Agenda Internacional
Año XXV N° 36, 2018, pp. 113-131
ISSN 1027-6750

Recent Developments in U.S. Cyberlaw

David P. Stewart*

Abstract

This article surveys recent developments in domestic U.S. law relating to key issues in Internet (or Cyber) Law. Rapid technological advances have posed serious challenges to traditional legal doctrines and approaches relating to (for example) fundamental issues of privacy, freedom of speech and expression, and protection against unwarranted governmental intrusion. How has the law responded to these key challenges? Since the United States lacks a comprehensive legislative structure addressing these issues, most of the recent developments have come in the form of judicial decisions.

Keywords: Cyberlaw, Internet Regulation, Freedom of Access, Privacy, Data Protection, Freedom of Speech and Expression, Right to Anonymity, Law Enforcement.

Desarrollos recientes sobre *Cyberlaw* (derecho de la Internet) en los EE.UU.

Resumen

Este artículo analiza los desarrollos recientes en la legislación interna de los EE.UU. relacionados con cuestiones clave en el Derecho de la Internet (o *Cyberlaw*). Los rápidos avances tecnológicos han planteado serios desafíos a las doctrinas y enfoques legales tradicionales relacionados (por ejemplo) con cuestiones fundamentales sobre privacidad, libertad de expresión, y la protección contra la intromisión gubernamental injustificada. ¿Cómo ha respondido la ley a estos desafíos clave? Dado que Estados Unidos carece de una estructura legislativa integral que aborde estos temas, la mayoría de los recientes desarrollos se han presentado en forma de decisiones judiciales.

Palabras clave: Cyberlaw, regulación de Internet, libertad de acceso, privacidad, protección de datos, libertad de expresión, derecho al anonimato, aplicación de la ley.

* Professor from Practice, Georgetown University Law Center, Washington, D.C. Email: stewartd@law.georgetown.edu. Former member, Inter-American Juridical Committee (2008-2016); President, American Branch, International Law Association.

https://doi.org/10.18800/agenda.201801.006

Significant advancements in technology have always presented legal challenges, but perhaps none as difficult as those created by the rapid revolution in information exchange and data sharing on the Internet. The legislatures and courts in the United States, as in other countries, have struggled to respond by applying traditional principles to new situations. This article provides an overview of relevant domestic law and discusses some of the most important recent developments in and challenges to that law.

The term «Internet Law» (or «Cyberlaw» as it is sometimes called) refers broadly to the legal issues related to the regulation and use of the Internet for a wide variety of purposes (private, commercial, governmental). It is less a distinct field of law than a conglomeration of rules from other areas (for example, contract, tort, intellectual property, law enforcement, etc.) in their application to new situations. But it also encompasses fundamental questions of individual rights. Consider, by way of example, the following questions recently addressed by U.S. courts.

- Do individuals have a right to access the Internet freely? Put differently, when —if ever— can the government properly restrict such access? In a recent decision, the U.S. Supreme Court struck down a North Carolina statute that prohibited convicted sex offenders—including those no longer on probation, parole, or supervised release—from accessing social media sites on the Internet. The statute made it a felony for a registered sex offender to access a commercial social networking Web site when the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages. The Court held that the law violated the First Amendment to the U.S. Constitution because it was «not narrowly tailored to serve the State's legitimate interest in protecting minors from sexual abuse.»[1]
- Can the government compel disclosure of cell phone usage in order to determine the past location of criminal suspects? The question is whether police officers must first obtain prior judicial permission («warrants») to obtain data on the past locations of criminal suspects based upon cellphone use. Under the Fourth Amendment to the U.S. Constitution (which protects against unreasonable searches and seizures), the courts have long recognized a distinction between the *content* of personal communications (which is protected) and the *external information* («meta-data») necessary to get those communications from point

[1] Packingham v. North Carolina, U.S., 137 S.Ct. 1730 at 1734–35 (June 19, 2017). Some years earlier, the Court decided that the police generally may not, without a warrant, search digital information on a cell phone incident to an arrest. Riley v. California, U.S., 134 S.Ct. 2473 (2014). See Commonwealth v. Mauricio, 477 Mass. 588, 80 N.E.3d 318 (Sup. Jud. Ct. Mass. 2017) (applying the principles in Riley to warrantless searches of digital cameras),

A to point B (which is not protected). A lower court has said no warrant is needed, describing an «email» as «the modern-day letter» and treating the meta-data used to route internet communications (like sender and recipient addresses on an email or IP addresses) as analogous to markings on an envelope.[2] The U.S. Supreme Court recently agreed to consider the case.

- May the government prohibit «online impersonation» by criminalizing the non-consensual use of another's name (or «persona») online? A Texas statute made it a felony to create a web page on a commercial social networking site or other Internet website, using another's name without consent, with the intent to harm, defraud, intimidate, or threaten any person. The Texas court of appeals rejected a constitutional challenge to the statute, holding that although it imposes a «content-based» restriction that criminalizes a substantial amount of speech otherwise protected under the First Amendment, the statute is «content neutral» in that it does not prohibit any particular topic or viewpoint but rather seeks to address malicious usage of someone else's name or persona.[3]
- Do individuals have a right of privacy in their use of the Internet? For example, what limits (if any) exist on the ability of online service providers to «track» their users' browsing histories (websites visited) through the use of «cookies»? Do purchasers of «smart» (internet-connected) consumer devices such as television sets capable of web-based video content delivery) have «invasion of privacy» claims if they were not properly informed of the capability of such devices? Courts are currently considering such claims.[4]
- What rules apply when the government seeks disclosure – for law enforcement purposes – of an individual's personal data and information stored on-line in «the cloud»? Such data can be readily moved by the service provider and is often located in another country, sometimes in more than one country. The U.S. Supreme Court is currently considering that question in the so-called *Microsoft/Ireland* case, in which U.S. prosecutors seek to compel an Internet service provider to turn over a U.S. customer's individual's data (including emails) which is hosted in a storage facility in Ireland. Microsoft refused, arguing that the government could not lawfully issue a warrant that reaches into other countries and that the

---

[2] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), cert. granted 137 S.Ct. 2211 (June 5, 2017). In Smith v. Maryland, 442 U.S. 735 (1979), the Supreme Court ruled that installation and use of a «pen register» by a telephone company does not constitute a «search» within the meaning of the Fourth Amendment.

[3] Ex Parte Maddison, 518 S.W.3d 630 (Tex. Ct. Appeals 2017).

[4] See, e.g., In re Vizio, Inc., Consumer Privacy Litigation, 238 F.Supp.3d 1204 (C.D. Cal. 2017); In re Facebook Tracking Litigation, 263 F.Supp.3d 836 (C.D. Cal. 2017); see also In re Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3rd Cir. 2016).

> authorities would need to work through Irish authorities. The trial court ruled against Microsoft; the appellate court reversed, saying the statute must be read consistent with the presumption against extraterritoriality and therefore does not apply abroad.[5]

The Supreme Court heard oral argument in the case in late February 2018. The issue is obviously consequential. If the Court upholds the government's action, some fear that foreign governments might pass protective «data localization» laws. If it rules in favor of Microsoft, others worry that efforts to combat transnational crime will be undercut. Either way, the decision will have significant effect on rights of privacy in the digital age.

I. U.S. Legal Framework

Part of the difficulty facing U.S. courts in addressing such questions is that, unlike many other countries, the United States lacks comprehensive national legislation to regulate the Internet or the collection, storage, and use of personal data online. It also lacks a centralized enforcement authority. In consequence, many of the issues are presented to the courts in the context of litigation.

Privacy law must constantly adapt in response to technological changes in computer technology, digitized networks, and the creation of new information products as well as the need for organizations to provide their stakeholders with greater comfort and transparency relating to their information sharing and protection practices.

In the United States, the legal framework is provided by (i) constitutional requirements, (ii) a patchwork of federal and state laws and regulations, adopted over time and in response to differing situations and problems, and (iii) guidelines and principles developed by governmental agencies and industry groups that do not have the force of law, but are part of self-regulatory guidelines and frameworks that are considered «best practices.»

Constitutional Provisions

The U.S. Constitution, and in particular the First and Fourth Amendments, provides an over-arching framework for many of the issues presented by Internet usage. The First Amendment protects freedom of speech and expression;[6] the Fourth

[5] In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., 15 F.Supp.3d 466 (S.D.N.Y. 2014), rev'd 829 F.3d 197 (2d Cir. 2016), cert. granted 138 S.Ct. 356 (Mem) (2017).

[6] «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

Amendment protects against unreasonable searches and seizures.[7] Their application to access and use of the Internet, of course, is a difficult exercise in interpretation; both were written in the eighteenth century and both apply primarily to government action.

Federal Statutes

At the national level, a complex set of federal privacy-related laws regulates the collection and use of personal data in discrete (sectoral) areas. Some statutes apply specifically to activities that use personal information, such as telemarketing and commercial e-mail.[8] Others protect particular categories of information (such as financial or health information).[9] In addition, a range of «consumer protection laws prohibit various unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.[10]

No single federal department or agency exercises overall supervision over the field. The Federal Trade Commission (an independent administrative agency) issues regulations concerning privacy and takes action against privacy violators under its authority to enforce certain statutory prohibitions against «unfair or deceptive acts or practices in or affecting commerce.»[11] It also investigates and prosecute actions based

Government for a redress of grievances.» U.S. Const. amdt. I.

[7] «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause … particularly describing the place to be searched, and the persons or things to be seized.» U.S. Const. amdt. IV.

[8] For example, the Federal Privacy Act of 1974, 5 U.S.C.A. §552a, limits the personal information which may be gathered or disclosed by federal government agencies. The Video Privacy Protection Act of 1998, 18 U.S.C.A. §2710, restricts the ability of video rental or sales outlets may disclose personally identifiable information about a consumer. The Computer Fraud and Abuse Act of 1984, 18 U.S.C. §1030, prohibits unauthorized access to «protected computers» and prohibits trafficking in computer passwords. The Identity Theft Assumption and Deterrence Act of 1998, 18 U.S.C. §1028, criminalizes misuse of identification documents and «authentication features» with intent to defraud the United States. The Controlling the Assault of Non-Solicited Pornography and Marketing Act, 15 U.S.C. §§7701-7713 and 18 U.S.C. §1037, and the Telephone Consumer Protection Act, 47 U.S.C. §227 et seq., regulate the collection and use of e-mail addresses and telephone numbers, respectively.

[9] For example, the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 («GLBA»), 15 U.S.C. §§6801-6827, regulates the collection, use and disclosure of financial information collected by a financial institution such as a bank, securities firm or insurance company. It applies to non-public personal information capable of personally identifying a consumer or customer. The Fair Credit Reporting Act of 1999 («FCRA»), 15 U.S.C. §1681, applies to certain consumer reporting agencies (such as lenders and credit card companies). The Health Insurance Portability and Accountability Act of 1996 («HIPAA»), 42 U.S.C. §1301 et seq., regulates individually identifiable health and medical information and applies broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information such as health plans and health care clearinghouses.

[10] The Right to Financial Privacy Act of 1978, 12 U.S.C. §§3401 et seq., prohibits (with certain exceptions) the disclosure to government authorities of a financial-institution customer's records without that customer's consent.

[11] The Federal Trade Commission Act, 15 U.S.C. §§41-58, prohibits unfair or deceptive practices that fail to safeguard consumers' personal information. It does not regulate specific categories of data but has been applied to offline and online privacy and data security policies. The FTC is also the primary enforcer of the Children's Online Privacy

on violations of privacy rights under other laws (such as COPPA and GLBA). The Commission's administrative actions provide guidance regarding best practices with respect to companies' collection, storage, use and protection of consumers' personal information.

Three federal statutes are particularly relevant to Internet developments.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act[12] was adopted in 1986 to apply the restrictions on government interception of telephone calls to transmissions of electronic data by computer. Most importantly, it provides that any such communication made on a public channel cannot be intercepted or read by any entity without a warrant. In its current form, it protects wire, oral and electronic communications while those communications are being made are in transit, and when they are stored on computers. It applies to email and data stored electronically. However, it only protects communications made on public servers (thus excluding, for example, emails sent on an employer's system or server in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service). Moreover, it only protects emails held on a server for 180 or less; after that time, the email will be deemed to have been «abandoned» and thus a subpoena (rather than a warrant) will suffice to permit access.

The Stored Communications Act

The Stored Communications Act, enacted as part of the ECPA, protects the privacy of the contents of files stored by service providers and of records held by those providers about individual subscribers, such as subscriber name, billing records, IP addresses, etc.[13] It provides a cause of action against anyone who «intentionally accesses without authorization a facility through which an electronic communication service is provided ... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.»[14] «Electronic storage» means either «temporary, intermediate storage ... incidental to ... electronic transmission,» or «storage ... for purposes of backup protection.»[15] The

Protection Act of 1998 (COPPA), 15 U.S.C. §§6501-6506), which applies to the online collection of information from children.

[12] Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. §§ 2510-22 (ECPA) was originally an amendment to the part of the Omnibus Crime Control and Safe Streets Act of 1968 that addressed interception of «hard» telephone lines conversations. Together with the Computer Fraud and Abuse Act, 18 U.S.C. §1030, it regulates the interception of electronic communications and computer tampering.

[13] Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. §§ 2701-12.

[14] 18 U.S.C. §§ 2701(a)(1), 2707(a).

[15] §2510(17).

Act exempts, inter alia, conduct «authorized ... by the person or entity providing a wire or electronic communications service» or «by a user of that service with respect to a communication of or intended for that user.»[16]

Communications Decency Act

The Communications Decency Act of 1996 provides a broad grant of immunity to internet service providers for all claims stemming from their publication of information created by third parties. In particular, it states that «[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.»[17] An «interactive computer service» is defined as «any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet....»[18] In addition, the law states that «[n]o cause of action may be brought and no liability imposed under any State or local law that is inconsistent with this section.»[19] As a result, an individual or entity claiming to have been defamed on the internet can sue the original speaker but not the messenger.

As enacted, the statute contained two other provisions aimed at protecting minor children from harmful material on the Internet: one criminalized the «knowing» transmission of «obscene or indecent» messages to any recipient under 18 years of age, and another prohibited the «knowing» sending or displaying to a person under 18 of any message «that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs.» In 1997, the U.S. Supreme Court struck down both provisions, holding that these «indecent transmissions» and «patently offensive display» provisions violate the First Amendment.[20]

State Privacy Laws

At the sub-national level, the laws in the 50 states (as well as Puerto Rico, Guam, the Virgin Islands, etc.) now address various aspects of internet usage and information security. Most states have enacted some form of privacy legislation. Some provide protections that are very similar to those provided under federal laws (i.e., state laws regulating wiretaps and eavesdropping); others provide greater protection.

---

16 §2701(c)(1) and (2).
17 Communications Decency Act of 1996, § 509, 47 U.S.C.A. §230(c)(1).
18 47 U.S.C. §230(f)(2).
19 47 U.S.C. §230(e)(3).
20 Reno v. American Civil Liberties Union, 521 U.S 844 (1997).

Obviously, differences in state law can cause difficulties for companies that engage in business activities in a number of states.

By way of example, the California Online Privacy Protection Act requires that any operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its site or service must conspicuously post its privacy policy on its Web site, or in the case of an operator of an online service, make that policy available in the manner provided in the Act.[21] In 2015, California enacted an Electronic Communications Privacy Act that sharply limited the ability of government authorities to seek electronic communication information for law enforcement purposes. [22]

Data Breach Provisions

One peculiarity of the U.S. legal framework is that data breach requirements are set primarily by state (rather than federal) law. To date, all states (except Alabama and South Dakota) as well as the District of Columbia, Puerto Rico and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information.[23] In 2017, nine states enacted or revised security breach laws in 2017..The first such statute, adopted in California, requires any person or business that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorized person. The term «personal information» includes an individual's name when used in conjunction with other identifying elements, such as social security number, driver's license number, account number, credit or debit card number, medical or health insurance information (but not publicly available information that is lawfully made available to the general public from federal, state or local government records).[24] While the California law became a model for the legislation adopted by other states, there are variations with respect to key definitions and exceptions.

---

[21] Cal. Bus. & Prof. Code §22575.

[22] Cal. Penal Code §1546.1(b) provides that a government entity may compel the production of or access to electronic communication information from a service provider only pursuant to a duly issued warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to existing state law, «provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense, and compelling the production of or access to the information via the subpoena is not otherwise prohibited by state or federal law.»

[23] See the website of the National Conference of State Legislatures at *www.ncsl.org*.

[24] Cal. Civil Code §1798.82.

Voluntary Guidelines

In addition, industry groups have adopted voluntary (non-binding) guidelines representing agreed «best practices» in the relevant industries. For example, the advertising industry continues to develop its self-regulatory program for online behavioral advertising. This program requires members of various advertising industry trade groups to comply with the groups' guidelines for online behavioral advertising, which largely mirror the FTC's guidelines. The program includes an icon that members should place on their websites if tracking data is collected. The icon links to information about the website's data collection practices and how an individual can opt out of some online tracking. The self-regulatory program was also expanded in 2015 to the mobile environment.

International Principles and Guidelines

The United States embraces a number of widely-accepted international principles regarding privacy and including for example, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[25] the APEC Privacy Framework (2015),[26] and the Inter-American Principles on Privacy and Data Protection.[27]

II. Internet Regulation

Two recent actions by the current Administration affecting Internet regulation have stirred considerable controversy, including allegations that the Administration is protecting broadband internet service providers from greater supervision and regulation.

Broadband Internet Service Providers

The first action involved what was generally seen as a battle to impose greater regulation on broadband internet service providers. In April 2017, President Trump signed a law repealing a set of proposed privacy and data security regulations for broadband internet service providers that had been adopted by the Federal Communications Commission (FCC) in 2016. The FCC's so-called «Privacy Rule» would have required broadband ISPs to obtain customer consent before they could use and share their customers' personal information. The rules would have treated browsing history and apps usage (along with other «sensitive» personal data like Social Security numbers, information about children, and financial, financial and location data) as

[25] See http://www.oecdprivacy.org.
[26] https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.
[27] http://www.oas.org/dil/data_protection.htm.

«sensitive information» requiring a customer's «opt-in» consent. They would also have included specific data security and breach notification requirements.

The rules were opposed, however, by the broadband ISP's, because until that time they had been regulated by a different agency, the Federal Trade Commission. While the FTC has long regulated false and misleading practices, it has limited authority and in particular cannot regulate «common carriers,» which includes companies that provide a utility service. A prior decision of the FCC in 2015 (the «Open Internet Order») had effectively reclassified ISPs as common carriers, thus creating different rules for them as opposed to such non-ISP entities as Google and Facebook. Accordingly, the FCC worked to create privacy rules specifically for ISPs. The broadband providers contended, however, that this action would unfairly tilt the playing field in favor of their internet rivals.

In April 2017 President Trump signed a law nullifying the FCC's proposed privacy regulations, an action proclaimed by many as a victory for internet service providers and a blow to privacy advocates.

Net Neutrality

The second action concerned so-called «net neutrality.» The term refers to the rules governing how the Internet's infrastructure operates. More particularly, it means the principle that internet service providers may not discriminate based on user or content but must instead treat online data equally. In other words, ISP's must not block, filter, or «throttle» a user's access or give preferential treatment to one end-user or content-provide over another. Many experts consider the principle essential to free, open access to and use of the Internet.

As long ago as 2005, the FCC had adopted principles of «network neutrality» in order to «preserve the vibrant and competitive free market that presently exists for the Internet» and to «promote the continued development of the Internet» as well as advanced broadband capability In 2015, the agency classified Internet access as a «common carrier telecommunications service» (in other words, a public utility), effectively prohibiting ISP's from speeding up (or slowing down) traffic from specific websites and apps. The new rule took effect in June 2015.

The new Administration disagreed, however, and in December 2017, the FCC (under new leadership) voted to repeal the net neutrality rule. As a result the FCC plans to eliminate the rules barring internet providers from blocking or slowing down access to online content or from prioritizing their own content. Absent Congressional action, the new rules are scheduled to go into effect in April 2018.

A number of lawsuits have been filed challenging the net-neutrality repeal, including actions by tech companies (such as Mozilla) and «class actions» by the attorneys general for .more than 20 states. A number of state legislators have also introduced bills to protect net neutrality in their own states (although the FCC's order purports to prohibit the states from contradicting the federal government's approach).

III. Freedom of Access and Expression

In the absence of any general legislation governing access to and use of the Internet, questions involving governmental restrictions in this area are generally evaluated under the guarantees of the First Amendment, which broadly protects (from governmental regulation) what individuals say, what they write, and their right to communicate and interact with others in public spaces. The Internet continues to pose challenges to traditional First Amendment law. The following describes a number of recent decisions.

Right to Access the Internet

Kentucky enacted a statute prohibiting convicted sex offenders from using any social networking sites that might be used by minors (under age 18). To ensure compliance with the statute, one such individual was required to provide his probation officer with all of his email and other Internet name identities. He challenged the statute as a violation of his right to free speech. Relying on the Supreme Court's decision in *Packingham*, discussed above, the court held the statute unconstitutional because it was over-broad and effectively prohibited sex offenders from engaging in «any speech whatever on a social media website, as innocent as that speech may be.» [28]

Similarly, a parole board's decision to impose a lifetime ban on a convicted sex offender's access to a computer and the Internet was «overbroad» and «a form of banishment.» Today, the court said, «access to the Internet is considered to be a basic need and one of the most meaningful ways to participate in the essentials of everyday life.»[29]

By distinction, a federal court declined to overrule a decision by authorities in a state hospital to deny a detainee the right to access the Internet. The individual was a convicted «sexually violent predator» who had been diagnosed with mental disorders and deemed likely to engage in violent behavior if released. He was permitted to possess and use certain electronic devices to store music, movies, personal items

[28] Doe v. Kentucky ex rel. Tilley, —F.Supp.3d—, 2017 WL 4767143 at *4 (E.D. Ky. Oct. 20, 2017) relying on *Packingham v. North Carolina*, supra n.1.

[29] J.I. v. New Jersey State Parole Board, 228 N.J. 204, 220, 155 A.3d 1008, 1018 (NJ Supreme Court 2017)

and legal materials, but not provided online access. The court acknowledged that convicted prisoners do not forfeit all constitutional protections by reason of their conviction and confinement, but the exercise of their First Amendment rights while incarcerated is limited by the fact of confinement and the needs of the penal institution. Citing significant safety concerns about the sharing and storage of child pornography, the court found no precedent for a constitutionally protected right to access the Internet in such circumstances. [30]

Freedom of Speech and Expression

In 1997, the U.S. Supreme Court held that under the First Amendment, the government can no more restrict a person's access to words or images on the Internet than it can snatch a book out of someone's hands or cover up a nude statue in a museum.[31] That case involved a challenge to the constitutionality of certain provisions of Communications Decency Act (CDA) aimed at protecting minor children from harmful material on the Internet. The Court ruled that provisions prohibiting the transmission of obscene or indecent communications by means of telecommunications device to persons under age 18, or sending patently offensive communications through use of interactive computer service to persons under age 18, were impermissible «content-based» blanket restrictions on speech.

Since then, states have sought to craft acceptable statutes criminalizing sexually related (but not necessarily obscene) speech when the exchange occurs electronically between an adult and a minor, with the intent to arouse sexual desire. Different courts have interpreted different statutes in different ways. For example, Texas's highest criminal court[32] and one federal court of appeals[33] have invalidated statutes criminalizing non-obscene sexually related electronic communications with minors made with an intent to arouse, holding that those statutes impermissibly prohibit a substantial amount of protected speech. In contrast, other courts have upheld similar statutes as permissible content-based restrictions on speech able to satisfy constitutional requirements. [34]

In *Scott v. State*,[35] for example, the defendant had been indicted under a state statute prohibiting «obscene Internet contact with a child … that is intended to arouse or satisfy the sexual desire of either the child or the person.» The Supreme Court

[30] Johanneck v. Ahlin, 2018 WL 1014454 *12-13 (E.D. Cal. Feb. 21, 2018).
[31] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
[32] Ex Parte Lo, 424 S.W.3d 10 (Tex. Crim. App. 2013).
[33] Powell's Books, Inc. v. Kroger, 622 F.3d 1202 (9th Cir. 2010).
[34] State v. Muccio, 890 N.W.2d 914 (Sup. Ct. Minn. 2017).
[35] Scott v. State, 299 Ga. 568, 788 S.E.2d 468 (Sup. Ct. Georgia 2016).

of Georgia rejected his constitutional challenge to the statute because, properly construed, it prohibited only specific categories of online contact made with the specific intent to arouse or satisfy the sexual desires of the accused or the child victim, and thus did not prohibit a real and substantial amount of expression protected under the First Amendment.

A Texas court recently rejected a constitutional challenge brought by an individual who had been indicted for the felony offense of online solicitation of a minor under a Texas statute proscribing solicitation of minor via electronic messaging with intent that the minor would engage in sexual conduct. [36] The court held that the statute was a permissible regulation on conduct (not an impermissible content-based restriction on free speech) and was neither overbroad nor vague.[37]

A somewhat different question was presented by a challenge to a California statute that established a database tracking all ammunition purchases in California. The database included the driver's license information, residential address and telephone number, and date of birth for anyone who purchases or transfers ammunition in California. An opponent of the legislation (who used the name «The Real Write Winger») maintained a political blog on which he posted the names, home addresses, and home phone numbers of all the «tyrant» legislators who had voted in favor of that legislation (obtained from publicly-available records). In response, the California legislature sought to require the company hosting the blog to delete that information when asked to do so by any individual legislator. The opponent challenged that requirement as an improper «content-based restriction» on constitutionally protected speech. The federal court agreed, describing the blog as a form of political protest and noting that viewed in that context of political speech, the legislators' personal information became a matter of public concern.[38]

Somewhat surprisingly, the Canadian Supreme Court recently sustained a lower court's injunction forcing Google to delete search results about pirated products not just in Canada but everywhere else in the world. The case began when one company (Equustek) accused another of selling counterfeit routers online, claiming that Google had facilitated access to the defendants' sites. Google voluntarily took down specific URLs that directed users to the defendants' products and ads under the local Canadian domain, but the British Columbia courts ruled that Google had

---

[36] Texas Penal Code section 33.021(c): «A person commits an offense if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.»

[37] Ex parte Moy, 523 S.W.3d 830 (2017).

[38] Publius v. Boyer-Vine, 237 F.Supp.3d 997 (2017).

to delete the entire domain from its search results, including in other countries. The Canadian Supreme affirmed that result.[39]

The extraterritorial effect of the ruling has generated some concern, especially to the extent it might encourage other courts (or regulatory authorities) to try to enforce their domestic laws by ordering global bans on particular uses of search engines. Reflecting these concerns, a federal court in California recently granted a preliminary injunction prohibiting enforcement of the global «de-indexing» order, citing §230 of the Communications Decency Act (which «immunizes providers of interactive computer services against liability arising from content created by third parties») and adopting Google's position that the Canadian Supreme Court ruling «threatens free speech on the global Internet.»[40] That ruling has been criticized as failing to give due consideration to traditional principles that govern the enforcement of foreign judgments demanded by principles of private international law and international comity.

Revenge Pornography, Cyber-Bullying and Cyber-Stalking

The courts have also had to consider the permissible limits on other kinds of improper Internet usage such as «revenge pornography» and «cyber-bulling.»

«Revenge porn» is popularly understood to include the distribution of sexually-graphic images of individuals without their consent, including pictures given by one individual to another or originally obtained without consent. For example, in Texas, a former boyfriend posted secretly-recorded sexual videos of his former girlfriend on Internet. The girlfriend sued to recover damages for several common law «torts,» including intentional infliction of emotional distress, intrusion on seclusion, public disclosure of private facts, and defamation. A jury found in favor of the girlfriend, awarded damages totaling $500,000. On appeal, including past and future mental anguish damages, past and future reputation damages, and exemplary damages, and entered permanent injunction. The verdict was upheld on appeal, but with some reduction in damages.[41]

Regarding «cyberbullying,» a state statute in North Carolina makes it unlawful for any person to use a computer or computer network to post (or to encourage others to post) on the Internet private, personal, or sexual information pertaining to a minor «with the intent to intimidate or torment a minor.» The state Supreme Court recently invalidated the statute on First Amendment grounds because it restricts some kinds of speech and not others (which, the court said, makes it impossible to determine

[39] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34 (Can.),
[40] Google LLC v. Equustek Solutions Inc., 2017 WL 5000834 (N.D. Cal. Nov 2, 2017).
[41] Patel v. Hussain, 485 S.W.3d 153 (Tex. Ct. App. 14th Dist. 2016).

whether the accused has committed a crime without examining the content of his communication») and because the restriction was «not narrowly tailored to the State's asserted interest in protecting children from the harms of online bullying.»[42]

In the same vein, the Supreme Court of Illinois struck down provisions of a «cyber-stalking» statute which criminalized two or more nonconsensual communications to or about someone that the defendant knew or should have known would cause a reasonable person to suffer emotional distress. In this case, the allegation was that that the defendant had used electronic communication to make Facebook postings in which he expressed his desire to have sexual relations with another individual, and threatened her coworkers. Under the relevant statutory language, the court said, communications that were «pleasing» to the recipient were not prohibited but communications that the defendant knew (or should have known) would be «distressing due to their nature or substance» were prohibited. Therefore, it was a «content-based» restriction because it could not be justified without reference to the content of the prohibited communications. Moreover, the statute did not require a «true threat or integral relation of speech with criminal conduct.» [43]

Liability of Internet Service Providers

As indicated above, the Communications Decency Act of 1996 was enacted in part to immunize internet service providers from liability arising from publication of information created by third parties. The statute has presented some interesting questions.

In 2017, a federal appellate court considered (and rejected) claims brought under the statute against Facebook alleging that Palestinian terrorists had used that platform's services to incite, enlist, organize and dispatch would-be killers to commit acts of violence and that Facebook had failed to take action to prevent such use.[44] Even if the comments were not protected by the First Amendment because they involved hate speech against plaintiff's African ethnicity, falsely accused plaintiff of being a criminal, or used fighting words, Facebook was entitled to immunity under Communications Decency Act (CDA).[45] In the same vein, a different federal court

[42] State v. Bishop, 368 N.C. 869, 876, 787 S.E.2d 814, 819 (N. Car. Sup. Ct. 2016).

[43] People v. Relerford, --- N.E.3d ----, 2017 WL 5894178 (Sup. Ct. Ill. Nov. 30, 2017).

[44] Cohen v. Facebook, Inc., 252 F.Supp.3d 140 (E.D.N.Y. 2017).

[45] Obado v. Magedson, 612 Fed.Appx. 90, 43 Media L. Rep. 1745 (3rd Cir. 2015). An earlier state court decision, Kathleen R. v. City of Livermore, 87 Cal. App. 4th 684, 104 Cal. Rptr. 2d 772 (1st Dist. 2001), had applied the statute to dismiss a taxpayer's suit against a public library for permitting her minor son to use the library's computer to download sexually explicit photographs from the Internet.

held that Facebook was protected from liability for having permitted third parties to publish allegedly defamatory statements bout Plaintiff's gender identity.[46]

IV. Emerging Issues

Technological developments continue to raise new issues for courts to consider. As noted above, the United States has no general federal «privacy» statute.[47] The main principles are provided by the Fourth Amendment, which limits the right of government to search locations and property over which a person has a reasonable expectation of privacy.

Use of GPS Information

Under what circumstances may the government use «global positioning satellite» (GPS) tracking information in its investigation of criminal activity? Some years ago, the U.S. Supreme Court made clear that the attachment of a GPS device to a private vehicle and subsequent monitoring of its movements on public streets was a «search» under the Fourth Amendment, thus requiring judicial permission based on «probable cause»). The Court made special note of the fact that GPS technology enables the government to gather, store, and exploit vast amounts of information at relatively little cost.[48]

In the years since that decision, more than a thousand judicial decisions have addressed GPS issues in diverse contexts, exploring various applications of the general rule. To take only three recent examples, the lifetime GPS monitoring of a convicted sex offender under statutory authority has been upheld against constitutional challenge, in light of the legislature's legitimate concern about protecting the public from such dangerous predators.[49] Similarly, following the movements of a convicted felon suspected of involvement with drugs by using GPS to determine the location of his cellphone (pursuant to warrant) has been upheld.[50] In a recent decision, the Supreme Court of Arizona allowed the admission of evidence of drugs discovered through GPS monitoring (without a warrant) of the movement of a commercial truck in which the defendant was a passenger. In that case, because the individual bringing the challenge did not own the vehicle (he was a passenger), the court said he lacked the necessary «possessory interest» to challenge the GPS monitoring as a trespass,

[46] La Tiejira v. Facebook, Inc., 272 F.Supp.3d 981 (S.D. Tex. 2017).
[47] The constitutions of ten U.S. states expressly recognize some form of privacy rights (Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington).
[48] United States v. Jones, 565 U.S. 400 (2012).
[49] State v. Muldrow, 377 Wis.2d 223, 900 N.W.2d 859 (Ct. App. Wisc. 2017).
[50] United States v. Ponce, 2017 WL 3251494 (M.D. Fla. July 31, 2017).

nor did he have a «reasonable expectation of privacy» with respect to the truck or its movements over public roadways.[51]

Inter-Connectivity

The advent of inter-connectivity (the «Internet of Things») has challenged these principles. For example, purchasers of television sets with integrated software for internet video content delivery (so-called «smart» TV's that permit access to on-demand services such as Netflix, Hulu, and Pandora) have brought a class action in federal court against the TV manufacturer alleging that the TVs secretly collect content-viewing histories and the manufacturer then sold that information to advertisers and media content providers. Plaintiffs allege that, unbeknownst to them, this software collects up to 100 billion content «viewing data points» along with detailed information about a consumer's digital identity, such as consumers' IP addresses, zip codes, MAC addresses, product model numbers, hardware and software versions, chipset IDs, region and language settings, as well as similar information about other devices connected to the same network. The court recently sustained the complaint against a motion to dismiss, subject to certain conditions.[52]

It has long been established that a person has no legitimate expectation of privacy in information he or she voluntarily turns over to third parties.[53] With regard to law enforcement, a defendant has no reasonable expectation of privacy in files retrieved from his or her personal computer on which that person installed and used software making files accessible to others.[54]

Facial Recognition Technology

The increasing sophistication of facial recognition technology presents significant privacy challenges, particularly when implemented in public places. U.S. law does not recognize a general «right to anonymity» but in some situations the Constitution has been held to provide some identity protection even in public spaces.[55] No federal laws currently constrain the use of facial recognition software but some states have begun to address these issues by statute. For instance, the Illinois Biometric Information Privacy Act[56] prohibits the non-consensual collection and storage of

---

51 State v. Jean, 243 Ariz. 331, 407 P.3d 524 (2018).

52 In re Vizio, Inc., Consumer Privacy Litigation, 238 F.Supp.3d 1204 (C.D. Cal. 2017).

53 Smith v. Maryland, 442 U.S. 735, 739-40, 743-44 (1979).

54 United States v. Stults, 575 F.3d 834, 843 (8th Cir. 2009).

55 Cf. United States v. Jones, 565 U.S. 400 (2012); NACCP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958); but see Illinois v. Lidster, 540 U.S. 419 (2004) and American Knights of the Ku Klux Klan v. Goshen, Ind., 50 F.Supp.2d 835, 839 (N.D. Ind. 1999) (the First Amendment protects «the right to communicate and associate anonymously»).

56 Biometric Information Privacy Act, 740 Ill. Comp. Stat. §14/1 (2008). Texas and Washington have similar laws.

certain types of biometric data (including retinal or iris scans, fingerprints, voiceprints, or hand or face geometry scans). Several suits under this statute are pending against Facebook for its use of «tag suggestion» program, which identifies faces in photographs uploaded by users – in effect, associating names with photographed faces and prompting users to «tag» those individuals without their consent.[57]

Right to be Forgotten

The so-called «right to be forgotten,» while recognized in Europe[58] and elsewhere, is not formally acknowledged in the United States. In 2013, however, the California legislature passed a statute entitled the «Privacy Rights for California Minors in the Digital World» law (otherwise known as the «eraser law»).[59] It provides that any operator of an Internet website «directed to minors» (18 years old or younger) must permit minors to «remove or, if the operator prefers, to request and obtain removal of, content or information posted» on the operator's site by the user. The website operator must also provide notice and «clear instructions» as to the means of erasing information. Exceptions include conflicts with other federal or state laws, content stored by a third party, content that has been «anonymized,» failure to follow the site operator's instructions, and circumstances where the minor has «received compensation or other consideration» for providing the content. The law has received some intense criticism - that, among other things, the law is ambiguous and constitutionally questionable.

V. Conclusion

As the foregoing demonstrates, the U.S. approach to cyberlaw, in particular issues of privacy in the digital age, involves a complicated, dynamic inter-play between the courts and the legislatures, between statutes and constitutional doctrine, and between federal and state law. In its larger dimensions, the problem can been seen as a struggle to adapt time-honored legal principles to rapidly-evolving technology largely though the resolution of specific situations as they present themselves in litigation.

The *Microsoft* case now pending decision by the U.S. Supreme Court is illustrative. As part of a law enforcement investigation (evidently involving drug trafficking), the federal government sought to obtain the emails of an individual (of undisclosed nationality) which are stored by Microsoft on a server in Ireland. The relevant

[57] See, e.g., Patel v. Facebook, Inc., 2018 WL 1050154 (N.D. Cal. Feb. 26, 2018). See also Morton v. Shutterfly, 2017 WL 4099846 (Sept. 15, 2017); Rivera v. Google Inc., 238 F.Supp.3d 1088 (N.D. Ill. 2017).

[58] See Case C–131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014).

[59] Cal. Bus. & Prof. Code §§ 22580-22582.

statute (the Stored Communications Act) was enacted thirty years ago, long before the world-wide web or the Cloud existed. Its purpose was to protect the privacy of stored electronic communications in the United States in much the same way that other forms of communication were protected under the Fourth Amendment. The question is how to interpret and apply that statute in light of today's technological advances and the realities of transnational crime.

At one level, the case implicates the question of the extraterritorial application of U.S. law. Microsoft has refused to provide the emails, claiming that the statute has only domestic application. The government responds that no extraterritoriality is involved since Microsoft can readily obtain the records in the United States even if they happen to be located elsewhere. It does not appear that the Government of Ireland has claimed that production of the documents would violate its laws, but many commentators have expressed serious concerns that a broad interpretation of the law might create conflicts of that sort in other cases.

At another level, the case is important for law enforcement. If Microsoft prevails, the government might not be able to obtain information in the emails of a U.S. citizen under investigation for a crime committed in the United States if the service provider has chosen (for its own reasons) to store them overseas. In response, many have argued that international cooperative agreements are the proper way to overcome that problem.

Finally, the case raises the obvious question whether such decisions are best made by Judges considering specific situations or legislators considering broader policy questions – or both. Legislation has already been introduced in the U.S. Congress (the «CLOUD Act») – to permit courts to issue warrants for data stored overseas, subject to a right of objection by email providers and the relevant foreign countries. The Court's decision will determine the future of that proposal.

Fecha de recepción: 17 de abril de 2018
Fecha de aprobación: 15 de junio de 2018