ledge of the infringement. Online providers who electronically screen or preview material may be held accountable for copyright infringements, although providers who act as common carriers may not.

Google, by uploading copyrighted book material, has become involved in what is known as the Google Book Search Settlement. An administrator in the class-action lawsuit is creating a system to pay authors for use of their works.

DVD copying is also a problem. An engineering student faced a lawsuit for publishing on the Internet a code to unscramble encryption for copy protection. Motion Picture Association of America representatives testified to Congress that an estimated 350,000 movies were being downloaded illegally each day at a cost of billions of dollars to the industry.

A new problem has arisen from the theft of wireless network signals from homes and business. People have broken into private networks in order to facilitate illegal file transfers. In 2005, for example, St. Petersburg, Florida, police arrested a 41-year-old who had hacked into a home network by parking his SUV nearby and using a laptop computer. The case was one of the first to raise significant legal issues about theft of online bandwidth. Further, in apartment complexes, a computer user might identify more than one access point, and it is possible for there to be confusion over legal (with permission) and illegal access.

Clearly, the convenience of wireless networking comes at a price — the availability of signals for potentially illegal activities and the possibility of invasion of privacy of legal and paying users. ISP liability continues to spawn new case law. For example, Craigslist — used by individuals to advertise — was found not liable for housing classifieds that discriminated in violation of federal law and also entitled to immunity from gun violence that may have resulted from a weapon purchased online. State attorneys general and lawmakers continued to target Craigslist and its inability to filter all illegal activities, including under-aged sex trafficking. Craigslist responded with changes — removing all adult advertising.

The Internet and Privacy Issues

Workers using the Internet for personal reasons could find that employers have access to everything. People using the Internet from home for banking, shopping and email could find they have less privacy protection than when engaging in such activities by mail or in person. Additionally, social networking sites allow users to set privacy settings, but new users may skirt them.

A 13-year-old in 2005 lied about her age and then at 14 met a 19-year-old man online. He sexually assaulted her when they met in person. Her mother sued, claiming, "MySpace failed to implement basic safety features," but a lower court rejected negligence because findings were "barred by the CDA and Texas common law" — a finding affirmed. In another MySpace case, criminal prosecution of a Missouri mother was tentatively tossed by a U.S. District Judge. Lori Drew was convicted of violating MySpace terms of service by creating a false profile of a boy named "Josh Evans." It was used to get back at her daughter's former girlfriend Megan Meier, 13, who later committed suicide after online flirting exchanges with the fictitious boy, who dumped her in a message that said "the world would be better without [you] in it."

Carpenter v. United States
138 S.Ct. 2206 (2018)

Facts: In a series of 2011 robberies and arrests, Timothy Ivory Carpenter was placed near four robberies via cellphone location data. Carpenter moved to suppress evidence because there was no warrant or showing of probably cause.

Issues: Historical mobile data offer a picture of user movement, and this raises Fourth Amendment privacy concerns. Under *Katz v. United States, Riley v California* and *Kyllo v. United States*, technologies are subject to not only the Stored Communications Act, but also Fourth Amendment protection of "people, not places."

Decision: Chief Justice John Roberts was joined by Justices Ginsburg, Breyer, Sotomayor, and Kagan to reverse and remand the case as an illegal search: "[W]e hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." The holding was narrow: "We do not express a view on matters not before us: real-time CSLI or 'tower dumps.'" Justices Kennedy, Thomas, Alito, and Gorsuch filed dissenting opinions. Kennedy thought location data were similar to business records, Alito found a distinction of physical searches, and Gorsuch desired to overturn *Katz* privacy dicta.

Reasoning: "But while the third-party doctrine applies to telephone and bank records, it is not clear whether its logic extends to the qualitatively different category of cell site records.... A person does not surrender all Fourth Amendment protection by venturing into the public sphere."

"Moreover, the retrospective quality of the data gives police access to a category of information otherwise unknowable."

Justice Gorsuch, in his dissent, argued that before *Katz*, a Fourth Amendment claim did not turn on "a judge's personal sensibilities about the 'reasonableness' of ... expectations...."

In other developments:

- A police search of a smartphone by arresting officers without a warrant generally violates the Fourth Amendment (*Riley v. California*, 2014).
- Google apologized for Street View vehicles collecting personal data from open WiFi networks, and Facebook reported conducting secret psychological content filtering experiments — a top company officer apologized that the routine product testing was "poorly communicated."
- Facebook won an $873 million judgment against a Canadian spammer who flooded more than four million users with sexually explicit messages promoting penis enlargement products and illegal drugs.
- YouTube banned videos intended to incite violence or en-

courage dangerous, illegal activities.

Politwoops, a Web site that archived politicians' tweets, raised issues about the privacy rights of a user to delete content once published. The Open Foundation created the site at a 2010 meeting of computer hackers in the Netherlands. The Sunlight Foundation extended access to the United States in 2012. Because of legal issues, Politwoops faced closure in about thirty countries. Twitter disconnected access within the United States, citing Terms of Service violations.

Walmart sent Jeph Jaques, author and cartoonist, a cease-and desist letter for the Walmart.horse Web site. It featured only the image of a horse pasted in front of a store photograph. Walmart did not accept simple fair use parody instead of trademark infringement. It then filed a complaint with the World Intellectual Property Organization under the Uniform Domain Name Dispute Resolution policy. Rather than litigate, the Web site was voluntarily removed.

PRIVACY AT WORK
Ontario v. Quon
560 U.S. 746 (2010)

The Supreme Court reversed the Ninth Circuit Court of Appeals in finding in favor of the Ontario, California, Police Department and its monitoring of on-duty officer text messages.

In 2001, the city had issued police officers pagers, which had limits on the amount of text sent and received each month. When some officers exceeded the limits, a review of two months found that SWAT team member Jeff Quon had many personal and sexual messages during work hours. After being disciplined, he and other officers alleged violation of privacy on Fourth Amendment grounds, as well as the Stored Communications Act.

A district court found that the city had conducted a reasonable audit of the text messages and that the officers' privacy had not been violated, but the appeals court reversed the decision. At issue was the nature of a reasonable expectation of privacy at work, the ability of employers to conduct legitimate investigations of work-related misconduct and the evolving nature of the technology.

In a narrow ruling, the Supreme Court found the police department's warrantless search was reasonable because it was motivated by a legitimate work-related purpose and was not excessive in scope. A city policy informed employees that all messages on city-owned equipment could be reviewed in connection with computer use, the Internet and email. The text messages, however, had been sent and received over radio frequencies. Still, police officers had been given verbal advance warning that the general policy applied to texting. A case-by-case precedent led Justice Anthony Kennedy to write: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." Justice Antonin Scalia disagreed on that point: "The-times-they-are-a-changin' is a feeble excuse for disregard of duty."

New technologies also threatened to erode traditional common law views about the sanctity of privacy in one's own home. Privacy becomes a question when law enforcement authorities tap into computer transmissions. While a court order is required, it may be possible for computer users to encrypt transmissions. In 1993 the National Security Agency proposed a clipper chip to allow decoding.

Web-based telephone services, such as Vonage, posed an interesting privacy problem for regulators and the courts. The U.S. Court of Appeals, D.C. Circuit, upheld the FCC decision that law enforcement agencies require wiretap compatibility. The court, though, exempted university and private computer networks, as well as instant messaging. The clarification of the scope of the Communications Assistance for Law Enforcement Act, CALEA, meant that voice over Internet protocol was not exempt from telecommunication regulation under all circumstances.

Another privacy issue involves Web site content that is considered a threat. A federal jury in Portland, Oregon, ordered abortion protesters to pay $109 million in damages resulting from the Nuremberg Files site. The site featured images of dripping blood and fetuses and was ordered to close. It resembled a hit list of abortion providers, some of whom were victims of violence, and listed names and towns of doctors providing abortions. The case was appealed on First Amendment grounds. A legal scholar worried that the decision may be used in the future as a precedent to hold protesters liable for the violent acts of others."

Beyond the Internet and Future Regulatory Issues

Congress has proposed dozens of bills seeking to regulate various aspects of the Internet — pharmacy consumer protection, online investor protection, spam advertising limitations, email protection and e-commerce protection. One bill sought to limit sales of prescription drugs by requiring Web sites to include a page that lists licensed pharmacists. The mood to regulate was promoted by cases such as that of a Seattle doctor ordered to halt online prescribing of the sexual dysfunction drug Viagra after a 16-year-old boy and a woman posing as a man obtained prescriptions. The Food and Drug Administration raised concerns about the rampant online sale of prescription drugs. State attorneys general, meanwhile, maintained that licensing and monitoring of health care professionals should continue to be a matter of state regulation. Nevertheless, former U.S. Senate Democratic Leader Tom Daschle of South Dakota concluded that Congress had not kept pace with technological change. He stated: "Internet users are often promised basic privacy protection, only to have their expectations disappointed and their personal information put up for sale or disseminated in ways to which they never consented."

The global nature of telecommunications will pose new challenges. In the United Kingdom, for example, the government in 2000 planned for a spy center capable of tracking every email and Web site hit; but civil libertarians were outraged at the plan, even if its purpose was to crack down on cyber crime.

In the last several years, a variety of telecommunication developments have provided a landscape for monitoring the years

ahead, including:

- FCC government auction of Advanced Wireless Services in 2006 raised more than $13 billion from 104 bidders, but mostly from the nation's largest carriers.
- Worldwide Interoperability for Microwave Access is leading to 3.5 and 4G high-speed broadband and video access. Internet convergence is accelerating because of new 5G broadband and deregulation.
- The Internet is increasingly *the* method of access to public records and information, such as televison station public files.
- Web privacy issues increased, as online advertising posed questions about user data gathered, stored and sold.

EMERGING TECHNOLOGY ISSUES

The development of Internet and social media sites offered fertile ground for important developments to watch:

- Google removal of search results, such as revenge porn.
- Facebook content filtering and removal.
- Social media site responses to government data requests.
- Reduced Internet speeds based upon huge usage.
- Legislative response to the FCC Net neutrality elimination.
- Illegal videotaping of subjects without consent.
- Regulation of small drone video cameras.
- Photographer image rights.
- The European right-to-be-forgotten cases.
- Mobile video blocking technology by Apple to protect live concerts, but also potentially useful during law enforcement and military operations.

Source: AEJMC Law & Policy Division, Facebook group, https://www.facebook.com/groups/281106198661787/.

Social Media and the First Amendment

While *Reno v. ACLU* established a strong First Amendment right to use the Internet, the shift of communication to social media and social networking sites presents new issues for the courts. Facebook users, for example, agree to a terms of service agreement based upon a set of community standards. Most other sites and computer software also require user agreements.

The Supreme Court ruled in an important social media case, *Packingham v. North Carolina*. The Court struck down a state statute that made it a felony for registered sex offenders to access social media. In 2002, Lester Gerard Packingham, then 21, had been convicted of having sex with a 13-year-old girl and became a registered sex offender. In 2010, he posted on Facebook under the identity "J.R. Gerrard" his joy at having a traffic ticket tossed out of court. In a sweeping First Amendment decision, the Supreme Court found that it "must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium."

The Court continued:

> North Carolina with one broad stroke bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard.
>
> They allow a person with an Internet connection to "become a town crier with a voice that resonates farther than it could from any soapbox."
>
> In sum, to foreclose access to social media altogether is to prevent the user from engaging in the legitimate exercise of First Amendment rights. It is unsettling to suggest that only a limited set of Web sites can be used even by persons who have completed their sentences.

The Supreme Court found that North Carolina law was overbroad, but the state may pass "specific, narrowly tailored laws that prohibit a sex offender from engaging in conduct that often presages a sexual crime, like contacting a minor or using a website to gather information about a minor."

Taken together, *Packingham*, *Reno* and *Elonis v. United States* offered a glimpse into the long-term thinking of a majority of justices. When coupled with the Fourth Amendment mobile geo-location data privacy concerns expressed in *Carpenter v. United States*, it appears that the Court believes there are significant individual rights to use online communication as the modern-day public square. The Supreme Court views the Internet and now social media sites as at the core of First Amendment political speech. It is unclear, however, whether the Court will extend this view beyond the reach of government state action within a criminal law context to civil litigation by private parties. As we learn in privacy chapter of this textbook, freedom of expression can be limited through this type of litigation.

A broader question is whether the Supreme Court will uphold National Labor Relations Board cases protecting employees from imposing broad company social media policies that reach into private page content. Corporations exercise their First Amendment rights when managing social media sites, but employees appear to have a right to communicate on social media about collective bargaining and broader union labor issues.

Social media present a wide range of new legal questions:

- Will the president challenge the recent ruling of the Second Circuit that he may not block Twitter users?
- Are the president's tweets official statements that may not be deleted? The 9th Circuit initially answered yes.
- Will the death of Gawker in the Hulk Hogan privacy settlement chill future online and social media?
- Will European Union antitrust fines against Google influence large social media company behavior?
- Will the UK idea that Facebook users have a right to delete