan couple that ingested chloroquine phosphate in an apparent attempt to self-medicate for COVID-19 after the couple learned of chloroquine's connection to COVID-19 from President Donald Trump).

campaign can be analogized to a supply chain framework with four stages: (i) raw materials, (ii) production, (iii) distribution, and (iv) consumption.[49]

Figure 1: Disinformation Supply Chain.

The first stage of the disinformation supply chain is the "raw materials." Although deceitful information is an important ingredient, disinformation is not always based on complete fabrication. That is, disinformation may carry some level of true information[50] which is then pieced together to distort reality or create false impressions.[51] For example, much of the disinformation disseminated by Trump's 2020 campaign relied on some kernel of truth.[52] The Trump campaign produced multiple short videos by editing clips of Joe Biden to create a false narrative about Biden's cognitive decline or mental state.[53] The videos were not complete fabrications, because Biden had in fact made the statements as shown in the viral clips. But the Trump campaign misled and deceived viewers by applying false captions that purposefully mischaracterized Biden's mental capacity.[54] Thus, some level of true information is often the first ingredient of disinformation.

The second stage of the supply chain is "production" whereby foreign and domestic actors frequently manufacture disinformation.[55] This can include both creating content and purchasing advertisements on platforms such as Facebook. The end-products may include fabricated content, content employing a misleading context, manipulated content, or content with headlines that misrepresent what is actually portrayed (this is sometimes referred to as "false connection"). Figure 2 contains a breakdown of the various disinformation "products" which actors may manufacture:

---

[49] *See generally* U.S. DEP'T OF ST., GEC SPECIAL REPORT: PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM 8 (2020) [hereinafter "GEC Report"] (describing the five pillars of Russian disinformation campaigns).

[50] *See* Hunt Allcott, et al., *Trends in the Diffusion of Misinformation on Social Media*, STAN. UNIV., Oct. 2018 at 4, https://web.stanford.edu/~gentzkow/research/fake-news-trends.pdf?mod=article_inline [hereinafter "Trends Report"] (measuring the trends in false content, fake news websites, and fake news stories on Facebook and Twitter); Brennen, *supra* note 47, at 1 (describing his study that found "most (59%) of the misinformation in our sample involves various forms of reconfiguration, where existing and often true information is spun, twisted, recontextualized, or reworked.").

[51] Mass Distraction, *supra* note 27, at 4.

[52] *See* Robert MacKey, *Anatomy of a Lie: How the Trump Campaign Edited Video of Biden to Create a Fake Gaffe*, THE INTERCEPT (Oct. 28, 2020), https://theintercept.com/2020/10/28/anatomy-lie-trump-campaign-edited-video-biden-create-fake-gaffe/ (describing how viral videos of then-candidate Vice President Joe Biden were edited to mislead viewers).

[53] *Id.*

[54] *Id.*; *See infra*, Figure 2.

[55] *See generally* Rand Report, *supra* note 2, at 8.

Advertisements[56]	**Imposter Content**	**Fabricated Content**	**False Connection**
Paid content containing false information or imagery.	Genuine sources are impersonated.	Content is 100% false.	Visuals or captions do not support the content.
False Context	**Manipulated Content**[57]	**Memes and Symbols**[58]	**False Personas**[59]
Genuine content is shared with false contextual information.	Genuine information or imagery is manipulated.	Slogans or statements coupled with images, or videos that convey a message.	The creation of false personas or account using real (stolen) or fake identities.

Figure 2: Common Disinformation Products.[60]

Distribution is the third stage of the supply chain. Disinformers have various distribution networks,[61] and individuals may consume the disinformation via traditional channels of communication (e.g., newspapers, cable news, etc.) or digital ones (e.g., mobile news applications, social media, etc.).[62] Often, disinformers disseminate the disinformation via one channel of communication before it spreads to other channels.[63] The kind of spread often takes the form of misinformation, i.e. the inadvertent sharing or resharing of false information.[64] There are four pathways by which misinformation can spread. [65] I plot these pathways on an *x-y plane* wherein each quadrant of the graph represents one of the pathways (*see* Figure 3). The *x-axis* represents the extent to which traditional media is used to disseminate the misinformation. The *y-axis* plots the extent to which

---

[56] *See, e.g.*, Amber Herrle, *Regulating Fact from Fiction: Disinformation in Political Advertising*, BROOKINGS INST. (Dec. 20, 2019), https://www.brookings.edu/blog/fixgov/2019/12/20/regulating-fact-from-fiction-disinformation-in-political-advertising/.

[57] *See, e.g.*, Hannah Denham, *Another Fake Video of Pelosi Goes Viral on Facebook*, WASH. POST (Aug. 3, 2020), https://www.washingtonpost.com/technology/2020/08/03/nancy-pelosi-fake-video-facebook/.

[58] *See* Joan Donovan, *How Memes Got Weaponized: A Short History*, MIT TECH. R. (Oct. 24, 2019), https://www.technologyreview.com/2019/10/24/132228/political-war-memes-disinformation/ (describing how memes are a serious threat in spreading misinformation).

[59] *See, e.g.*, Mueller Report, *supra* note 15, at 14-15 (describing the use of IRA-controlled Twitter accounts).

[60] *See* Claire Wardle, *Information Disorder, Part 3: Useful Graphics*, FIRST DRAFT (July 9, 2020), https://medium.com/1st-draft/information-disorder-part-3-useful-graphics-2446c7dbb485.

[61] *See generally* GEC Report, *supra* note 49, at 8.

[62] *See generally* Benkler, et al., *supra* note 5, at 1-3.

[63] *See generally id.*

[64] Harsin, *supra* note 3, at 8.

[65] *See generally* Benkler, *supra* note 5, at 3 (proposing three competing conceptions of how public opinion is shaped) (For this Article, I use the term "traditional media" in place of Benkler's "mass media" terminology, and I add a fourth conception).

digital media is used to spread misinformation. Thus, the four pathways describe both the channel of distribution by the disinformer and the channel of consumption by the consumer.

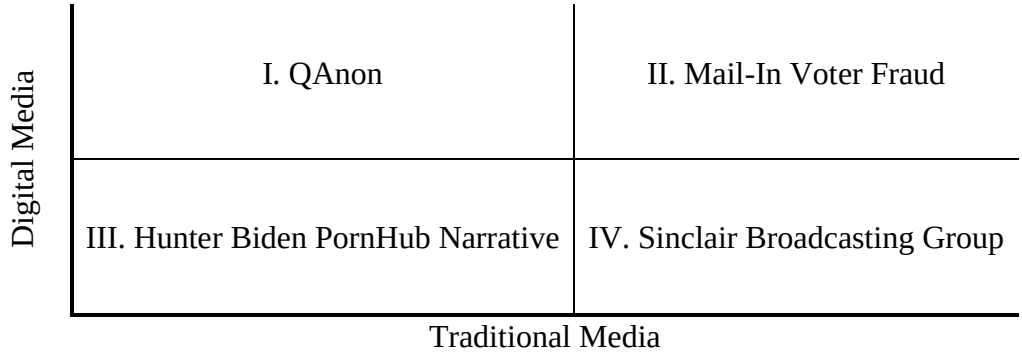

Figure 3: Four Pathways to Spreading Disinformation.[66]

Quadrant I reflects misinformation that spreads widely and deeply on social media with some traditional media spread. An example is the QAnon conspiracy theory, which alleges the world is run by a cabal of Satan-worshiping pedophiles who operate a global child sex-trafficking ring.[67] While the traditional media discussed QAnon in the weeks leading up to and following the 2020 U.S. presidential election, the QAnon conspiracy theory began on fringe online message boards as early as 2016 before spreading to mainstream social media.[68] Facebook and Twitter then saw QAnon discussions develop on their platforms as early as 2018—two years before traditional media reported on QAnon.[69]

Quadrant II reflects misinformation that spreads equally through both digital and traditional media. Mail-in voter fraud conspiracies are an example. Ahead of the 2020 U.S. presidential election, President Trump, the Republican National Committee, and conservative websites claimed that mail-in ballots would lead to voter fraud resulting in a "rigged election."[70] These same actors continued to bolster

[66] *See* Benkler, *supra* note 5, at 3.

[67] Kevin Roose, *What Is QAnon, the Viral Pro-Trump Conspiracy Theory?*, N.Y. TIMES (Oct. 19, 2020), https://www.nytimes.com/article/what-is-qanon.html.

[68] *Id.*; *see* Adrienne LaFrance, *The Prophecies of Q*, THE ATLANTIC (June 2020), https://www.theatlantic.com/magazine/archive/2020/06/qanon-nothing-can-stop-what-is-coming/610567/ (stating that QAnon was born out of the 2016 Pizzagate conspiracy theory which claimed Hillary Clinton was running a child sex ring out of Comet Ping Pong in Washington, D.C.).

[69] Craig Timberg & Elizabeth Dwoskin, *As QAnon Grew, Facebook and Twitter Missed Years of Warning Signs About the Conspiracy Theory's Violent Nature*, WASH. POST (Oct. 3, 2020), https://www.washingtonpost.com/technology/2020/10/01/facebook-qanon-conspiracies-trump/.

[70] Tiffany Hsu, *Conservative News Sites Fuel Voter Fraud Misinformation*, N.Y. TIMES (Oct. 25, 2020), https://www.nytimes.com/2020/10/25/business/media/voter-fraud-misinformation.html.

such claims post-election.[71] These false claims were shared broadly on social media and covered extensively by the traditional media.[72]

Quadrant III represents misinformation that circulates via digital media and traditional media, but does not spread widely, if at all. Quadrant III misinformation often remains in the "fringe" sections of online forums, blogs, etc. One example is the Hunter Biden "PornHub" narrative constructed by *Gateway Pundit*.[73] Before discussing the narrative itself, I advise the reader that *Gateway Pundit* is not a credible source of information.[74] Its content has consistently been debunked, and Newsguard, a journalism trust rating organization, gave *Gateway Pundit* a failing score of 20/100 for trustworthiness.[75]

Gateway Pundit claimed that it discovered Hunter Biden's personal account on PornHub.com, which allegedly contains videos showing Hunter Biden engaged in "depraved activities" with "seedy people in seedy places."[76] The publisher argued that this discovery was proof of the clear cover-ups by the Biden family to hide depraved behavior, but as of March 15, 2021, none of *Gateway Pundit*'s allegations have been substantiated.[77] This false narrative falls into Quadrant III because the allegations have not spread widely via digital or traditional media channels.

Quadrant IV represents misinformation that circulates widely via traditional media, but digital media acts only as an auxiliary pathway. Sinclair Broadcast Group ("Sinclair"), the owner of 193 local television affiliates, provides an example

---

[71] *See, e.g.*, Christina Cassidy & Mary Clare Jalonick, *Senate Hearing Elevates Baseless Claims of Election Fraud*, ASSOCIATED PRESS (Dec. 16, 2020), https://apnews.com/article/election-2020-joe-biden-donald-trump-senate-elections-elections-c827ef1b2d0415383dff4aa881d7d3fe (recapping a Senate Homeland Security and Governmental Affairs Committee hearing where Republican senators continued to perpetuate false claims of voter fraud).

[72] *See* Benkler, *supra* note 5, at 6-13 (quantifying and comparing the spread of mail-in voter fraud disinformation via social and mass media).

[73] *See* Joe Hoft, *Huge Breaking Exclusive: Hunter Biden Has a PornHub Account Where He Uploaded His Personal Porn – Including with Family Member*, GATEWAY PUNDIT (Oct. 29, 2020), https://www.thegatewaypundit.com/2020/10/huge-breaking-exclusive-hunter-biden-pornhub-account-uploaded-personal-porn-including-family-members/; Hunter Biden is the son of Joe Biden.

[74] *See* Paul Farhi, *What is Gateway Pundit, the Conspiracy-Hawking Site at the Center of the Bogue Florida 'Crisis Actors' Hype?*, WASH. POST. (Feb. 23, 2020), https://www.washingtonpost.com/lifestyle/style/what-is-gateway-pundit-the-conspiracy-hawking-site-at-the-center-of-the-bogus-florida-crisis-actors-hype/2018/02/23/dded562a-174e-11e8-b681-2d4d462a1921_story.html (describing how *Gateway Pundit* circulated the conspiracy theory that the survivors of the mass shooting at Marjory Stoneman Douglas High School were crisis actors and not real victims).

[75] *See id.*; Anna-Sophie Harling, *thegatewaypundit.com*, NEWSGUARD TECH. INC. (2020), https://www.newsguardtech.com/wp-content/uploads/2020/02/The-Gateway-Pundit-NewsGuard-Nutrition-Label.pdf (NewsGuard provides trust ratings for 6,000+ news websites that account for 95% of online engagement with news. Co-CEO Steven Brill founded the Yale Journalism Initiative and Court TV. Co-CEO Gordon Crovitz was the publisher of *The Wall Street Journal*. Its investors include the John S. & James L. Knight Foundation and former Secretary of Homeland Security, Tom Ridge, among others. For a full list of its advisors and investors, *see* https://www.newsguardtech.com).

[76] Hoft, *supra* note 73.

[77] *See id.*

of such disinformation.[78] Sinclair was criticized for requiring its local news anchors to express specific narratives on-air that were designed to strengthen Sinclair's position on various issues."[79] For instance, in 2008, Sinclair ran an ad attempting to tie then-Senator Barack Obama to Weather Underground terrorist Bill Ayers; the ad declared that Obama was "friends with Ayers" and his political career began in Ayers home.[80] This false narrative, among many others propagated by Sinclair, began on traditional media (e.g., local television stations). In this quadrant, the false narrative may spread via digital media, but the misinformation *originates* from and *primarily spreads* through traditional media.

C. The Research of Disinformation

By illustrating the creation of disinformation as a supply chain and conceptualizing how false information spreads via traditional and digital media, one can better understand the different ways that disinformation spreads. Studies suggest, for example, that disinformation spreads faster and wider than the truth.[81] This Section briefly examines some recent studies that demonstrated this phenomenon.

Some studies show how disinformation spreads more quickly than the truth. As a postdoctoral associate at MIT Media Lab, Soroush Vosoughi investigated the spread of false information.[82] This research suggested that false information spreads more quickly than the truth—approximately six times faster.[83] In the study, true information on Twitter took about six times longer to reach 1,500 accounts than false information did.[84]

---

[78] *See generally* Dominic Rushe, *Trump Defends Rightwing TV Network Sinclair after 'Fake News' Script Goes Viral*, GUARDIAN (Apr. 2, 2018), https://www.theguardian.com/media/2018/apr/02/sinclair-trump-video-script-fake-news-president-defends-tv-news-twitter (describing how Sinclair Broadcast Group required its anchors to read an identical script criticizing fake news).

[79] *Id.*

[80] Dylan Matthews, *Sinclair, the Pro-Trump, Conservative Company Taking over Local News, Explained*, VOX (Apr. 3, 2018), https://www.vox.com/2018/4/3/17180020/sinclair-broadcast-group-conservative-trump-david-smith-local-news-tv-affiliate.

[81] *See generally* Vosoughi, *supra* note 17, at 2 (showing the quantity of disinformation on Twitter and how quickly and deeply disinformation spreads on the platform).

[82] *Id.* at 1 (the study considered approximately 126,000 stories tweeted by approximately three million people more than four and a half million times. Vosoughi classified the news as true or false using information from six independent fact-checking organizations that exhibited a 95-98% agreement on the classifications); *see generally* Michela Del Vicario, et al., *The Spreading of Misinformation Online*, 113 PROC. OF THE NAT'L ACAD. OF SCI. 554 (Dec. 4, 2015), https://www.pnas.org/content/113/3/554 (detailing their quantitative study that suggested similar results to the Vosoughi Study) (for this Article, I reference the Vosoughi Study, but I note that Del Vicario's study suggests similar results and conclusions).

[83] *See* Benkler, *supra* note 5, at 3.

[84] *Id.* at Figure 2F.

Furthermore, disinformation appears to spread wider than true information.[85] A study comparing fake and true news on Facebook during the 2016 U.S. presidential election found that the top fake stories drew more user engagement than true news stories by a margin of 7.3-8.7 million, measured by the number of shares, reactions, and comments on the stories.[86] This trend continued into the 2020 U.S. presidential election, during which President Trump's false attacks on mail-in voting generated approximately 3.8 million interactions on Facebook.[87] *Breitbart*, a conservative website that has been repeatedly criticized for reporting false or misleading narratives, had more engagement on its voting-related stories than *any other publisher* from April through July 1, 2020.[88]

Research also suggests that disinformation frequently reaches users that other content does not.[89] Here, the disinformation distribution contributes to the breadth of the consumption. The Vosoughi study suggested that the users who spread false information had significantly fewer followers, followed significantly fewer people, were significantly less active on Twitter, verified significantly less often, and had been on Twitter for significantly less time.[90] Therefore, in order for disinformation to reach more users, the false information is shared more often to reach the widespread target audience compared to true information.[91]

There are several high-profile examples of disinformation capturing high user engagement rates. One false story, originated by Sean Hannity of Fox News, claimed that Donald Trump sent his personal plane to transport 200 stranded marines in 1991.[92] This story collected 893,000 user impressions.[93] Another story wrongly claimed that Pope Francis endorsed Donald Trump in the 2016 U.S.

---

[85] *See id.* at 6 (showing the difference between true and false information spread); *see also* Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, WALL ST. J. (May 26, 2020), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499 (discussing an internal Facebook study that found Facebook's "algorithms exploit the human brain's attraction to divisiveness").

[86] W. Lance Bennett & Steven Livingston, *The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions*, 33 EUR. J. OF COMMC'N 122, 133 (Apr. 2018), https://www.doi.org/10.1177/0267323118760317 [hereinafter "Disinformation Order"].

[87] McCarthy, *supra* note 20.

[88] *Id.* (noting that *Breitbart* garnered more interactions since April 2020 on voting-related stories than equivalent articles by *The Washington Post*, *The New York Times*, and *NBC News* combined); *see, e.g.*, Charlie Spiering, *Donald Trump Lays Out Evidence of Mail-In Voting Fraud to Reporters*, BREITBART (Sept. 27, 2020), https://www.breitbart.com/2020-election/2020/09/27/donald-trump-evidence-mailin-voting-fraud-reporters/ (claiming numerous voter fraud incidents leading up to the 2020 U.S. presidential election, as noted by then-President Donald Trump).

[89] *See* Vosoughi, *supra* note 17, at 6.

[90] *Id.*

[91] *Id.* at 4.

[92] *Id.*

[93] *Id.*; Hannah Ritchie, *Read All About It: The Biggest Fake News Stories of 2016*, CNBC (Dec. 30, 2016), https://www.cnbc.com/2016/12/30/read-all-about-it-the-biggest-fake-news-stories-of-2016.html.

presidential election and picked up 960,000 user impressions on Facebook.[94] The story originated from a site called WTOE 5 News and then cascaded when it was amplified by a fake news publisher called *Ending the Fed*.[95]

In addition, the Vosoughi study suggested the quantity of disinformation has increased since 2006 and generally spikes around major news events.[96] By counting the number of false tweets since 2006, the study noted clear spikes in the number of false tweets around major news events like the Boston Marathon bombing in 2013, the annexation of Crimea in 2014, and the 2016 U.S. presidential election.[97]

With the rise in production of disinformation and its spread, this prompts a new question that is not often explored by researchers and scholars: what *enables* the disinformation campaigns to spread false or misleading information more effectively than true information? The next Part explores the enablers of disinformation.

III. THE ENABLERS

The rise of social media amplifies the negative consequences of misinformation; but for these recent technology advancements, the ability to persuade a large mass of people with disinformation campaigns in order to achieve political goals would not be possible. This Part argues that social media platforms enable misinformation to spread much more effectively because they 1) are widespread, 2) are addictive, and 3) personalize content, leading to echo chambers and rapid misinformation spread. Finally, it argues that this is only possible because of the weak data privacy regime in the United States.

A. Social Media Platforms Are Widespread and Addictive

Social media's broad reach explains why these platforms enable the spread of disinformation. While studies vary, on average about two-thirds of American adults say that they get news from social media.[98] Facebook has approximately 2.7 billion monthly active users.[99] Twitter reports that it has 187 million "monetizable" daily active users.[100] This data shows that social media reaches billions of people every

---

[94] *Id.*

[95] *Id.*

[96] *See* Janna Anderson & Lee Rainie, *The Future of Truth and Misinformation Online*, PEW RSCH. CTR. 66 (Oct. 19, 2017) (quoting a North American researcher, "the amount of mis/disinformation will continue to increase."); Vosoughi, *supra* note 17, at Figure 1, C and E (graphing the amount of false news online by year).

[97] *See* Vosoughi, *supra* note 17, at 2.

[98] Elisa Shearer & Katerina Eva Matsa, *News Use Across Social Media Platforms 2018*, PEW RSCH. CTR. 4 (Sept. 10, 2018), https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/ (a total of 4,581 individuals responded between July 30-August 12, 2018. The margin of sampling error for the 4,581 respondents is ± 2.5%. For the survey's methodology, *see* Shearer & Matsa at 11-12).

[99] *See* FACEBOOK, INC., FORM 10-Q: QUARTERLY REPORT (July 31, 2020).

[100] *See* TWITTER, INC, FORM 10-Q: QUARTERLY REPORT (Oct. 30, 2020).

day, and similarly, it suggests that social media platforms are successful at maintaining user engagement. Further, many social media platforms have features, like "single sign-on" capabilities, that allow other developers to build on top of the platform. These technologies make social media more "sticky" in that users are less likely to delete their accounts because of the widespread integrations.[101]

In addition to the broad reach, social media is addictive and stimulates humans in a subconscious and hormonal way.[102] For instance, social media use can trigger a release of oxytocin—the human stimulant of empathy, generosity, and trust.[103] Users may experience symptoms similar to other addictions, including withdrawal, relapse, and mood modification.[104]

Some researchers argue that social media's features can be a form of operant conditioning.[105] Users associate behaviors with consequences; when an action is followed by a pleasant consequence, it is likely to be repeated.[106] So, when a user posts a picture and receives a "Like", they are likely to repeat this engagement because the user's action receives positive reinforcement. More specifically, the positive reinforcement is a dopamine hit—meant to "hook" the user to the platform.[107]

Indeed, social media platforms have designed their products and features to reinforce engagement by "hooking" the user.[108] Recognizing that engagement increases when users have an emotional response to the content, social media has developed methods to detect their users' emotions.[109] Further, emotional detection may inform what content the user sees.[110]

Thus, two contributing factors to why social media helps disinformation spread so effectively are its breadth and addictive nature. This means that unlike other

---

[101] *See, e.g.*, Jessica Dolcourt, *Facebook Introduces Single Sign-On for Mobile Apps, Services*, CNET (Nov. 3, 2010), https://www.cnet.com/news/facebook-introduces-single-sign-on-for-mobile-apps-services/ (describing Facebook's launch of the single sign-on feature); Jason Aten, *Google Suffered a Major Outage. It Turns Out This Simple Step Could Have Prevented It*, INC. (Dec. 14, 2020), https://www.inc.com/jason-aten/google-suffered-a-major-outage-it-turns-out-this-simple-step-could-have-prevented-it.html (describing the thirty minutes on December 14, 2020, where Google's services were down or inaccessible, including its SSO feature that crippled any third-party website that utilized Google's SSO).

[102] Ronald J. Deibert, *The Road to Digital Unfreedom: Three Painful Truths about Social Media*, 30 J. OF DEMOCRACY 25, 29 (Jan. 2019).

[103] Adam L. Penenberg, *Social Networking Affects Brains like Falling in Love*, FAST CO. (July 1, 2010), https://www.fastcompany.com/1659062/social-networking-affects-brains-falling-love.

[104] Deibert, *supra* note 102, at 29.

[105] *Id.*

[106] Saul McLeod, *Skinner – Operant Conditioning*, SIMPLY PSYCH. (2018), https://www.simplypsychology.org/operant-conditioning.html.

[107] Deibert, *supra* note 102, at 30.

[108] Deibert, *supra* note 102, at 30.

[109] *See generally* Damian Clifford, *Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?* KU LEUVEN CTR. FOR IT & IP LAW, Sept. 15, 2017, at 5-6 (discussing the "emotional capabilities" of big technology players).

[110] *See generally* Clifford, *supra* note 109, at 6.

traditional media platforms, disinformation can spread more to a much broader social graph, and users may feel emotional or hormonal responses to the content they see.

B. Social Media Platforms Profile Users and Personalize Content

This Section discusses how social media platforms profile their users. It first discusses how the platforms construct personal profiles, before detailing how they use them. Social media platforms create personal profiles of their users, and then use those profiles to present personalized content to those users.[111] For example, a Twitter user's timeline used to show tweets in reverse-chronological order (from most recent to the oldest).[112] But since 2017, Twitter has used machine learning (i.e., artificial intelligence) to determine what content appears on each user's timeline on an individualized.[113]

Though Twitter and other social media platforms do not use the terms "personal profiles" or "personal profiling," the technologies that power social media platforms do exactly that.[114] First, Twitter and other social media platforms collect, procure, and generate data about each user.[115] This data includes how the users interact with the platform, such as their clicks, shares, retweets, views, scrolling patterns, reading rates, and more.[116] With this user data, the platforms construct personal profiles about each user.[117] Such profiles can reveal a user's habits, social relationships, tastes, political preferences, thoughts, opinions, and more.[118]

Once personal profiles are created, the platforms leverage a user's personal profile to automatically curate, and even generate, content.[119] The curated or autogenerated content is then presented to the user.[120] The content personalization

---

[111] *See, e.g.*, Nicolas Koumchatzky & Anton Andryeyev, *Using Deep Learning at Scale in Twitter's Timelines*, TWITTER (May 9, 2017), https://blog.twitter.com/engineering/en_us/topics/insights/2017/using-deep-learning-at-scale-in-twitters-timelines.html (discussing how Twitter uses deep learning to surface content that is relevant to the individual user) (hereinafter "Twitter Blog Post").

[112] *Id.*

[113] *Id.*

[114] *See generally id.*

[115] *See* Wayne Unger, *Katz and COVID: How a Pandemic Changed the Reasonable Expectation of Privacy*, 12 HASTINGS SCI. & TECH. L.J. 40, 47 (2020) (describing three types of data: user-generated, queried, and autogenerated data) [hereinafter "*Katz* and COVID"].

[116] *See* Lauren Jones, *Social Media Algorithms and How They Work*, HEARST BAY AREA (June 29, 2020), https://marketing.sfgate.com/blog/social-media-algorithms (describing how social media platforms curate and push content to its users).

[117] *Id.*

[118] Deibert, *supra* note 102, at 27 (describing the "surveillance capitalism" of social media and its data collection processes).

[119] *See* M.Z. van Drunen, et al., *Know Your Algorithm: What Media Organizations Need to Explain to their Users about News Personalization*, 9 INT'L DATA PRIVACY L. 220, 231 (explaining how algorithms personalize news content).

[120] *Id.*

enables each user to see different content—tailored to his, her, or their interests—and sometimes even different versions of the same story.[121]

Attracting and keeping users' attention is critical to the social media's business models.[122] For instance, investors gauge Facebook's performance by evaluating its user engagement metrics, such as its daily and monthly active users.[123] Facebook monetizes user engagement via advertising, and its advertising business generates approximately 98.5% of its annual revenues.[124] And content curation or personalization *promotes* user engagement on social media platforms.[125] To maintain or increase user engagement, social media platforms leverage the personal profiles by applying algorithms to identify and present content that is interesting or engaging to the user.[126]

How does using personal profiles to curate content help spread disinformation? When users see content tailored to their interests, they are much more likely to fall into a rabbit hole of disinformation. This may become a negatively-reinforcing cycle because as users interact with disinformation, they become more likely to see further disinformation.[127] This contributes to the "echo chamber" effect—where information is more likely believed opposing viewpoints are presented less frequently.[128]

This phenomenon is even more concerning when one considers the research on how humans utilize their analytical judgment. Under a psychological theory known as the "dual process theory," humans have two systems of thinking: (1) they process ideas automatically using little effort, and (2) they process ideas using analytical processing that requires significant effort.[129] Humans tend to default to the former system (often called "System 1") because they are "cognitive misers."[130] In other words, humans tend to solve problems in simple and straight-forward ways rather than use more effort-intensive ways (i.e., critically analyze an issue).[131] Therefore, it is much easier to believe disinformation when it is presented repeatedly than it is

---

[121] *Id.* at 232.

[122] *See id.*; *see also* Deibert, *supra* note 102, at 33.

[123] *See generally* Facebook, Inc., Annual Report (Form 10-K) (Jan. 30, 2020) (stating that Facebook's total revenue was $70.70 billion, of which $69.66 billion came from its advertising business) [hereinafter "Facebook 10-K"].

[124] *See id.* at 45-46.

[125] *Id.* at 33.

[126] *See generally* Kai Shu & Huan Liu, DETECTING FAKE NEWS ON SOCIAL MEDIA 1-3 (Jiawei Han et al. eds., 2019) (discussing algorithmic design of social media platforms) (hereinafter "Detecting Fake News").

[127] Deibert, *supra* note 102, at 29.

[128] *Id.*

[129] Tommy Shane, *The Psychology of Misinformation: Why We're Vulnerable*, FIRST DRAFT NEWS (June 30, 2020), https://firstdraftnews.org/latest/the-psychology-of-misinformation-why-were-vulnerable.

[130] *Id.*; *see Cognitive Miser*, AM. PSYCH. ASS'N DICTIONARY, https://dictionary.apa.org/cognitive-miser.

[131] *Id.*

to critically question its validity. In addition, humans are more susceptible to disinformation because of the tendency to default to System 1.

Second, humans are susceptible to confirmation bias. This is the tendency to believe information that confirms your existing beliefs and to reject contradictory information.[132] So, when a user sees the same curated disinformation repeatedly, in the user's mind, it confirms that the disinformation is true—in this way using personal profiling to curate content can actually help make disinformation more believable.

Both dual process theory and confirmation bias lead to lazy thinking, where information is not challenged critically, analytically, or logically. This type of lazy thinking is a key factor in users' vulnerability to misinformation.[133] While some scholars and policymakers argue users have or should have the analytical judgment to decipher truth from fiction,[134] the January 6, 2021, attack on the U.S. Capitol by Trump supporters, who legitimately believed his election fraud claims, suggests otherwise.[135]

President Trump's tweets are a great example here. Prior to the suspension of President Trump's account, his posts and shares contained misinformation, and these tweets would go viral—reaching millions of people around the world.[136] With Twitter's algorithmic design that prioritizes tweets by relevance and popularity, President Trump's tweets spread rapidly because of the aforementioned technical and human factors.[137] As the Brookings Institute highlighted, "Since [humans are] more likely to react to content that taps into our existing grievances and beliefs, inflammatory tweets will generate quick engagement."[138] As user engagement increases, so does its popularity and relevance to specific users—this is where the algorithmic design amplifies the message's spread.[139] Further, this cyclical pattern contributes to societal polarization because the curation taps into existing

---

[132] Shane, *supra* note 129.

[133] *Id.* (quoting David Rand and Gordon Pennycook, two cognitive scientists at the University of Virginia and MIT, respectively).

[134] *See, e.g.*, Kelcee Griffis, *Sens. Struggle to Nail Down Central Section 230 Issues*, LAW 360 (Nov. 17, 2020), https://www.law360.com/articles/1329278 (quoting Senator John Kennedy, R-LA, who pressed why social media platforms make overreaching content-moderation decisions when it could instead opt to "*trust its users' own judgment*.") (emphasis added).

[135] *See generally*, Zack Stanton, *The Problem Isn't Just One Insurrection. It's Mass Radicalization*, POLITICO (Feb. 11, 2021), https://www.politico.com/news/magazine/2021/02/11/mass-radicalization-trump-insurrection-468746.

[136] Chris Meserole, *How Misinformation Spreads on Social Media—And What to Do About It*, BROOKINGS INST. (May 9, 2018), https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it/.

[137] *Id.*

[138] *Id.*

[139] *See id.*

grievances and beliefs—bringing together people with broadly similar opinions and rejecting opponents.[140]

Here, social psychology helps explain how platforms influence society as a whole. The law of group polarization explains how extremism, radicalization, cultural shifts, and the like occur and how they are fueled by social media.[141] Group polarization happens when people who have a broadly similar opinion regarding a topic come together, but some have more extreme views than others.[142] Oftentimes, group decisions trend towards the more extreme view or perspective, and the group members who originally had a less extreme view become more radicalized.[143] While historically, it took significant time to radicalize the masses, social media platforms have shortened the timespan because more extreme views are shared more quickly, widely, and broadly.[144]

To conclude, social media platforms enable disinformation to spread very effectively. They do so because of their size, stickiness, and addictive nature. And most prominently, they do so by using personal data to profile users and curate the content each user sees. Such content curation leads to users who interact with some disinformation seeing much more, which helps confirm in their minds that this disinformation is true. This is done automatically at an unprecedented scale using the algorithms that power social media's key features.

C. This Is Only Possible Due to a Weak Data Privacy Regime

As argued by the previous Section, social media platforms' ability to use personal data for content curation leads to an environment in which disinformation can spread very effectively. This Section argues that this is permitted by the weak data privacy regime in the United States. Indeed, the lack of limits on these platforms' abilities to use personal data is a root cause of the disinformation-friendly environment they create.

The present data privacy and security regime in the U.S. is a patchwork of federal and state laws, rules, and regulations.[145] Data privacy and security protections are found in federal constitutional law, state constitutional law, and sector-specific legislation.[146] The U.S. Constitution, for example, provides certain

---

[140] Charles Arthur, *Social Media Polarises and Radicalises – and MPs Aren't Immune to its Effects*, GUARDIAN (Mar. 11, 2019), https://www.theguardian.com/commentisfree/2019/mar/11/whatsapp-facebook-extreme-polarise-radicalise-mps-politicians.

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] *See* Stanton, *supra* note 135 (quoting Michael Jensen, a researcher at the National Consortium for the Study of Terrorism and Responses to Terrorism).

[145] *See* Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH. 1, 4-5, no. 1 (2020) (while no comprehensive federal protections exist, a few states have enacted comprehensive data privacy and security protections, such as California with the California Consumer Privacy Act) [hereinafter "PROA"].

[146] *See Katz* and COVID, *supra* note 115, at 59-60 (while the inherent right to privacy is found in multiple amendments to the U.S. Constitution, I focus on the Fourth Amendment for this Article).

privacy rights, but only against state actors.[147] Certain federal statutes, such as the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA") protect consumer privacy, but only within specific industries.[148] At the state level, the California Consumer Privacy Act ("CCPA") is generally considered the most comprehensive data privacy and security state statute in the U.S.[149]

A common thread amongst the constitutional, statutory, and regulatory privacy and security protections is the *reasonable expectations of privacy* standard—whether an individual has an objectively reasonable expectation of privacy with respect to the data at issue.[150] While the reasonable expectation of privacy standard stems from federal constitutional law, this standard is generally considered a foundational inquiry to any assessment of privacy protections.[151] With constitutional protections, the reasonable expectation of privacy standard is found throughout Fourth Amendment jurisprudence.[152] With statutory protections, the rights and protections are often, if not always, *based* on this standard.[153] For example, one has a reasonable expectation of privacy with respect to one's personal health information, and accordingly, Congress enacted HIPAA to protect the privacy and security of this information.[154] Statutory protections also *promote* the reasonable expectation of privacy—individuals expect their personal health information to be protected because HIPAA exists today.[155]

The 116th Congress proposed several comprehensive data privacy and security bills that were inspired by the reasonable expectation of privacy—what information do individuals expect some level of privacy and how should it be protected? While the 116th Congress proposed these bills, none were enacted.[156] Additionally, the social media industry's attempts at self-regulation have failed, as the industry's business model precludes effective regulation.[157] Absent effective and comprehensive self-regulation, statutory protections, or constitutional protections,

---

[147] For example, *Carpenter v. United States* upheld the warrant requirement for cell-site location data. 138 S. Ct. 2206 (2018) (recognizing that when the Government tracks the geolocation data of one's cell phone, the Government surveils the user).

[148] *See* STEPHEN P. MULLIGAN ET AL., CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 1-23 (2019) (providing an overview of statutory data privacy and security protections; HIPAA applies to the healthcare industry, and GLBA applies to the financial services industry).

[149] *See id.*

[150] *Katz* and COVID, *supra* note 115, at 60.

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] PROA, *supra* note 145, at 17.

platforms can and will continue to aggressively collect, use, store, and disseminate all types of personal information at scale.[158]

There are three types of digital personal information: user-inputted, queried, and autogenerated data (*see* Figure 4).[159] User-inputted data is information that the user provides to the data collector (e.g., entering one's date of birth on Facebook).[160] Queried data is procured from a data supplier (i.e., purchasing credit reporting data), and autogenerated data is created and collected via automation (e.g., behavioral analytics).[161]

	Description	**Source of Data**	**Example(s)**
User-Inputted Data	The data that a user provides the data collector.	User	Name, Address, Phone Number, Zip Code
Queried Data	The data that a data collector sources.	Internal Systems or Third Parties	Credit Report and Score
Autogenerated Data	The data that is created and collected via automation.	Internal Systems or Third Parties	Behavioral Analytics, User Interactions

Figure 4: Data Categories Chart.[162]

The current data privacy and security regime is weak because (i) the current patchwork of protections is not comprehensive and all-encompassing, and (ii) it is only beginning to recognize these three data types. I discuss these in turn.

Unlike the patchwork data privacy and security regime in the U.S., the European Union has the Global Data Protection Regulation ("GDPR") that provides broad data privacy and security protections. GDPR contains provisions that effectively limit the ability to micro-target on social media platforms.[163] For instance, GDPR substantially limits the collection of personal information from any device in Europe.[164] Further, social media platforms can be held jointly liable for

---

[158] *See generally Katz* and COVID, *supra* note 115.

[159] *Id.* at 47.

[160] *Id.*

[161] *Id.*

[162] *Id.* at 48.

[163] *See* Karen Kornbluh, *Could Europe's New Data Protection Regulation Curb Online Disinformation?*, COUNCIL ON FOREIGN RELATIONS (Feb. 18, 2018), https://www.cfr.org/blog/could-europes-new-data-protection-regulation-curb-online-disinformation.

[164] *Id.*

third parties on whose behalf they furnish data if those third parties do not comply with GDPR's requirements.[165]

Generally, one of GDPR's main objectives is to limit the misuse of personal information.[166] This includes the use of personal information to profile users—thus, limiting the ability to curate the personalized content to the specific user. By limiting access to the personal information that enables the personalized and targeted content, which perpetuate polarizing echo chambers, comprehensive and robust data privacy laws can "render disinformation a weapon without a target."[167]

Furthermore, the legal system in the U.S. is only beginning to recognize the three data types. Each data type carries a different set of privacy expectations. The present regime is weak because it barely recognizes how each type of data can and should be protected.

Take, for example, the third-party doctrine; while the third-party doctrine only applies to government actors under the Fourth Amendment, the doctrine generally provides that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.[168] By definition, information that an individual *voluntarily* turns over to third parties is user-inputted data.

However, Supreme Court recognized that even though a third party holds cell-site location information ("CSLI"), "the unique nature of cell phone location records" places the data within the Fourth Amendment's protection.[169] The Court reached this conclusion because CSLI is highly personal, voluminous in nature, and inexpensive for the state to obtain, the third-party doctrine should not extend to all cases where a third party holds information on the data subject.[170] It is important to point out that CSLI is not user-inputted data, but rather autogenerated data, because, like in *Carpenter*, the user does not affirmatively act to submit the data to the third party.

Before continuing, I note two important observations regarding *Carpenter*. First, even though the Court considered the third-party doctrine, it should have been irrelevant in scenarios like *Carpenter*, where the data at issue is autogenerated, because definitionally, the doctrine should only apply to user-inputted data. Second, *Carpenter* demonstrated that the Court is beginning to recognize the three data types because it afforded autogenerated data greater privacy protection than user-inputted data. While the Court did not use the terms "user-inputted" or "autogenerated" data nor did it distinguish data types in its reasoning, the Court

---

[165] *Id.*

[166] Annina Claesson, *Coming Together to Fight Fake News: Lessons from the European Approach to Disinformation*, CTR. FOR STRATEGIC & INT'L STUDIES (Apr. 9, 2019), https://www.csis.org/coming-together-fight-fake-news-lessons-european-approach-disinformation.

[167] Alex Campbell, *How Data Privacy Laws Can Fight Fake News*, JUST SEC. (Aug. 15, 2019), https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/.

[168] United States v. Miller, 425 U.S. 435, 442 (1976) (holding that bank clients have no legitimate expectation of privacy in banking information revealed to a third party).

[169] Carpenter, 138 S. Ct. at 2217.

[170] *See Katz* and COVID, *supra* note 115, at 65.

effectively and properly recognized that privacy expectations differ. And in essence, assigning a higher level of protection to autogenerated data versus user-inputted data provides for a more robust data privacy regime.

Consider this, if the same CSLI at issue in *Carpenter* was user-inputted, not autogenerated, then the third-party doctrine would easily apply. Thus, the distinction between data types is important in determining the appropriate level of privacy protection.

Turning back to personal profiling and the platforms' algorithms, both require substantial amounts of PI from all three data types. However, personal profiling relies heavily on autogenerated data, which should receive the greatest protection under a more robust data privacy regime.

Notwithstanding the fact that no comprehensive data privacy and security protections exist today, a regime that is only beginning to recognize the three distinct data types falls short in providing truly effective privacy protections. Because the current data privacy and security regime is weak for the foregoing reasons, social media platforms can continue to collect and use the substantial amount of PI from all three data types with little to no limitations. Thus far, this Article has worked to familiarize the reader with the definition and structure of disinformation campaigns. This foundation will help facilitate an understanding of how disinformation campaigns exploit platforms' personal profiling and algorithms.

IV. CASE STUDY: HOW THE WEAK REGIME HELPED ENABLE THE 2020 ELECTION DISINFORMATION AND HARMED AMERICAN DEMOCRACY

The previous Part explored why disinformation spreads so effectively and how social media platforms enable this by curating content using personal information. It also argued that the weak data privacy and security regime is a root cause. By using the 2020 U.S. presidential election as a case study, this Part demonstrates these dynamics in action. In doing so, it also explores how disinformation campaigns can erode democracy and harm our democratic institutions.

Donald Trump's pre- and post-election campaign about widespread voter fraud and the 2020 presidential election being rigged against him is a fitting example of a disinformation campaign enabled by personal profiling and weak data privacy.[171] To quickly summarize, President Trump, conservative media outlets, and some Republicans falsely claimed that widespread voter fraud led to Joe Biden's win;

---

[171] *See, e.g.*, @realDonaldTrump, TWITTER (Nov. 13, 2020), https://twitter.com/realDonaldTrump/status/1327319294057848832?s=20; *see also* Philip Bobbitt, *Trump's Disinformation Campaign Threatens to Undermine the Government*, TIME MAG. (Nov. 23, 2020), https://time.com/5914894/trumps-disinformation-campaign-undermine-government/ (discussing the continuity of government); while it is difficult to ascertain whether President Trump *purposely* disseminated false information—thus making it a disinformation campaign vs. a misinformation campaign—this Article presumes President Trump's messaging was intentional.

they claimed that Democrats rigged the presidential election.[172] While the election fraud disinformation contained *some* level of truth in its messaging, the messaging was largely not true for the matter asserted because there was no verifiable or reliable evidence of systemic election fraud.[173] Accordingly, the end-product (e.g., disinformation messaging) was false or misleading.[174]

President Trump disseminated his election fraud disinformation campaign[175] through traditional and digital media pathways. While President Trump relied on Twitter to spread his false messaging, traditional media reported heavily on his false claims.[176] As President Trump and other conservatives distributed their election fraud disinformation through social media,[177] Trump's White House staff distributed messaging via official press communications, and third-party platforms (e.g., Fox News) distributed the campaign via their platforms and channels.[178]

A. Social Media Platforms and Personal Profiling Helped This Disinformation Spread Effectively

The election fraud campaign's main message spread quickly and widely.[179] For example, one of Trump's election disinformation tweets collected at least 1.1 million favorites and 884,500 retweets.[180] The live broadcast of President Trump's

---

[172] *See generally* Maryclaire Dale, *Trump's Legal Team Cried Vote Fraud, but Courts Found None*, ASSOCIATED PRESS (Nov. 22, 2020), https://apnews.com/article/election-2020-donald-trump-pennsylvania-elections-talk-radio-433b6efe72720d8648221f405c2111f9 (describing the Trump campaign's legal challenges regarding the election results).

[173] *See id.*

[174] *See supra* Figure 1.

[175] For the remainder of this Part, I refer to this campaign generally and employ the past tense even though the false messaging continues to spread as of the time of writing.

[176] *See supra* Figure 3; *see, e.g.*, Colby Itkowitz, et al., *Trump Falsely Asserts Election Fraud, Claims a Victory*, WASH. POST (Nov. 4, 2020), https://www.washingtonpost.com/elections/2020/11/03/trump-biden-election-live-updates/.

[177] *See id.*

[178] *See id.*

[179] It is difficult to quantify the campaign's spread because no quantitative analysis has been conducted as of November 24, 2020. A quantitative analysis is out of scope for this Article. Instead, this Article provides examples of the message's spread; *See, e.g.*, Jeremy Duda, *AZGOP Chair Kelli Ward Is Making Up Claims About 'Hidden' Precinct Voting Data*, AZMIRROR (Nov. 20, 2020), https://www.azmirror.com/blog/azgop-chair-kelli-ward-is-making-up-claims-about-hidden-precinct-voting-data/ (Arizona Republican falsely claiming fraud); Rebecca Heilweil, *YouTube Is Awash with Election Misinformation—and It Isn't Taking It Down*, VOX (Nov. 6, 2020), https://www.vox.com/recode/21551696/stolen-election-misinformation-youtube-trump-voter-fraud (reporting a slew of videos on YouTube that perpetuate the false claims); Jessica Guynn, *Trump Says the Election Is Not Over as 'Stop the Steal' and 'Voter Fraud' Disinformation Go Viral on Facebook and Twitter*, USA TODAY (Nov. 6, 2020), https://www.usatoday.com/story/tech/2020/11/06/election-fraud-claims-trump-facebook-twitter-stop-the-steal/6189479002/ (reporting that messages about how President-elect Biden is attempting to "steal" the election are gaining momentum on social media platforms).

[180] *See, e.g.*, @realDonaldTrump, TWITTER (Nov. 7, 2020), https://twitter.com/realDonaldTrump/status/1325099845045071873?s=20 ("I WON THIS ELECTION, BY A LOT!"); @realDonaldTrump, TWITTER (Nov. 4, 2020), https://twitter.com/realDonaldTrump/status/

election night speech collected 23.2 million views.[181] Here, the social media platforms' rapid cycle and huge social graph added fuel to the spread.

Personal profiling and content curation by social media platforms also contributed to this spread.[182] Individuals who interacted with the misinformation by liking, retweeting, or sharing the content were more likely to see more of the same content.[183] As Twitter's engineers explicitly stated, "The [algorithmic] model's score predicts how interesting and engaging a Tweet would be *specifically to you*."[184] This depends on personal data—for a social media platform to "predict how interesting and engaging" content will be, the platform tracks users' behaviors, interactions, and engagements with the content.[185] If a voter interacted or engaged with content related to Trump's election fraud campaign on a social media platform, by algorithmic design, the voter was more likely to see additional content on the same topic.

Social media platforms can recommend "interesting and engaging" content because the platforms can collect the different types of user data.[186] For instance, autogenerated data, such as a user's likes, shares, and retweets, is used to build a personal profile for each user; this data feeds the algorithms that determine what content is shown. The lack of data privacy protections allows the platform to collect such data and couple it with other information inputted by the user or procured from third parties in order to present more content that is "interesting and engaging." So, the platforms that prioritized the election fraud disinformation were able to do so *because* the platform could collect the vast amount of personal information. There were little to no comprehensive data privacy protections to prevent that from happening.

B. This Disinformation Hurt American Democracy

The danger with the Election Fraud Campaign's misinformation is an erosion of democracy, its principles, and its institutions. The January 6, 2021, attack on the U.S. Capitol was just one manifestation of this danger as it showed the sheer number of people who legitimately believed the misinformation's core narrative. But disinformation about the 2020 election had other erosive effects: it tainted the

---

1324032541544927233?s=20 (collecting nearly 200,000 retweets and 623,300 favorites—"They are finding Biden votes all over the place . . . .").

[181] @realDonaldTrump, TWITTER (Nov. 4, 2020), https://twitter.com/TeamTrump/status/1323888133390348288?s=20 (President Trump retweeting the then-live broadcast of his election night speech).

[182] *See supra* Part II.

[183] *See, e.g.*, Twitter Blog Post, *supra* note 111 ("we have worked to improve the underlying algorithms in order to surface content that is even more relevant to you.").

[184] *Id.* (emphasis added); this statement was made in 2017. This Article presumes that social media's technical capabilities, algorithms, artificial intelligence, etc. have improved since 2017.

[185] This Article presumes that other digital media platforms are designed similarly.

[186] *See supra* Part II.B.

marketplace of ideas, delegitimized of the press, and damaged trust in the integrity of a democratic election.

First, the election fraud campaign's misinformation tainted the marketplace of ideas. The idea behind this model is that truth will ultimately prevail over false information in the marketplace of ideas.[187] Though some amount of false or misleading information is inevitable and expected, the presupposition of the marketplace model is that the false or misleading information is *fairly countered* with true information.[188] However, from the individual's perspective, the election fraud campaign's misinformation *flooded* the marketplace of ideas because the enablers allowed for it.[189] In general, misinformation overwhelms the marketplace of ideas when the misinformation is prioritized because it is more "interesting and engaging."

Significant content curation may lead to false or unbalanced perceptions. By presenting users only with content they are predisposed to find interesting or engaging, social media platforms actually *promotes lazy thinking*.[190] When users are shown content that is interesting or engaging, like the election fraud disinformation, they are more likely to believe the curated content because humans are cognitive misers: due to confirmation bias, users are more likely to believe the curated content is true because it is familiar, feels right, and is understandable.[191]

Put another way, from a user's perspective the marketplace of ideas is overwhelmed by one narrative of information. The opposing narrative is deprioritized or curated out. Consequently, the user sees a disproportionate amount of content that supports the first narrative rather than the opposing one. As a result, the user may form a misperception or false belief (e.g., that the 2020 election was stolen from President Trump).

Second, the election fraud disinformation campaign delegitimized the press. This was not a new trend; President Trump and others attacked traditional media long before the election fraud campaign began. This delegitimization erodes the trust and faith that individuals place in the democratic institution tasked with informing the public (the press). An informed citizenry, empowered by the freedoms of the press, is a foundational requirement of a vibrant democracy. Thus, a delegitimization of the press harmed American democracy.

The spread of disinformation over social media platforms has helped enable this delegitimization, and it has benefited from it. This delegitimization of traditional media leaves a void that digital media has filled. Social media platforms allow

---

[187] *See generally* Lee Levine, et al., *Newsgathering and the Law*, § 1.01 (5th Ed. Matthew Bender & Company 2018) (describing the marketplace model); Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market . . . .").

[188] *See* Bobbitt, *supra* note 171.

[189] *See supra* Part II.

[190] *See id.*

[191] *See id*.

individuals to easily distribute information, regardless of whether it is true or false.[192] Because President Trump had for so long attempted to delegitimize the press, in the eyes of some Americans, it was difficult for the press to effectively combat his election fraud campaign.[193] President Trump consistently and pervasively called traditional media "fake news" and the "enemy of the people."[194] These attacks had dangerous effects on *what* and *whom* individuals believed. Countless comments from Trump supporters suggest that they believe the false information from President Trump, his campaign, and the Trump White House.[195]

In effect, President Trump eroded democracy and its principles by delegitimizing traditional media and pumping misinformation regarding the pandemic into the civic discourse. This disinformation campaign handicapped the press's role in checking government and officials, limiting its ability to hold the government to account. Here, millions of voters refused to believe anything the press reported, which in turn, hurt the democratic function of the press.

Third, the tainting of the marketplace of ideas and delegitimization of the press led some voters to lose faith in the integrity of a democratic election.[196] Many of the January 6 insurrectionists demonstrated this loss of trust and faith when they

---

[192] *Id.*

[193] *See* Wayne Rash, *As the U.S. Prepares for COVID 19 Disinformation Stokes Panic and Discord*, FORBES (Apr. 8, 2020), https://www.forbes.com/sites/waynerash/2020/04/07/as-the-us-prepares-for-covid-19-disinformation-stokes-panic-and-discord/?sh=3b98ed271b91.

[194] Emily Stewart, *Trump Calls Media the "True Enemy of the People" the Same Day a Bomb Is Sent to CNN*, VOX (Oct. 29, 2018), https://www.vox.com/policy-and-politics/2018/10/29/18037894/donald-trump-twitter-media-enemy-pittsburgh.

[195] *See, e.g.*, CNN, *Voter Gets Heated Defending Trump Response to Covid-19 Pandemic*, YOUTUBE (July 28, 2020), https://www.youtube.com/watch?v=MSGtwCKbCQo; Michael Goodwin, *Trump Got My Vote in 2016, Here's Why He Gets it Again in 2020*, FOX NEWS (Oct. 27, 2020), https://www.foxnews.com/opinion/trump-vote-2016-again-2020-michael-goodwin (an opinion piece); Paul Sacca, *VIDEO: Protesters in Huntington Beach Fight Back against Newsom's Curfew and California Lockdowns*, THEBLAZE.COM (Nov. 22, 2020), https://www.theblaze.com/news/lockdown-protest-california-newsom-trump-rally; CNN, *Biden and Trump Voters Discuss Trump's Virus Response*, YOUTUBE (Sept. 24, 2020), https://www.cnn.com/videos/politics/2020/09/24/voter-panel-vaccines-coronavirus-pandemic-unemployment-camerota-newday-vpx.cnn; Meredith Lee, *As Pence Heads to Minnesota, Voters in Key Battleground State Weigh Trump's Pandemic Response*, PBS (Apr. 27, 2020), https://www.pbs.org/newshour/politics/as-pence-heads-to-minnesota-voters-in-key-battleground-state-weigh-trumps-pandemic-response ("The president has done a reasonable job handling [the pandemic]."); Trip Gabriel, *Trump's Fights Are Their Fights. They Have His Back Unapologetically*, N.Y. TIMES (Aug. 25, 2020), https://www.nytimes.com/2020/08/25/us/politics/trump-reelection-supporters.html ("the coronavirus turned out to be 'a lot less severe . . . .").

[196] *See, e.g.*, Domenico Montanaro, *Poll: Just a Quarter of Republicans Accept Election Outcome*, NAT'L PUB. RADIO (Dec. 9, 2020), https://www.npr.org/2020/12/09/944385798/poll-just-a-quarter-of-republicans-accept-election-outcome (reporting that a solid majority of Americans trust the 2020 U.S. presidential election results, but noting that just 24% of Republicans surveyed trust the results); the NPR/PBS NewsHour/Marist poll surveyed 1,065 U.S. adults from December 1-6, 2020. For the poll's results and methodology, *see* http://maristpoll.marist.edu/npr-pbs-newshour-marist-poll-results-the-transition-trump-covid-19/#sthash.zs79O6pc.dpbs.

attacked the U.S. Capitol while falsely claiming election fraud.[197] The election fraud disinformation campaign's core narrative was that the 2020 U.S. presidential election was tainted by rampant voter fraud. Social media platforms' algorithmic design and content curation perpetuated this false narrative by presenting it to users whose personal profiles suggested that they would find this false narrative interesting or engaging.

Believing the misinformation and rejecting the truth has dangerous consequences.[198] The Trump campaign challenged the election results in the courts, but the courts that ruled on merits of the Trump campaign's claims flatly rejected its baseless allegations.[199] Still, many of Trump's followers pressed forward, despite the courts' rejections.[200] Although a majority of Americans are confident in the result of the 2020 Presidential election, "most Trump voters think Biden's victory is due to voter fraud."[201]

In summary, the election fraud disinformation tainted the marketplace of ideas with the help of the enablers while delegitimizing the press that is tasked as the check on government; consequently, many individuals wrongly believe(d) that an election was not fair.[202] All of this—the disinformation campaign, its false narratives, and its effects—culminated in the January 6, 2021, attack on the U.S. Capitol.[203] This insurrection demonstrated the dangerous consequences of disinformation campaigns. Hundreds, maybe thousands, of individuals who believed the election fraud campaign's core message gathered in Washington D.C.,

---

[197] *See* Timothy Snyder, *The American Abyss*, N.Y. TIMES (Jan. 9, 2021), https://www.nytimes.com/2021/01/09/magazine/trump-coup.html (describing the false narratives ahead of the 2020 U.S. presidential election and the contributing factors to the January 6, 2021, insurrection).

[198] *See, e.g.*, Kenya Evelyn, *Capitol Attack: The Five People Who Died*, GUARDIAN (Jan. 8, 2021), https://www.theguardian.com/us-news/2021/jan/08/capitol-attack-police-officer-five-deaths (describing the five individuals who died as a result of the U.S. Capitol insurrection).

[199] *See, e.g.*, Maryclaire Dale, *Appeals Court Rejects Trump Challenge of Pennsylvania Race*, ASSOCIATED PRESS (Nov. 27, 2020), https://apnews.com/article/election-2020-donald-trump-pennsylvania-elections-philadelphia-d9c96c4593ec278f3b1d4bc564068df6 (quoting a 3-0 decision from the Third Circuit Court of Appeals, "Free, fair elections are the lifeblood of our democracy. Charges of unfairness are serious. But calling an election unfair does not make it so. Charges require specific allegations and then proof. We have neither here.").

[200] *See, e.g.*, Bill Whitaker, *"It Is Not Cheating, It Is Democracy": A First-Hand Look at Ballot Counting in Pennsylvania*, CBS NEWS (Nov. 9, 2020), https://www.cbsnews.com/news/pennsylvania-ballot-counting-2020-election-60-minutes/ (quoting a Philadelphia commissioner who received death threats such as, "This is what the Second Amendment is for . . ." in response to Philadelphia "counting votes in a democracy.").

[201] Monmouth University Polling Institute, *More Americans Happy About Trump Loss than Biden Win*, MONMOUTH UNIV. (Nov. 18, 2020), https://www.monmouth.edu/polling-institute/reports/monmouthpoll_us_111820/ (finding that 77% of Trump supporters believe Biden's win was due to fraud; the survey was conducted by telephone from November 12-16, 2020, with 810 U.S. adults with a margin of error of ± 3.5%).

[202] *See generally* Donald J. Trump for President v. Pennsylvania, No. 20-3371 (3d Cir Nov. 27, 2020) (finding that the 2020 U.S. presidential election was fairly held).

[203] *See generally* Lauren Leatherby, et al., *How a Presidential Rally Turned into a Capitol Rampage*, N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/interactive/2021/01/12/us/capitol-mob-timeline.html.

marched to the U.S. Capitol, attacked law enforcement, and forced their way inside the Capitol building.[204]

As harmful as it was, the election fraud disinformation campaign is far from the only example.[205] Accordingly, the 116th and 117th Congresses have explored legislative and regulatory changes to combat the disinformation on digital platforms, such as regulating the content itself; how a platform identifies, detects, or moderates misinformation; and changes to § 230 of the Communications Decency Act ("CDA" or "Section 230"). [206] The next Part examines these proposals and recommends a path forward.

C. Legal Solutions to Disinformation Campaigns

This Part begins by examining various proposals from practitioners, scholars, and policymakers regarding policy reforms to combat the issue of misinformation. It argues that their proposals are insufficient or ineffective. It then argues that comprehensive data privacy and security protections are necessary to mitigate the damage caused by foreign and domestic actors and their disinformation campaigns.

1. Regulating the Content Is Insufficient

Since Russia's disinformation campaign during the 2016 U.S. presidential election, the federal government has sought to curb misinformation on social media platforms.[207] Specifically, Congress and scholars have explored amending Section 230, regulating content itself, and setting rules for how platforms identify, detect, or moderate misinformation.[208] While any effort by Congress or industry practitioners to help mitigate misinformation online is welcome, none of the regulatory, legislative, or technological proposals will sufficiently combat the problem. This Section discusses three proposals in particular. It argues that these proposals are insufficient because none of them address the poor data privacy and

---

[204] *Id.*; *see* Rebecca Harrington, et al., *420 People Have Been Charged in the Capitol Insurrection So Far. This Searchable Table Shows Them All.*, INSIDER News (Apr. 16, 2021), https://www.insider.com/all-the-us-capitol-pro-trump-riot-arrests-charges-names-2021-1 (listing the 400 individuals who have been charged with crimes related to the January 6, 2021, U.S. Capitol attack).

[205] For more examples, *see supra* Introduction.

[206] *See, e.g., Does Section 230's Sweeping Immunity Enable Big Tech Bad Behavior?: Hearing Before the S. Comm. on Com., Sci, and Tech.*, 116th Cong. (opening statement of Mark Zuckerberg, witness) [hereinafter "Zuckerberg's Statement"]; § 230 grants broad immunity to digital media platforms for the third party content on their platforms; *see* 47 U.S.C. § 230.

[207] *See, e.g.*, Mueller Report, *supra* note 15 (discussing the findings of the special counsel investigation into Russia's election interference).

[208] *See, e.g.*, Griffis, *supra* note 134; Ryan Tracy & John McKinnon, *Tech CEOs Square Off with Senators in Hearing Over Online Speech*, WALL ST. J. (Oct. 28, 2020), https://www.wsj.com/articles/senate-tech-hearing-facebook-twitter-google-11603849274 (recapping a U.S. Senate hearing that discussed social media's post-2016 U.S. presidential actions in combatting misinformation).

security regime in the U.S., which is a critical root cause that enables disinformation to spread, and instead focus on the content itself.

First, the 116th Congress explored amending Section 230. Section 230 grants broad immunity to digital media platforms, preventing them from being held liable for the content that third parties post or upload.[209] Both Republicans and Democrats in the 116th Congress agreed that Section 230 reform may be necessary, but policymakers cannot agree on what these changes should be.[210]

Many Republicans have argued that Section 230 allows digital media platforms to infringe on free speech, and President Trump even called for its outright repeal.[211] Senator Ted Cruz (R-TX) for instance, argues that social media platforms "collectively pose the single greatest threat to free speech in American and the greatest threat we have to free and fair elections."[212] Accordingly, Congressional Republicans have proposed limits to the right of who the platforms can exclude, narrowing content moderation rights to specific types of speech not protected by the First Amendment, and removing protection for discriminatory content moderation decisions.[213] Senator Lindsey Graham (R-SC), however, does not support the repeal of Section 230 and argues instead that social media platforms should self-regulate.[214]

Democratic senators also criticize and propose reforming Section 230. They argue that the industry's business model incentivizes platforms to keep their users engaged as much as possible,[215] and also that the platforms should increase their efforts in identifying and labeling misinformation.[216] Some Democratic proposals have included removing protection for any kind of paid speech (e.g., advertising) and increasing the responsibility of platforms in identifying and removing offensive, abusive, or illegal content.[217]

Both parties' proposals for Section 230 reform would likely be insufficient and ineffective at combatting the spread of disinformation. Proposals that include or rely on industry self-regulation are flawed because social media platforms are not incentivized to make changes to their products that would decrease user

---

[209] 47 U.S.C. § 230.

[210] *See* Griffis, *supra* note 134.

[211] Sara Morrison, *Republicans Accuse Twitter's Jack Dorsey and Other Big Tech CEOs of Violating Their Free Speech Rights*, VOX (Oct. 28, 2020), https://www.vox.com/recode/2020/10/28/21536780/facebook-twitter-google-zuckerberg-dorsey-pichai-senate-section-230-hearing.

[212] *Id.*

[213] Lauren Feiner, *House Republican Staff Outline Principles to Reform Tech's Liability Shield*, CNBC (Apr. 15, 2021), https://www.cnbc.com/2021/04/15/house-republicans-outline-principles-for-reforming-section-230.html.

[214] Morrison, *supra* note 306.

[215] *Id.* (quoting Sen. Amy Klobuchar, D-MN).

[216] Griffis, *supra* note 134 (quoting Sen. Diane Feinstein, D-CA).

[217] Bobbie Johnson, *How a Democratic Plan to Reform Section 230 Could Backfire*, MIT TECH. R. (Feb. 8, 2021), https://www.technologyreview.com/2021/02/08/1017625/safe-tech-section-230-democrat-reform/.

engagement.[218] Indeed, their business model incentivizes platforms to keep their users engaged as much as possible.[219]

Further, the Democrats' proposals to mitigate misinformation, such as identifying and labeling the misinformation, are reactive where a proactive solution is needed. While platforms can identify and label misinformation, as both Twitter and Facebook did in the 2020 U.S. presidential election,[220] users can ignore the labels as they can perceive the labels as contradictory to their beliefs.[221]

In addition, Senator Cruz and other conservatives are mistaken in their belief that the First Amendment protects third parties' speech on the social media platforms. This is because the First Amendment does not apply between two *non*-government actors—the user and the platform.

Second, scholars have proposed misinformation identification, detection, and removal solutions. For example, Professor Huan Liu and Ph.D. Candidate Kai Shu, data scientists at Arizona State University, propose an "intelligent fake news detection system" that utilizes advanced data mining.[222] In their research, Shu and Liu compiled several fake news detection platforms that identify, detect, or remove misinformation.[223] They assert that "detecting fake news in the early stage is important to prevent its further propagation on social media."[224]

While it is true that detecting disinformation may help, it is only a partial solution. This is because this solution only affects how disinformation is consumed. Mitigating disinformation consumption is limited in effectiveness because disinformers can still distribute it.[225] Accordingly, while the false information may not reach millions of impressions because the consumption was mitigated, it still may reach a significant number of people because disinformers are free to continue distributing content. Thus, a complete solution must target both distribution and consumption.

Third, many individuals across government, the technology sector, and academia propose content moderation or censorship. According to Mark

---

[218] *See* PROA, *supra* note 145, at 17 ("the fundamental issue with self-regulation is the conflict of interest that exists—the regulators are the regulated . . . [self-regulation] is at conflict with the regulator's source of revenue.").

[219] Morrison, *supra* note 211.

[220] *See* Ellen Goodman & Karen Kornbluh, *How Well Did Twitter, Facebook, and YouTube Handle Election Misinformation?*, SLATE (Nov. 10, 2020), https://www.slate.com/technology/2020/11/twitter-facebook-youtube-misinformation-election.html (providing an overview of digital media platforms' efforts to identify and label misinformation).

[221] *See supra* Part II (users may disregard the contradictory information due to confirmation bias).

[222] *See generally* Detecting Fake News, *supra* note 126, at iii, 1-8.

[223] *See id.* at Appendix B (listing Hoaxy from Indiana University, FakeNewsTracker from Arizona State, and dEFEND and NewsVerify from private parties).

[224] *Id.* at 7.

[225] I classify these solutions as consumption solutions. These proposals are not distribution solutions because the distribution of misinformation still occurs; a distribution solution would disable the dissemination of misinformation.

Zuckerberg, Facebook's founder and chief executive, in the first half of 2020, Facebook removed over 250 million pieces of content that violated Facebook's policies, including content that promoted terrorism, violence, cyberbullying, child nudity, etc.[226] Senator Ed Markey (D-MA) responded, "[t]he issue is not that [digital media platforms] are taking too many posts down [but rather] [t]he issue is that they are leaving too many dangerous posts up."[227]

Automation is required for this content moderation and censorship to operate at scale. Mass content moderation and censorship requires artificial intelligence-powered misinformation detection, identification, and removal solutions, such as the fake news detection solutions compiled by Shu and Liu.[228] While content moderation and censorship would help mitigate the effects of misinformation, these proposed solutions are similarly insufficient because these mostly mitigate consumption and not distribution of misinformation.[229] Moreover, disinformers would identify and circumvent the automation that powers the content moderation and censorship, similar to how fraudsters evolve their strategies to commit fraud against the world's largest companies.[230]

While these proposals would likely reduce the number of user impressions, the misinformation itself would still be distributed to those users who find the content interesting or engaging. Content moderation and censorship are reactive mitigation strategies that disinformation campaigns can circumvent.

In brief, measures that merely react to misinformation, such as identification, labeling, and removal, and measures that conflict with social media platforms' monetization models are likely ineffective or insufficient at combating the misinformation. Instead, an effective solution must include proactive measures. This might include mitigating the technological capabilities that power misinformation dissemination rather than moderating the content itself, for instance.

Not all proposed reforms would be ineffective. During the 117th Congress, Representatives Anna Eshoo (D-CA) and Tom Malinowski (D-NJ) proposed the Protecting Americans from Dangerous Algorithms Act ("Algorithms Act").[231] The

---

[226] *Id.* at 2.

[227] Tracy & McKinnon, *supra* note 208.

[228] *See* Detecting Fake News, *supra* note 126.

[229] *See supra* Figure 1.

[230] *See, e.g.*, Glenn Larson, *Synthetic Identity Fraud Is the Fastest Growing Financial Crime – What Can Banks Do to Fight it?*, FORBES (Oct. 8, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/10/08/synthetic-identity-fraud-is-the-fastest-growing-financial-crime-what-can-banks-do-to-fight-it/?sh=5cf399067ecb (discussing synthetic identity fraud as a new rising form of fraud); Chris Schnieper, *Study Reveals Fraud Flourishes Amid COVID-19 Pandemic*, LEXISNEXIS RISK SOLUTIONS (Nov. 6, 2020), https://blogs.lexisnexis.com/fraud-and-identity-in-focus/study-reveals-fraud-flourishes-amid-covid-19-pandemic-mdr/ (discussing how fraud changed with the pandemic).

[231] Lauren Feiner, *Facebook's Suggestion to Reform Internet Law Is a 'Masterful Distraction' Says Silicon Valley Congresswoman*, CNBC (Mar. 24, 2021), https://www.cnbc.com/2021/03/24/facebook-section-230-suggestion-masterful-distraction-rep-eshoo.html.

Algorithms Act would remove immunity under Section 230 in cases "where a platform's algorithm has amplified or recommended a post directly relevant to a case involving acts of international terrorism or civil rights violations."[232] This proposed reform would be effective because, unlike the content moderation proposals previously mentioned, the Algorithms Act targets an *enabler* of the misinformation spread.

While Section 230 reform, misinformation detection, and content moderation and censorship would add some value in the fight against misinformation campaigns, none of these solutions address a critical root cause of the dissemination. A more successful strategy at combating disinformation campaigns must focus on impairing algorithms that curate content based on personal data by enacting comprehensive data privacy and security reform.

2. The Preservation of Democracy Requires Data Privacy Protection Now

To thwart misinformation distribution, an effective solution must proactively address the personal profiling and the algorithmic design that enables content curation. This Section proposes legislative reforms that Congress can pass to address this problem, balancing their benefits and costs.

As argued throughout this Article, the current data privacy regime lacks comprehensive federal data privacy and security protections. Social media platforms can collect and use many types of user data with almost no constraints. This data forms the personal profiles that platform algorithms use to curate the content that users find engaging. This dynamic enables disinformation to spread more effectively.[233] So, Congress must target these the personal profiling and content curation algorithms by strengthening the data privacy and security regime. By effectively disabling or limiting the algorithms that result in content curation, Congress would create greater protections for individuals and American democracy. But how strong should the data privacy and security protections be? To what extent should such protections be enacted? And why must it be Congress and not industry self-regulation?

If social media platforms were prohibited from collecting user-inputted, queried, or autogenerated data, then the platforms' ability to construct personal profiles would be grossly limited. However, a full prohibition of data collection is impractical because websites need to collect some data to deliver their products and services. Accordingly, similar to Europe's GDPR, more data privacy and security protections, controls, and limitations are necessary in order to curb disinformation spread.[234]

---

[232] *Id.*

[233] *See supra* Part II.

[234] *See generally* Natasha Lomas, *US Privacy, Consumer, Competition and Civil Rights Groups Urge Ban on 'Surveillance Advertising'*, TECHCRUNCH (Mar. 22, 2021), https://techcrunch.com/2021/03/22/us-privacy-consumer-competition-and-civil-rights-groups-urge-ban-on-surveillance-advertising/ (proposing a ban on mass tracking and profiling of web users and pointing out "less toxic non-tracking alternatives").

This raises the question as to why the industry has not proposed comprehensive reform to data privacy and security controls and protections. The answer to this question is simple: because data is the internet's currency—it is how digital media platforms monetize their products and services.[235] Any increase in user privacy threatens social media's revenues. For example, Apple proposed and implemented a privacy change to iOS that makes it more difficult for third-party applications to track iPhone users and collect user data.[236] Facebook rang the alarm; it said that Apple's change would hurt its bottom line because the change limits the kind of personalized targeting that Facebook is able to do.[237] Facebook estimated that its annual revenue would decline by *half* as a result.[238] This example illustrates why industry self-regulation is unlikely to help protect user privacy. No industry would adopt self-regulation with such a damaging effect on its profitability.

Since social media platforms cannot be counted on to regulate themselves, government must act.[239] However, Congress must move beyond its focus on insufficient and ineffective reactive solutions, such as Section 230 reform and content moderation and censorship. One major challenge is that policymakers fundamentally lack the technological knowledge necessary to address the root of the problem.[240] For example, Senator Orrin Hatch (R-UT) asked Facebook CEO Mark Zuckerberg, "How do you sustain a business model in which users don't pay for your service?"[241] This question demonstrated a fundamental lack of understanding regarding social media's monetization models.

To effectively mitigate the effects of misinformation, Congress must address the root causes and contributing factors. To do this, it must first better its understanding of technology, technological systems, and industry incentive structures for the reasons stated herein. However, this bettered understanding cannot come from the social media platforms themselves because their interests and incentives are not aligned with combating the rise in misinformation. Comprehensive data privacy and security controls and protections must be at the core of any Congressional proposal for it to be effective. Like how some states have

---

[235] *See generally*, *Katz* and COVID, *supra* note 115, at 54; PROA, *supra* note 145, at 17.

[236] Reed Albergotti & Elizabeth Dwoskin, *Apple Makes a Privacy Change, and Facebook and Advertising Companies Cry Foul*, WASH. POST (Aug. 28, 2020), https://www.washingtonpost.com/technology/2020/08/28/facebook-apple-ios14/.

[237] *Id.*

[238] *Id.* (According to the Washington Post, Facebook estimates that it would experience a 50% drop in its revenues. The $38.8 billion approximation is calculated by halving Facebook's annual revenues from its advertising business—$69.66 billion according to Facebook's 10-K released in January 2020); *see* Facebook 10-K, *supra* note 123.

[239] *See generally* PROA, *supra* note 145 (discussing specific data privacy and security reforms that Congress should enact in a comprehensive data privacy and security regime).

[240] *See, e.g.*, Emily Stewart, *Lawmakers Seem Confused about what Facebook Does—and How to Fix It*, VOX (Apr. 10, 2020), https://www.vox.com/policy-and-politics/2018/4/10/17222062/mark-zuckerberg-testimony-graham-facebook-regulations (recapping a joint Senate hearing before the Senate Judiciary and Senate Commerce, Science, and Transportation Committees that discussed Facebook, its data privacy practices, and Cambridge Analytica).

[241] *Id.* (Sen. Hatch retired in January 2019 and was succeeded by Sen. Mitt Romney).

enacted GDPR-inspired data privacy and security legislation, Congress should rely on GDPR when drafting the federal legislation. The remainder of this Section details a non-exhaustive list of several components of an overall proposal that would curb the distribution of disinformation.

First, where possible and logical, Congress should replace the *reasonable expectation of privacy* standard—a standard directly and indirectly present in various areas of privacy law—with a stronger standard that affords the data subject (i.e., user) greater control and protection.[242] For instance, a right of control would be a stronger standard than the reasonableness test.[243] The right of control standard would ask whether an individual's right to control her data, its privacy, and its security was violated or infringed.[244] Unlike the reasonable expectation of privacy standard, where objective and subjective privacy expectation fluctuate and wane over time,[245] the right of control standard would not weaken when privacy expectations shift because this standard relies on *tangible control*, not intangible expectations.[246] Here, a right of control would thwart misinformation distribution by flipping the decision-making power from social media platforms to the users; users would decide who collects, uses, and stores their personal information and to what extent.

Second, comprehensive data privacy and security legislation should include a private right of action—allowing users to sue social media platforms for violations of data privacy and security protections, such as the right to control.[247] A private right of action would alter market incentive structures, which in turn, would drive systemic change across social media platforms.[248] This is because such actions would serve a deterrent function—platforms will look to avoid potential litigation and liability by proactively mitigating its risks, including the risk of a data breach.[249]

Data minimization is one mitigation strategy to reduce liability exposure; data minimization involves collecting, using, and storing only the personal information necessary to complete the transaction between the platform and the user.[250] A private right of action, which would likely result in the increase of data minimization practices, would curb the distribution of misinformation by limiting the collection of some personal information that would have otherwise been collected for a platform's algorithms.

---

[242] *Katz* and COVID, *supra* note 115, at 79.

[243] *Id.*

[244] *Id.*

[245] United States v. Jones, 565 U.S. 400, 427 (Alito, J., concurring) (arguing that the reasonable expectation of privacy standard is flawed because it presumes stability and fails to address how technological advances may erode privacy expectations).

[246] *Id.*

[247] PROA, *supra* note 145.

[248] *Id.*

[249] *Id.* at 9.

[250] *See id.*

Third, legislation should recognize the different data types (user-inputted data, automatically generated data of the user's activity, and data procured from third-parties) and distinguish the data privacy and security protections, controls, and limitations accordingly.[251] Moreover, protections, controls, and limitations must recognize the various activities associated with data (i.e., what a data collector or processor does with the data); this includes data collection, use, processing, and storage.

By distinguishing data types, when all things being equal (e.g., the content of the data itself), social media platforms would still have the ability to collect and store certain data, such as the user-inputted data, but face stricter protections and limitations for other types, such as autogenerated data.[252] Take, for example, the hypothetical posed in Part II, Section C. If the CSLI at issue in *Carpenter* was user-inputted, not autogenerated, then the third-party doctrine would easily apply, but CSLI is autogenerated data that holds a higher level of privacy expectations.[253] Accordingly, CSLI should be afforded a higher level of privacy protection.

The level of protection, control, or limitation should also depend on what is happening with the data—whether it is being collected, used, processed, or stored. For instance, the collection of user-inputted data should be less restrictive than the collection of autogenerated data because, with the former, the user is affirmatively providing the data to the data collector. In addition, a form of control may be providing proper notice to the user regarding (i) what data is being procured about him or her, (ii) how will that data be used, and (iii) where and how that data will be stored, if at all. And an example of a limitation could be restricting the collection and use of autogenerated data for the purposes of advertising or content curation.

These types of protections, controls, and limitations are foreign, either. Individuals already maintain some level of control with respect to their credit reports—a form of queried data. Typically, an individual must authorize the data collector (e.g., lender) to obtain or procure the credit data from a data bureau (e.g., Experian). Congress can expand controls like these to other types and forms of data.

With reforms like the foregoing proposals, misinformation that erode the trust and faith in democratic elections, institutions, and principles would be limited in their reach and effect. A private right of action would disrupt the industry incentive structure that is currently focused on user engagement through content curation, and a stronger privacy standard (right to control) and distinctions among the data types would afford the user greater control and protection.

Unfortunately, it is unclear whether the federal government can enact comprehensive data privacy and security reforms. As previously mentioned, the 116th Congress introduced various proposals regarding data privacy and security, but as of June 2021, none of these proposals have advanced out of committee

---

[251] *See* Part II.C.

[252] *See* Part II.C.

[253] *Id.*

(during the 117th Congress).[254] While a few of the proposed bills have bipartisan support, the contentious areas are the private right of action and preemption.[255] Congressional Republicans are generally opposed to a private right of action while Congressional Democrats generally support it.[256] The converse is true with respect to provisions preempting state law.[257]

Unless the political parties reach an agreement regarding these provisions, it appears unlikely that any data privacy and security proposal will advance in the near-term.[258] Even with the Democrats in control of both the legislative and executive branches, intraparty disagreements and technological ineptitude on Capitol Hill may still result in legislative gridlock.[259]

V. CONCLUSION

Congress must enact comprehensive data privacy and security protections to combat the rise of misinformation on social media platforms. These protections would platforms' ability to display targeted disinformation to the users most vulnerable to it. Disinformation campaigns have caused serious damage to democracy, its institutions, and its principles. By strengthening the country's data privacy regime, Congress can begin to repair this damage.

---

[254] *See generally* JONATHAN M. GAFFNEY, CONG. RSCH. SERV., LSB10441, WATCHING THE WATCHERS: A COMPARISON OF PRIVACY BILLS IN THE 116TH CONGRESS (2020) (comparing various data privacy and security proposals by the 116th Congress); *Right of Privacy*, GOVTRACK, https://www.govtrack.us/congress/bills/subjects/right_of_privacy/5910#sort=-introduced_date (last visited Dec. 21, 2020) (tracking all proposed bills in the U.S. Congress related to the right of privacy, as determined by the Library of Congress).

[255] Müge Fazlioglu, *Tracking the Politics of US Privacy Legislation*, INT'L ASS'N OF PRIVACY PROF'LS (Dec. 13, 2019), https://iapp.org/news/a/tracking-the-politics-of-federal-us-privacy-legislation/.

[256] *Id.*

[257] *Id.*

[258] GAFFNEY, *supra* note 254, at 5.

[259] *See generally* Amber Phillips, *What You Need to Know About the Georgia Senate Runoff Elections*, WASH. POST (Dec. 17, 2020), https://www.washingtonpost.com/politics/interactive/2020/georgia-senate-runoff-guide/ (discussing the January 2021 special election in Georgia for its two U.S. senate seats that will determine control of the Senate).