PART I

A Lawless Internet

1

The Hidden Rules of the Internet

In August 2017, several hundred white nationalists marched on the small university town of Charlottesville, Virginia. The rally turned tragic when one of the protesters rammed his car into a crowd of counterprotesters, killing 32-year-old Heather Heyer. The *Washington Post* characterized the protesters as "a meticulously organized, well-coordinated and heavily armed company of white nationalists."[1]

Heyer's death was mourned across the United States, but to people on the Nazi website The Daily Stormer it was reason to celebrate. Stormer editor Andrew Anglin wrote that Heyer was a "Fat, Childless 32-Year-Old Slut" and that "most people are glad she is dead."[2] On the site's forums and in its private chat channels, participants spewed hateful memes and made plans to send armed Nazi agitators to Heyer's funeral.

Rampant abuse and hatred on digital networks is not new. The pressure to combat hate is strongest on such ubiquitous social media platforms as Facebook, Twitter, and Reddit. Governments and civil society organizations worldwide have complained for years that, even though their terms of service generally prohibit abuse and hate speech, these platforms do not do enough to enforce their rules. Social media platforms are responding to increasing pressure by more clearly articulating their standards of acceptable behavior and banning users and groups that spread hatred and abuse. These rules are not yet uniformly enforced, but they are becoming enforced more regularly.

As the large and well-known networks begin to crack down on abuse and hate, hate groups are moving to less mainstream sites. The Daily Stormer is a perfect example. It is one of the larger neo-Nazi sites, described by the nonprofit Southern Poverty Law Center in 2016 as the "top hate site in America" and "the most popular English-language radical right website in the world."[3] Southern Poverty Law Center senior research analyst Keegan Hankes explains that the site "took its name from *Der Stürmer*, an astoundingly vile and pornographic Nazi newspaper started by Julius Streicher and specializing in attacking Jews. Streicher was later hanged for war

crimes at Nuremberg."[4] Like many extremist sites, The Daily Stormer operated on the safety of its own domain and hosted its own site, which meant it was free to follow its own rules.

Even on the open web, away from the policies of social media platforms, there are always points of control on the internet. Each website must have a hosting service for its hardware or virtual servers, lease a network connection, and register a domain name. Everyone who wants to use the internet has to enter into an agreement with an internet service provider (ISP). The contracts for these services usually contain a clause that allows the provider to cancel the agreement at any time. This means that companies that provide infrastructure services on the internet can make decisions about who is allowed to speak and participate online. Still, it's rare for an internet infrastructure service provider to get involved in public debates about the content that people distribute over their networks. Many of these infrastructure companies see themselves as neutral, and the presumption that they shouldn't get involved in debates about content is as old as the internet itself. This means that, even though an ISP might cancel an account on occasion, hate groups have not traditionally had difficulty finding a host that will accept their content.

Charlottesville was a game changer. During the media storm about the rise of domestic extremist groups, infrastructure companies made unprecedentedly concerted moves to disconnect The Daily Stormer. GoDaddy, a well-known domain registrar, informed The Daily Stormer that it would no longer host the site's domain name. The Daily Stormer moved to Google's domain management service and was kicked off within hours. In addition, Google placed a "hold" on the site, which prevented it from moving to a different registrar and effectively confiscated the main domain. This was a serious problem for the Stormer; without a well-known domain name, websites are extremely difficult to find. The site operators then attempted to register a series of other domains, including through registrars in China, Russia, and Albania, each of which was canceled only hours later.

The most significant move came when Cloudflare, a content distribution network, canceled its contracts with The Daily Stormer. Cloudflare is not a host, but a security and content distribution company that accounts for nearly 10 percent of the world's internet traffic.[5] It makes copies of its clients' websites and distributes them worldwide so that they are faster to access and protected against hackers and other security breaches. Most of us never think about companies like Cloudflare because they exist in the background of the internet and, although they are what allow sites we access every day to function smoothly, we would have little to no reason to interact directly with the company. Companies like Cloudflare not only make the web faster, they provide crucial protections from attackers who routinely try to force websites offline. A distributed denial of service (DDoS) attack works by flooding a web server with so many fake requests that it becomes unable to respond – effectively shutting the website down. DDoS attacks are so commonplace now that any high-traffic or controversial site must use a content distribution network or risk being

blasted off the internet by malicious attackers. Very little technical skill is needed to coordinate a DDoS attack. Without the protection of a service like Cloudflare, a site like The Daily Stormer could be easily taken offline by anyone who disagreed with its hateful content. In fact, it was a would-be attacker that first contacted Cloudflare and asked it to drop The Daily Stormer as a client: "Get out of the way so we can DDoS this site off the Internet."[6]

Cloudflare historically shied away from making decisions about which sites should stay online. It has a policy to follow the law and only remove accounts or provide identifying information subject to a valid court order in the jurisdictions in which it operates. Since 2013, it had prominently stated that "Cloudflare has never terminated a customer or taken down content due to political pressure," and it assures users that it will "exhaust all legal remedies" to try to protect its users before it terminates a customer account.[7] The decision to drop The Daily Stormer was an important one. The site could have continued shopping around for hosts and domain registrars, but without the protection offered by one of a small number of content distribution networks like Cloudflare or its competitors it was unlikely to survive on the open web.

After running out of options, The Daily Stormer moved to a part of the "dark web."[8] The dark web is almost like the internet's alternate universe; it's not findable by search engines and can only be accessed through special anonymizing browsers, like Tor, that are designed to be private and resilient. Tools like Tor have become relatively easy to install, but they still require technical skills, knowledge, and some determination to use. Even without the dark web, it is almost impossible to completely remove any site from the internet; there will always be people willing to create copies and archives of content that others try to block. But censorship doesn't have to be perfect to be effective. By making The Daily Stormer difficult enough to find and getting it off the mainstream of the open web, anti-racism advocates hope that they can substantially slow its influence and starve it of attention.

The decisions by major internet infrastructure companies to remove The Daily Stormer from the open web have been extremely controversial. The strongest critics are not the people who want to support the site's vile propagation of hate; rather, it's those who worry about the implications of putting public pressure on infrastructure companies and how that affects regulation of speech in the future. The Electronic Frontier Foundation (EFF), a civil society group dedicated to protecting freedom of speech online, took a hard line in response: "Protecting free speech is not something we do because we agree with all of the speech that gets protected. We do it because we believe that no one – not the government and not private commercial enterprises – should decide who gets to speak and who doesn't."[9] The EFF and others worry about the precedent set by these decisions, particularly as major internet companies are facing a lot of pressure to do more to police the internet on an ever-widening set of issues. It points out that decisions made at the infrastructure level – like the domain name system, crucial backbone links, or the massive pipes

operated by content distribution networks – will always be somewhat crude. The companies that operate this infrastructure cannot target single posts or individual pieces of content; they only have a blunt ability to refuse to host an entire site or domain. This power, many free speech advocates believe, should almost never be exercised because it will inevitably censor more than the specific posts or content targeted.

What makes this so difficult is that infrastructure services are sometimes the only viable option to target some websites. The standards for hate speech are very different outside the United States, and The Daily Stormer website would probably be illegal in countries like Germany or France, which have strong laws designed to ensure that people cannot publicly advocate genocide. Without tackling internet infrastructure on some level, these laws are basically unenforceable – sites like The Daily Stormer can easily move to a jurisdiction that will give them the protection that they seek. Infrastructure may not be the best way to tackle harmful content, but sometimes it is the only option.

The crux of the issue is not really about speech but due process. Due process is the difference between enforcing a legitimate law in a careful and accountable way and making an arbitrary or capricious decision that can have serious consequences. When Cloudflare announced it had dropped The Daily Stormer, Cloudflare's CEO Matthew Prince blogged about his deep ambivalence about the decision. He stood behind the decision but worried about the precedent it set for the future: "Law enforcement, legislators, and courts have the political legitimacy and predictability to make decisions on what content should be restricted. Companies should not."[10] In a memo to the company, he elaborated:

> This was my decision. Our terms of service reserve the right for us to terminate users of our network at our sole discretion. My rationale for making this decision was simple: the people behind the Daily Stormer are assholes and I'd had enough.
>
> Let me be clear: this was an arbitrary decision. It was different than what I'd talked with our senior team about yesterday. I woke up this morning in a bad mood and decided to kick them off the Internet. I called our legal team and told them what we were going to do. I called our Trust & Safety team and had them stop the service. It was a decision I could make because I'm the CEO of a major Internet infrastructure company.
>
> Having made that decision we now need to talk about why it is so dangerous. I'll be posting something on our blog later today. Literally, I woke up in a bad mood and decided someone shouldn't be allowed on the Internet. No one should have that power.[11]

This is what I mean when I say the internet is governed in a "lawless" way. The rule of law is the difference between arbitrary decisions and decisions that are fair and accountable. Cloudflare, like many other companies that influence what we see and say online, operates within the law. But when such companies make decisions about who uses their networks and how, they have almost unlimited discretion. They are

accountable only to the market; there are no checks and balances on how they wield their power. Whether we agree with the outcome or not, Cloudflare's decision to disconnect an entire website was based on the personal whim of its CEO. Prince is right: no one should have that power.

PROCESS MATTERS

This is not an isolated example. For as long as the commercial internet has been available, concerns about bullying, harassment, hate speech, and abuse have prompted calls for internet companies to better police the web. Civil society organizations are constantly lobbying for social media platforms to better protect vulnerable people, and users themselves are threatening to leave social media platforms that have become toxic with rampant abuse. Executives at these companies know that they need to take these issues seriously. Hosting company DigitalOcean terminated web hosting for both The Daily Stormer and pro-hate speech crowdfunding site Hatreon; it said in a statement that "[t]his is a terrible situation, but DigitalOcean believes that tech has a role in preventing hate crimes and violence from spreading, and takes that responsibility seriously.[12]" Undoubtedly, tech companies are going to continue to face more demands to take action against users who are spreading hatred.

Technology companies are facing mounting pressure from many different directions to do much more work to police what their users do online. New laws are being introduced around the world – and particularly in Europe – that impose tough new requirements on the way the industry deals with personal data, hate speech, copyright infringement, and other issues. The recent revelations of foreign interference in the 2016 US presidential elections has led to increasing calls for social media platforms and search engines to filter out disinformation and to crack down on fake accounts. The copyright industries have been lobbying for years for the power to require domain name registrars to confiscate the domains of sites that facilitate piracy, to prohibit payment processors from forwarding donations or payments for advertising, and to require ISPs to block their traffic.[13]

The issue of due process has not yet been solved. In the past, due process would involve the courts, which are set up to ensure fairness. It's not realistic to think that courts will have a primary role in the future of the internet, though. They're too expensive and too slow to make a real dent in online abuse and hate, or copyright infringement, or many other problems that involve user-generated content on a massive scale. Technology companies have become the preferred way to enforce the law online because they are able to cheaply influence large numbers of users, but this efficiency always comes at the cost of due process.

When technology companies make decisions that affect their users, there are few avenues of redress for people who feel that they have been treated unfairly. US federal law provides technology companies immunity for their decisions to

moderate their networks, and absolves them of liability for what their users say online. Their power to control their users is protected by the First Amendment, but the First Amendment does not protect users from the decisions of technology companies. The First Amendment only prevents the US government from interfering with speech; US tech companies are private entities and are free to decide whether or not they provide services to a particular person or group. US tech companies are not obliged, under the First Amendment, to respect free speech rights of users.

The absence of government regulation is not freedom. This book is called *Lawless* because so many of the decisions about what we can do and say online are made behind closed doors by private companies. This is the opposite of the standards we expect of legitimate, legal decision-making in a democratic society. Where governments do not set laws to regulate the internet, platforms and other powerful telecommunications providers are constantly making decisions about what types of speech they will carry. The major social media platforms all have rules about the content they deem acceptable, and many of these have expressed limits on hatred and abuse. Without law, though, these rules are not enforced in any way that can be called legitimate. There's no easy way to ensure either that the rules are consistently enforced or that they are enforced in a way that is fair and free from bias.

Technology companies exercise an unprecedented degree of power over how we share information, who we communicate with, and what news we see. Search engines have a massive degree of influence over the information we find and how we connect with other individuals and businesses. Social media platforms like Facebook, Twitter, YouTube, and Instagram constantly make decisions that directly influence what we can see and share. Infrastructure companies can prioritize certain types of internet traffic and block access to services and websites. Hosting companies store the websites, files, and documents we share and make them available to the world. These companies "govern" our online social lives. They don't govern in the way that governments do, through binding laws and armed police, which means we shouldn't hold them to the same standards as governments. But their rules do influence how we communicate with each other, what we can say, and what information is available for us to see. We don't currently have any useful ways to think about how they govern or how we should limit their power.

This is a book about the future of our democracies and shared social spaces. Governments in countries across the world are trying to regulate internet companies. Governments will inevitably continue to try to make them responsible for removing hate speech or preventing foreign governments from interfering in elections or reducing abuse and bullying. Unfortunately, these kinds of laws often create new problems because they focus on various questions about content and not the *processes* of governing how users behave.

The core point of this book is that process matters. These challenges of governance are *constitutional* problems – in the sense of rules that set out how

our shared social spaces are *constituted* and how decisions that affect our lives are made.

For several years, pressure has been mounting steadily for powerful technology companies to wield their power over us more responsibly. We are now at a constitutional moment, a time of profound potential change, where we all have an opportunity to demand more from those who rule over our digital lives. Sir Tim Berners Lee, inventor of the World Wide Web, has called for a Magna Carta for the digital age. The metaphor is an excellent one: In 1215, the Magna Carta marked an historic turning point when the barons of England demanded legal protection from the king's tyranny. It was a declaration that the king was not above the law – that his power had to be exercised in a way that respected the fundamental rights of his subjects. Now, many people think that we too deserve better from our digital rulers.

This book takes seriously the challenge of making the decisions of technology companies more legitimate: more fair, more predictable, and more accountable. Ultimately, I argue that we need a new constitutionalism – a new way of thinking about the power that technology companies wield and the discretion they exercise over our lives. To constitutionalize power means to impose limits on how rules are made and enforced. Constitutionalism is the difference between lawlessness and a system of rules that are fairly, equally, and predictably applied. We should expect the technology companies that rule over us to take on the hard work, now, to develop their own constitutional protections that can help ensure that *our* rights are protected.

With this book I hope to provide a guide to what more legitimate digital governance might look like. The pressure to regulate is strong, and laws are being implemented around the world that will impose new obligations on technology companies. Not all of these laws are well designed, and some even try to enlist tech companies in illegitimate spying and censorship on behalf of governments. Meanwhile, many of the people in the major tech companies are now working hard to improve how they make decisions, and some companies are realizing that it is best if this sort of change comes from within. This book outlines how tech companies can improve their own systems, how governments can enact better laws, and how we can all work to hold power to account. Real change will require the active participation of a broad range of civil society groups, activists, journalists, academics, and regulators. It will be hard work and require many difficult public debates with no easy answers, but there is a great deal at stake. For those who believe in a vibrant, flourishing, competitive, and innovative internet that is governed fairly and accountably, we have an opportunity and an obligation to work together to develop a new constitutionalism.