**INFORMATION BRIEF**
**Research Department**
**Minnesota House of Representatives**
600 State Office Building
St. Paul, MN 55155

Mary Mullen, Legislative Analyst
651-296-9253

May 2018

# The Internet and Public Policy: Challenges and Policy Considerations for State Regulation

This brief is one of a series of publications on public policy and the Internet, with special attention to the laws and public policies of the state of Minnesota.

There is some debate as to if and how the Internet should be regulated. Some states have enacted laws related to the Internet, but there are challenges for states when they attempt to regulate the Internet. In particular, varying state regulation has resulted in a patchwork of state laws. Additionally, state are limited by federal preemption and constitutional issues. This brief outlines the challenges facing the state, when laying its interests against the global phenomenon of the Internet.

## Contents

### *About The Internet and Public Policy Series*

The Internet is a worldwide communication web created through technology, hardware and software, and human use patterns, which are shaped by mores, customs, and occasionally laws. States have their own roles within the larger national and international network that is the Internet. The challenge for policymakers is that the Internet itself is malleable, and no static definition can capture its breadth and changing uses.

This series of information briefs isolates discreet policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. See the list at the end of this document for other titles in this series.

# Theories of Internet Regulation

Scholars, computer programmers, politicians, lawyers, and many others have weighed in on whether or not the Internet should be regulated and how that regulation should occur. Some have argued that regulation is most appropriate from an international approach, often called transnational governance, and is the best route to uniform policy. Others still believe that the laws of individual nations can and should be applied to Internet users and providers. It has been argued that market forces or computer software and hardware designs will transform, and in a sense, regulate the Internet. Prominent Internet theorists and lawyers have discussed each of these models for regulation, while politicians at the local, state, national, and international level continue to disagree on who should regulate the Internet and how.[1]

Internet law in the United States has largely been dictated by federal legislation and regulation by federal agencies. The discussion has been focused on whether or not the Internet should be regulated as a utility or as an information service. The Federal Communications Commission (FCC) is the center of discussion over Internet policy and the debate about "net neutrality"—which is the position that Internet traffic should be treated neutrally and have no content-based restrictions. Ongoing actions at the federal level to change privacy policies and to deregulate have caused state legislatures to look at Internet regulation more closely.[2]

While the debate continues over federal regulation of service providers, new and evolving individual and corporate activities—cultural, social, political, and economic—fall into various legal gray areas. These activities have been traditionally regulated at multiple levels: federal, state, and local. Existing laws that apply to social and commercial interactions have struggled to fit with new ways of doing business online and the new crimes and torts that occur in cyberspace.

# State Internet Regulation Trends

Over the last three years, there has been a drastic rise in the number of state laws creating new torts, addressing civil liability, regulating property transfers, and criminalizing behavior in cyberspace. “Cybertorts” and “cybercrime” are a growing area of law, as are laws designed to protect consumer privacy from changing technology. Federal and state laws address new behaviors that occur on the Internet in a way that simply could not occur in the brick-and-mortar world. States have contemplated and passed legislation related to evolving technologies and Internet culture in a variety of different areas.

- Illinois passed the Biometric Information Privacy Act in 2008. The law requires companies using facial recognition or other biometric indicators to get the user’s consent before activating the software. A class action lawsuit against Facebook has been filed under the new law.[3]

- California legislators passed a student data bill, the Student Online Personal Information Protection Act, which prohibits companies whose websites or applications are primarily used by K-12 programs from creating commercial profiles or sending targeted advertising to students or their parents.[4]

- More than 35 states have passed laws making “revenge porn” a crime, and many of those states have also provided for civil remedies, making the publication of images without the consent of the person depicted a new form of harassment and actionable in some cases for civil penalties and damages.

- The Revised Uniform Fiduciary Access to Digital Assets Act (UFADAA) has been passed by 38 states, creating parameters for access to digital accounts and assets held by a person who is incapacitated or deceased and clarifying the law for access that was otherwise prohibited.[5]

- More than a dozen states introduced bills to protect consumer privacy from Internet service providers, requiring consent before the broadband or Internet service provider collected information or sent targeted advertising to customers.[6]

# Challenges to State Internet Regulations

States traditionally have the police power to regulate crime and the regulatory authority over local commerce, and therefore, have a vested interest in controlling Internet activity, despite legal and practical challenges of implementing regulations on the international system that facilitates these activities. Nearly 20 years ago, law professor Steven Salbu addressed the role and interests of individual states in regulating individual and corporate activities on the Internet in the *Harvard Journal of Law and Technology*, where he noted, "State interests are undiminished by the medium shifts."[7] While it may seem curious that states did not act on these interests until recently, there are numerous legal hurdles to imposing those police powers on the borderless Internet. Only after pressure from individual citizens and interest groups emerged and federal action became a distant hope, did state legislatures begin to pass legislation to address new harms brought about by widespread Internet use.

## Patchwork of State Laws and Jurisdiction

The arguments against state laws regulating the Internet are strong. A lack of uniformity in a patchwork of state legislation would be confusing if not impossible for companies and websites to comply with and may inhibit the growth and "borderlessness" of the Internet. There are also other legal concepts in American law that complicate the ability of states to regulate Internet behavior. The reach of a state court's jurisdiction, along with the three constitutional principles—the dormant Commerce Clause, federal preemption, and the First Amendment right to free speech—have constrained state's ability to act on their inherent police powers.

States generally have jurisdiction over the people, property, and companies that are located or doing business within the state. Each state has a long-arm statute allowing it to reach some people and companies outside of the state's borders—but this is limited by the Due Process Clause in the Fourteenth Amendment to the U.S. Constitution, which provides that the state courts' exercise of personal jurisdiction over nonresidents must require certain minimum contacts so that the exercise of jurisdiction does not violate traditional notions of fair play and substantial justice. Jurisdiction is another substantial complication in the ability of states to pass laws regulating Internet conduct, which may or may not occur within their borders, and to enforce the statutes that are passed against anyone outside of the state.

## Preemption

Another limitation for state action is the constitutional principal of federal preemption. This legal principle is based on the Supremacy Clause of the U.S. Constitution, which states that federal law is the supreme law of the United States, and where Congress has spoken, the states cannot act. There can be explicit preemption—that is, a federal statute can say that states may not pass laws in a certain area—and also implied preemption, which occurs when the federal government has acted in such a way that it is clear the federal law was intended to preempt any state action (field preemption) or where a state law is in conflict with a federal law (conflict preemption). There are a number of federal laws addressing criminal and civil liability related to Internet behavior, and which thereby complicate state action.

The following are a few notable federal laws that expressly preempt state action or cause the potential for a challenge to state action based on preemption.

- The Federal Trade Commission (FTC) has federal legislative authority to look at unfair and deceptive trade practices. The same unfair billing practices, pyramid schemes, and fraudulent advertising that occur in the brick-and-mortar world also occur on the Internet. The FTC also deals with the cyberspace issues of spyware, online endorsements, and pop-up ads. These types of consumer protections continue to evolve at the federal level.

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), requires commercial e-mails to contain certain information making it clear that the e-mail message is an advertisement or solicitation for sales and allowing the opportunity to "unsubscribe" to further e-mails.[8] The law also requires the e-mail to contain a physical address for the entity sending the e-mail.[9] CAN-SPAM has limited provisions for private civil actions for consumers, Internet service providers, and state attorneys general; consequently, the FTC does most of the enforcement for this federal law. The act also explicitly preempts states' antispam laws.[10]

- The Electronics Communications Privacy Act (1986), which prohibits the interception of any wire, oral, or electronic communication in the absence of consent, business necessity, or a warrant. The law was amended to include electronic communication, including e-mail or other Internet-related communications and making it a violation to intercept, disclose intercepted mail, or use the content of that intercepted mail. (18 U.S.C. § 2511, (1) (A-D). Even though the federal government has acted to legislate in this area, states' wiretap statutes, which have been extended to e-mail, have been allowed to build on those protections.

- The Criminal Fraud and Abuse Act is notable for creating crimes that were specific to invention and use of computers. The law addresses trespassing to government computers, accessing a computer to defraud someone, damaging another person's computer or data, and trafficking in passwords to defraud.[11]

These federal laws create a framework for Internet law in the United States and also create issues related to federal preemption. But as the day-to-day activities of most Americans become entirely intertwined with the Internet, the federal laws are outpaced by crimes and commercial activities that had not been anticipated by the existing legislation. States cite Congress's subsequent failure to act as an impetus for moving forward with legislation, despite potential legal challenges based on federal preemption.

## The Commerce Clause

Because only Congress has the power to regulate commerce between the states,[12] states cannot act to pass or enforce legislation that would materially burden or discriminate against interstate commerce, a principal known as the "dormant Commerce Clause." While borderless Internet changed the way people do business, it did not change states' interest in wanting to protect and regulate commerce. One of the first and most formative decisions in this area was *American Library Association v. Pataki*.[13] The New York law was similar to the federal Communications

Decency Act (CDA) in that it attempted to prevent offensive and sexual content from reaching minors, but it went beyond the CDA and did so in a manner that opponents—including free speech advocates and libraries—argued violated both the First Amendment right to free speech and the Commerce Clause.

In 1997, the federal district court in the *Pataki* decision "invalidated the New York dissemination law on all three grounds which the Supreme Court has established as the basis for dormant Commerce Clause violations: as an excessive burden on commerce with little local benefit, as an impermissible extraterritorial regulation, and as a regulation introducing the possibility for inconsistent legislation."[14] The *Pataki* decision discusses the difficulties of state regulation on a borderless Internet:

> The New York Act, therefore, cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist. No user could reliably restrict her communications only to New York recipients. Moreover, no user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a Web site, receiving a mail exploder message or a newsgroup posting, or participating in a chat room. Similarly, a user has no way to ensure that an e-mail does not pass through New York even if the ultimate recipient is not located there, or that a message never leaves New York even if both sender and recipient are located there.[15]

Three years after *Pataki*, Jack Goldsmith and Alan Sykes, law professors at the University of Chicago Law School, wrote their law review article, "The Internet and the Dormant Commerce Clause." The article discusses the *Pataki* decision before presenting an interpretation of the dormant Commerce Clause that would allow for some state regulation of the Internet.[16] They examine the final comments of the Court, which indicate that Internet regulation must occur at the national level: "[T]he Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether."[17] They go on to point out how many other federal circuit courts have followed the *Pataki* decision in both pornography regulations and antispam cases. They fear the repercussions could extend widely and an interpretation of the dormant Commerce Clause that prevents any state regulation of Internet conduct would dramatically limits states' police powers.

> [T]he dormant commerce clause argument, if accepted, threatens to invalidate nearly every state regulation of Internet communications. . . This explains why the dormant commerce clause has been called "a nuclear bomb of a legal theory" against state Internet regulations. *(citation omitted)* . . . But the logic of *Pataki* and the cases that follow its reasoning extends to state anti-gambling laws, computer crime laws, various consumer protection laws, libel laws, licensing laws, and much more.[18]

Other federal circuit courts have reached similar conclusions, finding that the legitimate state interests are barred by the dormant Commerce Clause, and just as often, the First Amendment

right to free speech.[19] Subsequently, states have been hesitant to act, despite a perceived need by the public for greater consumer and privacy protections.

Some federal courts have followed the *Pataki* decision. In *American Booksellers Foundation v. Dean,*[20] the court deemed the Vermont dissemination statute violated the dormant Commerce Clause since the Internet has no geographic boundaries, which makes it unconstitutional for states to regulate Internet activities without projecting it onto other states. Similarly, *Southeast Booksellers Ass'n v. McMaster*[21] identified the South Carolina statute as invalid since it placed undue burden on interstate commerce in comparison to the local benefit conferred. The issue is that Internet users cannot practically determine what geographic locations will be impacted by their actions and it is unfair for the states to impose their regulation on other states in such murky waters.

However, some courts have moved in a different direction than the *Pataki* decision. The Supreme Court of Florida found in *Simmons v. State*[22] that the state's transmission statute was distinctly different from those under *Pataki,* which applied to all Internet disseminations. The Florida statute only applied to e-mails. The court found the Florida statute did not violate the dormant Commerce Clause because the geographic reach of the statute is only to Florida residents. A person sending an e-mail with harmful material to minors must know or believe the specific recipient is a minor *in Florida*. Determining that any effects this statute has on interstate commerce are merely incidental and that the law is not overly burdensome to interstate commerce.

Similar to the *Simmons* case, laws that have a strong policing power specifically against the transmission of pornographic materials to minors have been upheld despite dormant Commerce Clause challenges in the courts. In *People v. Hsu,*[23] *Hatch v. Superior Court,*[24] *People v. Foley,*[25] and *People v. Barrows,*[26] the courts found that intentionally transmitting harmful materials to minors with the intent of sexual conduct does not constitute economic activity that would traditionally require protection under the Commerce Clause. As a result, such activity does not burden interstate commerce contrary to the *Pataki* findings. The *Hatch* court confirmed there is no protection under the dormant Commerce Clause for the narrow class of adults intending to engage in sex with minors through Internet communications. It seems that most statutes challenged after *Pataki* were narrower in scope and did not apply to all general information dissemination over the Internet, making it easier for courts to find legitimate state interests outweigh potential burdens on interstate commerce.

In *Ford Motor Co. v. Tex. DOT,*[27] the Fifth Circuit found that incidental regulation of Internet activities does not violate the Commerce Clause. This court found that *Pataki* could not be applied since it would permit corporations and individuals to avoid constitutional state laws simply by linking any transaction to the Internet. The challenged statute sought to prohibit *all* forms of marketing and sales, not just those conducted over the Internet. Since the statute merely had an incidental effect on interstate activities and would not impact the sale of out-of-state vehicles, it was upheld. The conferred in-state benefits outweighed the potential burden on commerce since it meant to prevent against unfair practices.

Various other cases had similar holdings, including *Ferguson v. Friendfinders,*[28] *Miracle, LLC v. First Choice Internet, Inc.,*[29] *Washington v. Heckel,*[30] and *People v. Lipsitz.*[31] These cases uphold

state antispam statutes. In comparison to *Pataki*, the valid statutes are those regarding e-mail regulation not broad Internet regulation. The courts have consistently identified that e-mails can be targeted towards specific geographic areas whereas Internet posts are easily accessible to any Internet user in any geographic location. These holdings suggest a general trend towards affirming the more specific regulatory statutes that are traceable to geographic locations and invalidating those that are broader in scope due to the higher likelihood they burden interstate commerce. Minnesota courts and the Eighth Circuit Court of Appeals have found both that computers connected to the Internet are likely to be considered engaged in interstate commerce, and also found that state laws regulating commercial activity occurring in Minnesota may be regulated despite the use of the Internet to facilitate the activity.[32]

## The First Amendment Right to Free Speech

The right to free speech has been used to challenge a number of "content"-based restrictions related to information distributed over the Internet.[33] The U.S. Constitution has been interpreted to allow "time, place, and manner" restrictions on speech that are content neutral, but the general legal jurisprudence in the American system favors the freedom of speech—even when it is offensive, embarrassing, or adversarial—over the privacy concerns of a given citizen, company, or public persona. This is contrary to most European countries, which tend to provide greater privacy protections and which often results in policy and legal decisions that are contrary to the American system. If a government restriction on speech is directed at a certain type of speech, which means it is not content neutral, then the question is whether or not the speech is one of the types the court has allowed to be limited. Some of the areas the court has found that can be limited include: "false statements of fact, obscenity, commercial advertising, fighting words, express incitement of unlawful conduct, and threats, that do not appreciably further the central purposes of the First Amendment."[34]

Courts look at whether the state interest justifies the restriction and if it does not fall into the category of speech that the court has deemed justifiably restricted, then a law restricting speech will not be upheld unless "it is necessary to prevent a clear and present danger of a very grave harm."[35] Generally though, none of this prevents people from making disparaging, embarrassing, or offensive remarks on the Internet; this creates a public policy issue when the speech may be deemed as an invasion of privacy, aimed at facilitating harassment, or promoting hate-speech. Traditional laws designed to regulate publication, commercial advertisement, and daily communication are ineffective when applied to the Internet with its inherent opportunities for self-publication, anonymity, and the ability to reach a large public audience—speech on the Internet happens in fundamentally different ways than it ever has before. But both state legislatures and Congress have been reluctant to act where a First Amendment challenge may come up against an attempt to curb harassing speech or exploitative commercial behavior.

# Conclusion

There is a federal framework for Internet regulation, with emerging trends in state legislation related to online social and commercial activity. The challenges outlined in this brief highlight some of the pushback to state legislative proposals. It is likely that if there is little federal action on Internet regulation, or if federal policy choices promote deregulation, that states will continue to look try to protect Internet users and online consumers based on the demands of local constituencies and regional public policy considerations.

## *Other Works in the Series*

This series of information briefs isolates discreet policy issues and the ways in which specific Internet issues provide choices for the Minnesota marketplace and for lawmakers. The following publications are part of the Internet and Public Policy series:

- Privacy and consumer protection
- Cybertorts and property rights online
- Criminal activity on the Internet
- Jurisdiction and procedures in Internet law cases
- Federal Internet laws
- State and federal accessibility laws

There may be more topics added, as needed. A special attempt will be made to keep all of these pieces up to date, but the pace of change may prove challenging.

**ENDNOTES**

[1] See Michael L. Rustad, *Global Internet Law*, St. Paul: West Academic Publishing, 2014, pp. 57-100.

[2] Joshua Brustein, "What Happens When States Have Their Own Net Neutrality Rules," *Bloomberg*, Jan. 5, 2018, https://www.bloomberg.com/news/articles/2018-01-05/what-happens-when-states-have-their-own-net-neutrality-rules.

[3] Conor Dougherty, "Tech Companies Take Their Legislative Concerns to the States," *New York Times*, May 27, 2016.

[4] A.B. 1442, California Code § 49073.6, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1442.

[5] Fiduciary Access to Digital Assets Act, Revised (2015), http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015).

[6] National Conference of State Legislatures, *Privacy Legislation Related to Internet Service Providers*, Jan. 2, 2018, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-Internet-service-providers.aspx.

[7] Steven R Salbu, "Who Should Govern the Internet: Monitoring and Supporting a New Frontier," *Harvard Journal of Law and Technology* Vol. 11, No. 2 (Winter 1998), pp. 430-480.

[8] Rustad, at 331.

[9] Id.

[10] Rustad, at 334; See also *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040 (9th Cir. 2009).

[11] 18 U.S.C. § 1030.

[12] U.S. Const. art. 1, § 8, cl. 3.

[13] 969 F. Supp. 160 (S.D.N.Y. 1997).

[14] Chin Pann, "The Dormant Commerce Clause and State Regulation of the Internet: Are Laws Protecting Minors from Sexual Predators Constitutionally Different than Those Protecting Minors from Sexually Explicit Materials?" *Duke Law & Technology Review* No. 8 (2005).

[15] *American Libraries Association v. Pataki*, 969 F. Supp. 160 (S.D.N.Y 1997).

[16] Jack Goldsmith and Alan Sykes, "The Internet and the Dormant Commerce Clause" *John M. Olin Law & Economics Working Paper No. 105 (2D Series)*, The University of Chicago Law School (2000).

[17] Id.

[18] Id.

[19] Ibid. Pann.

[20] 342 F.3d 96 (2d Cir. 2003).

[21] 371 F. Supp. 2d 773 (D.S.C. 2005).

[22] 944 So. 2d 317 (Fla. 2006).

[23] 82 Cal. App. 4th 976, 99 Cal.Rptr.2d 184, 189 (Cal. Ct. App. 2000).

[24] 80 Cal. App. 4th 170, 94 Cal.Rptr.2d 453 (Cal. Ct. App. 2000).

[25] 94 N.Y.2d 668, 731 N.E.2d 123, 709 N.Y.S.2d 467 (N.Y. 2000). This case was distinguished from *Pataki* because an additional luring prong was challenged regarding intent of the sender. In other words, if the sender intended to send harmful material to a minor, then the sender may or should have known where the minor was located.

[26] 273 A.D.2d 246, 709 N.Y.S.2d 573 (N.Y. App. Div. 2000).

[27] 264 F.3d 493 (5th Cir. 2001).

[28] 94 Cal. App. 4th 1255, 115 Cal. Rptr. 2d 258 (Cal. Ct. App. 2002). This court found a state law regulating unsolicited e-mails only applied to California residents that received the e-mails in the state. It did not regulate conduct outside the state.

[29] 166 Md. App. 481, 525-26, 890 A.2d 818 (Md. Ct. Spec. App. 2006). The court found that regulating transmissions of e-mails containing false information applied only to transactions involving Maryland devices or an e-mail address in the state.

[30] 143 Wn.2d 824, 839-40, 24 P.3d 404 (Wash. 2001). This court found similarly as *Miracle LLC*, in that the statute only regulated disseminated information from a Washington computer or to a Washington e-mail address.

[31] 174 Misc. 2d 571, 663 N.Y.S.2d 468, 475 (N.Y. App. Div. 1997). The court validated the statute for consumer protection in regulating only local, online business conduct.

[32] In *State v. Integrity Advance, LLC*, 870 N.W.2d 90 (Minn. 2015), the Minnesota Supreme Court ruled that the Commerce Clause does not preclude Minnesota from applying its payday lending law to loans to Minnesota residents made over the Internet from a company in Delaware. The Minnesota law only applies to Minnesota residents in the state and the effect is not "wholly extraterritorial." In *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007), the defendant challenged the determination that the computer system he was charged with disrupting under the Computer Fraud and Abuse Act was not a part of interstate commerce. The court concluded that the Internet is an instrumentality and channel of interstate commerce since it is part of the international network of interconnected computers. Therefore, once a computer is used in interstate communication, such as sending and

receiving communications between states, Congress can protect it. Similarly, *United States v. Giboney*, 863 F.3d 1022 (8th Cir. 2017), held that applying federal child pornography statutes to the defendant based on his use of the Internet to receive and transport child pornography did not violate the Commerce Clause since the Internet is an instrumentality and channel of interstate commerce.

[33] U.S. Const. amend. I, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

[34] Geoffrey R. Stone, "Privacy, the First Amendment, and the Internet," *The Offensive Internet*, Eds. Saul Levmore and Martha C. Nussbaum, Harvard University Press (2012).

[35] Id.