DOI:10.1145/3319077

James Grimmelmann

Law and Technology
Continuity and Change in Internet Law

The fundamentals of the field of Internet law have remained consistent, but details have evolved in response to technological innovation.

This is my first column as editor for *Communications*' Law and Technology column. I am taking over from the very capable Stefan Bechtold, who established the column in its current form and imbued it with his high standards of rigor, relevance, and readability. I thought I might mark this transition with some historical reflections on how the field of Internet law has changed over the last few decades, and what has stayed the same.

Start with the continuity. The basic issues around intellectual property rights in software have been the same for a very long time. In 2014, the U.S. Supreme Court expressed serious skepticism about patents to "do X on a computer" and a federal appeals court allowed Oracle to assert copyright in the Java APIs. Neither issue is new. The Supreme Court was just as skeptical about software patents in 1972 and 1978, and a different federal appeals court held in 1995 that Lotus 1-2-3's macro interface was uncopyrightable.

Modern encryption controversies would look very familiar to a 1990s technology policy wonk who lived through the Clinton Administration's failed attempt to impose a key escrow scheme that would have enabled government wiretapping of encrypted communications. Can the government force hardware vendors to make unlockable devices? Can criminal suspects be forced to disclose their passwords? Do the police need a warrant to search a computer? Can government hackers break into computers remotely? All of these controversies are in the headlines again.

Similarly, today's legal disputes over network neutrality reflect the definitions Congress used in the Telecommunications Act of 1996. While Congress didn't quite anticipate the Internet, the distinction it drew between "telecommunications" and "information" services was rooted in previous regulation of early pre-Internet online services and in many decades of telephone regulation. Today's networking technology is new, but the debates over networks, monopoly, and nondiscrimination are not.

Everything old is also new again with cryptocurrencies. People have hoped or feared for years that strong cryptography and a global network would make it impossible for governments to control the flow of money. There is a direct line from 1990s-era cypherpunk crypto-anarchism and experiments with digital cash to Bitcoin and blockchains. The regulatory disputes are almost exactly the ones that technologists and lawyers anticipated two decades ago. They just took a little longer to arrive than expected.

In other ways, things look very different today. One dominant idea of the early days of Internet law was that the Internet was a genuinely new place free from government power. As John Perry Barlow wrote in his famous 1996 "Declaration of the Independence of Cyberspace": "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. ... You have no sovereignty where we gather. ... Cyberspace does not lie within your borders."

If there was a moment that this

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

Matrix-esque vision was definitively unplugged, it was probably the 2003 decision in *Intel v. Hamidi*. Intel tried to argue that its email servers were a virtual, inviolate space—so that a disgruntled ex-employee who sent email messages to current employees was engaged in the equivalent of breaking into Intel buildings and hijacking its mail carts. The court had no interest in the cyber-spatial metaphor. Instead, it focused on more down-to-earth matters: Intel's servers were not damaged or knocked offline.

"Cyberspace" turned out not to be a good description of how people use the Internet or what they want from it. Most Internet lawsuits involve familiar real-world problems—ugly divorces, workplace harassment, frauds and scams, and an endless parade of drug deals—that have spilled over onto cellphones, Facebook pages, and other digital platforms.

Internet law has fully embraced the idea that the Internet matters, not because it is somewhere new for people to go, but because it is everywhere that people already are. Courts have held that websites are "places of public accommodation" that must be made accessible to the disabled, just as physical stores are. And local regulators are mostly winning their claims that sharing-economy companies like Uber, Airbnb, and Bird are operating in their cities and must comply with zoning and licensing laws.

Indeed, in the story of governments versus the Internet, governments seem to have the upper hand for now. The Securities and Exchange Commission regularly shuts down fraudulent or unregistered initial coin offerings. The European Union is increasingly confident in its ability to regulate the Internet to protect its vision of its citizens' welfare and the common good, as with its recently enacted privacy law, the General Data Protection Regulation. And China has quite successfully imposed extensive filtering and surveillance on its domestic portions of the Internet.

A second shift in Internet law is the waning of the file-sharing wars. The battle lines were drawn in the 1990s, with a series of policy battles that culminated in the U.S. with the passage of the Digital Millennium Copyright Act of 1998 (DMCA). Section 512 of the DMCA created a "notice and takedown" system under which content hosts are not liable for infringing user uploads—but only so long as they respond "expeditiously to remove" those uploads when they receive notice from the copyright owner. Section 1201 of the DMCA made it illegal to disable digital rights management (DRM) technology that limits access to copyrighted works. Both were deeply controversial.

Fighting broke out in earnest in 1999 when numerous record companies sued Napster, eventually forcing it to shut down. Movie studios, photographers, book publishers, and other copyright owners filed lawsuits against file-sharing services, Web hosts, hardware makers, search engines, videogame modders, and the creators of DRM-removing software—as well as against less likely targets like replacement toner cartridges and third-party garage-door openers. And this is to say nothing of the many thousands of

suits against individual uploaders and downloaders (often filed in the hope of extracting a quick settlement).

The initial ferocity of these disputes has faded. There are still some large copyright lawsuits, and some raising major legal issues. (The record company BMG's suit against Cox Communications, an Internet service provider, for not cutting off service to copyright infringers, is an example of both.) There is, however, less of a sense that the future of either content creation or technological innovation is at stake. Instead, the Internet has settled into an uneasy detente: many copyright owners and technologists have moved on to other fights.

One reason is that the basic legal compromises in the DMCA have proven surprisingly durable. Copyright owners have not been able to force content hosts to do significantly more than the notice-and-takedown rules of Section 512 require (Viacom lost its lawsuit against YouTube on this point), but they have generally been able to keep them from doing significantly less, either. "Graduated response" or "three strikes" schemes, which would force ISPs to cut off service to unrepentant infringers, have been tried around the world and have mostly failed, but voluntary algorithmic filtering of uploads, like YouTube's ContentID, may be here to stay.

Another reason is that the courts have also been increasingly aware of the value created by innovative digital uses of media. The Authors Guild's suits against Google and its library partners ended with resounding judicial declarations that scanning books to make them searchable and accessible to the blind is protected as legal "fair use," opening the door to large-scale machine learning using copyrighted works. Search engines, plagiarism checkers, video remixers, and meme-makers have generally been blessed by the courts. Although the creators of second-generation decentralized file-sharing services like Grokster and Morpheus were successfully sued for inducing users to infringe, BitTorrent has not met a similar fate.

And finally, the rise of downloadable media and subscription streaming services has created a new and apparently stable revenue stream. Even where pirated alternatives are readily available, many people seem perfectly content to pay for Hulu and Spotify subscriptions. Copyright owners no longer fear they must hunt down every last infringing upload: they usually focus their attention on the most egregious cases.

Copyright owners no longer fear they must hunt down every last infringing upload: they usually focus their attention on the most egregious cases.

In both of these domains, technology policy has gone from alarm to acceptance. With jurisdiction, society asserted its control over the Internet; with copyright, society learned to live with it. In a third domain, however, the trend is in the other direction: from comfort to concern.

Early online-speech fights were about governments' ham-handed attempts to limit access to pornography. For example the Communications Decency Act (CDA) of 1996, which made it illegal to post "indecent" but legal-for-adults material anywhere online that a child could see it, was obviously unconstitutional. The Supreme Court struck it down in 1997.

The CDA also contained an immunity, Section 230, for Internet intermediaries. Unlike Section 512 for copyright, which applies only if the intermediary responds to takedown requests, Section 230 is nearly absolute. Intermediaries are immune if they leave up harmful content; they are immune if they take it down.

Section 230 was justified in terms of giving websites, search engines, and other such intermediaries the ability to be "good Samaritans" in developing their own content policies. Without it, they feared that if they made any attempt to enforce policies of truthfulness, decency, or community standards, they would be tagged and held liable for all of the harmful content they did not catch. Early cases showed Section 230's obvious value in enabling platforms like AOL and MySpace to host a huge range of user-generated content without the fear of crippling liability.

In the years since, many lawyers have come to think that Section 230 goes too far. In their view, the absolute immunity gives websites too little incentive to care when bad actors weaponize their platforms. They think, for example, that Twitter might do a better job of preventing neo-Nazis from making death threats against Jewish users if it faced any legal consequences for failing to respond. Other sites, like 4chan and Gab, have been accused of affirmatively fostering toxic cultures in which harmful and blatantly illegal conspiracies are birthed and allowed to grow. Proponents of Section 230 respond that with a weaker immunity, platforms might go to the other extreme, taking down users' speech at the slightest suggestion of controversy.

These debates are mirrored in other debates about free speech online. What counts as a "threat" of harm when users are separated by thousands of miles and the speaker is pseudonymous? Is a coordinated campaign of nasty tweets actionable harassment? How should bullying laws and disciplinary policies developed to deal with the schoolyard be adapted to social media?

Online speech law, which previously embodied a confident pro-speech consensus that the Internet was all bark and no bite, is going through a distinct crisis of faith. Harassment and abuse have become inescapable parts of online life, particularly for women and members of vulnerable groups. It is not yet clear what path forward the legal system will take, but online speech is becoming one of the defining legal issues of our time. C

James Grimmelmann (james.grimmelmann@cornell.edu) is a law professor at Cornell Tech and Cornell Law School, New York, NY, USA.