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: Privacy and Consumer Protection

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

Internet privacy and consumer protection are of increasing concern. This publication will look at the various legal mechanisms that have developed to protect the privacy of Internet users and existing laws dealing with consumer protection and privacy.

Contents

*Chloe Margulis provided research assistance with this publication.

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.

Introduction

Consumer protection and privacy are some of the most talked about areas of Internet law. Economic and technological shifts that allow people to do their banking, shopping, and daily business online have opened the door for companies and financial institutions to do business with people all over the world. This online economy results in more personal information being shared and stored in electronic formats, raising major concerns that the government will access the data and that private companies will fail to protect it.

Commercial activities are just one area where individuals provide private personal information over the Internet. Federal, state, and local governments collect information from individuals through various online activities. Private and public schools, colleges and universities, and even preschools use online programs for payment, educational activities, and school records. Internet service providers and Internet search engines collect information from their users. In many cases, regardless of whether or not a commercial transaction occurs, a website collects information from the users who visit their sites. News and opinion websites, social and professional networking sites, online job boards, gaming sites, and online gambling websites are all examples of online activities that often request some personal information from their users.

Privacy protections are imbedded in many aspects of federal and state law, and in the U.S. Constitution. The Fourth Amendment guarantees individuals protections from unlawful government searches and seizures.[1] The right to freedom of assembly, beliefs, and association are guaranteed by the First Amendment, and those rights to freedom of beliefs and opinions are further protected by a right to privacy. The Fourteenth Amendment guarantees freedom from intrusions into some private decisions such as marriage, families, and relationships.[2] These constitutional provisions restrain the government from intrusions into specific aspects of individual privacy. Some state constitutions have similar provisions to the Fourth Amendment.[3] Some states have expanded privacy provisions in state constitutions specifically identifying the right to be secure from an invasion of privacy.[4] In some cases the courts have found that, along with protection from unwanted government intrusion into individuals' private lives, the protection against intrusions of privacy creates a privacy interest that protects individuals from private entities and companies.[5]

These privacy considerations in state and federal constitutions were contemplated long before the Internet. As the use of the Internet and home computers has increased, the courts in the United States have applied existing privacy laws and constitutional protections to electronic communications and the electronic containers that hold so much of an individual's personal information. In 2004, the Second District Court of Appeals held that there is an expectation of privacy in the contents of a home computer.[6] But one state has extended privacy protections in its constitution to specifically cover electronic data: Missouri passed a constitutional amendment to include electronic documents in the state constitution's Fourth Amendment protection from unlawful search and seizure.[7] While there are some existing provisions that protect consumers, emerging technologies continue to outpace regulations.

This publication looks at the various legal mechanisms that have developed to protect the privacy of Internet users, including an examination of how contract law has evolved to govern the user and licensing agreements between companies and consumers. The brief also looks at how federal and state laws have been enacted to regulate some of the consumer protection issues and privacy concerns that have been raised as more personal information is increasingly exchanged via the Internet. Finally, this brief looks at how companies have had to modify policies to respond to consumer demands (and maintain their reputations) by instituting privacy policies that protect consumers' personal information.

Common Terms in Privacy Legislation

The Internet allows the government and private entities to collect a vast array of personal information from individuals. The definitions below have been used by the private and public sector and have also been used in some newer federal and state legislative proposals.

- Personal identifiable information (PII) or sensitive personal information, which can include various forms of identifying information such as name, date of birth, Social Security number, address, or IP address and device identifiers.

- Personally identifiable financial information (PIFI), which is often used to refer to financial and banking information, such as credit card numbers or bank account balances.

- Nonpublic information (NPI) is a term often used to describe the information collected to create an account, such as financial institution account information and tax information, but also other personal information, like health records used to obtain a life insurance policy.

Contract Law and Terms of Use Agreements

User agreements are contracts between the website (or merchant) and the user (or consumer). Much of the information exchanged between Internet users and the websites they visit are governed by the website's "terms of service" agreements, also called "terms of use" agreements. This is a contract between the user and the website that individuals agree to when they view a website. Often a website will have a page stating that, by using the website's services, consumers are agreeing to all the terms contained in the terms of service or terms of use agreement.

A contract forms when the user agrees to the terms required by the website to view or access the website. Sometimes this is explicit, through an opt-in process, such as checking a box saying the viewer has read the terms and agrees to them. Other times, this is done through a notification on the website, stating that an individual using the website has agreed to the terms posted on the website. Some of these notifications are easy to find but others are not. The validity of these agreements as enforceable contracts continues to be debated in state legislatures and court cases around the country.[8]

Privacy policies, such as what information is collected about an individual, or stored or maintained for an individual's account, as well as information on how that individual's information is shared with others, are often contained in the terms of service agreements. While the agreements are quick and easy to use, consumer advocates warn that few consumers read them, and even if they do read them, the consumer has no power to negotiate for new terms.

Courts Use Contract Law to Interpret Terms of Service Agreements

These terms of service agreements have been interpreted by the court using contract law. Many of the early cases in this area related to "end user licensing agreements" (EULA), also called "shrink wrap" agreements, which are licensing agreements that come in the package with a new computer or software. These agreements govern the purchaser's ability to use the software. The terms of use agreements that are on websites and accompany software downloads are given the nickname "click wrap" agreements because the user is required to click a box to consent to the terms before installing software on a home or business computer, use an operating system on a mobile device or cell phone, or interact with any number of service providers on the Internet. A third term, "browser wrap agreements," has been used to define the terms of service agreements that appear on a website's homepage or information page, or at the bottom of the page of a website a user is accessing. These do not require any action on the part of the user to accept the terms, but instead a user is agreeing to the terms simply by using the website.

The provisions of the terms of service agreements often dictate where cases may be brought (the venue for a court action), which state's laws will apply in the case (choice of law provisions), as well as what remedies are available in a legal dispute. Sometimes these user agreements will restrict users to binding arbitration, which prevent a consumer from filing a lawsuit if there is a dispute with the company and can prevent class action lawsuits.

The provisions of the "click wrap" or "terms of use" agreements have been viewed by some consumer advocates as one-sided because they offer no opportunity for negotiation on the terms in the agreement. The company offers the terms and the consumer has to accept them to use the

product, access software, or use a web service. The agreements are often seen as unfair and even coercive to consumers who may not be aware of the terms in the agreement, which are sometimes hard to find, difficult to understand, and often lengthy.[9] Websites and online retailers have argued that creating more specific agreements would be onerous and costly, and that providing additional requirements to contract with a website or company would irritate consumers who are trying to use a service or make purchases.

Courts Have Upheld Terms of Use Agreements

Courts in the United States have generally upheld the terms of use agreements even though some consumers have argued the contracts are unconscionable[10] or contracts of adhesion.[11] Because these contracts are not negotiated, it is sometimes argued that they are "one-sided" as the terms are written by one party[12] and "accepted" through silence (using the website) or action (clicking a box indicating the user had read and accepted the terms). The trend has been for courts to enforce the online agreements in an effort to uphold the principles of contract law—the assumption being that both parties willingly agreed to the terms of the contract.[13] While a few cases have found that a "buried" arbitration clause or choice-of-law provision is invalid,[14] most U.S. courts have upheld the mandatory arbitration and choice-of-law provisions in Internet contracting that occur between commercial businesses and their consumers.[15]

Courts have typically found that when users have signified they have read, understood, and agree to the contract provisions, the contract terms will be upheld. Agreeing to the terms can include opening a product and keeping it,[16] using a website where the terms are posted,[17] or clicking on an agreement indicating users have read, understood, and agreed to the terms.[18] Courts have generally found that parties are not excused from the terms of a contract for failing to read them. While courts have upheld "click wrap" and "browser wrap" agreements as valid contracts, the courts will consider if the terms of the contract are fair and enforceable under the federal and state contract law provisions that apply in each case.[19] The conclusions by U.S. courts are in contrast to the European system, which often only upholds mandatory arbitration and choice-of-law provisions in contracts between commercial entities.

Terms Must Be Presented in a Reasonable Manner

While "terms of use" agreements are typically enforced, several courts have found that the terms must be presented in a reasonable manner so that a consumer can find the terms of service or use before agreeing to them. U.S. courts have found that these types of contracts "must be presented to the plaintiff, rather than merely posted inconspicuously on a website."[20] This general rule does not prevent "browser wrap agreements" or links to further terms and conditions that are binding on a consumer, but does present some limits to what will be upheld. For example, in the case *In re Zappos*, the court found that a provision in the company's user agreement that allowed it to change the terms of service at any time was unenforceable.[21]

The case law in this area continues to evolve as consumers sue companies to enforce provisions of state consumer protection laws and avoid binding arbitration agreements, choice of law provisions, prohibitions on class actions, and enforcement of provisions of state consumer protection laws. To determine if the agreement is enforceable, the courts will generally examine how the agreements are presented and the ability of a consumer to find and access the agreement.

If the agreement is enforceable, the court will then look at established laws regarding arbitration, choice of law, and contract provisions prohibiting class actions to determine if these terms in the contract are enforceable under state and federal contract law.

Federal and State Consumer Protection Law

Congress passed a number of federal laws designed to address consumer protection and privacy issues as the Internet was becoming accessible and popular in the 1990s and early 2000s. This section discusses the regulatory aspect of consumer protection related to the Internet. Two federal agencies, the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), are assigned to oversee a variety of federal laws and policies regulating the Internet. These two agencies have rulemaking and enforcement authority over various Internet-related activities, including net neutrality, broadband regulation, and consumer privacy. Generally, the FCC tracks and oversees consumer issues related to telecommunication billing and services, while the FTC focuses on false and deceptive business practices, consumer privacy, and Internet scams.

FCC Regulates Communication Utilities

The FCC is the federal agency tasked with regulating communication utilities such as telephone, wire, satellite, and cable. The FCC can enforce some laws that affect Internet access and communication via the Internet, including issues like net neutrality, availability of Internet services, Internet speed and equipment, billing practices, and some privacy issues.

In 2015, the FCC approved "Open Internet" rules, which adopted the principle known as net neutrality. The current rules require content to be treated equally and prevent broadband providers from allowing "fast lanes" for certain types of media or for media from certain companies. The FCC also adopted privacy rules for Internet service providers (ISPs) that would have regulated ISPs' ability to collect and sell customers' information, such as browsing history, and would have required customers to be notified and consent to the collection and distribution of certain information. The FCC rules never went into effect and were overturned by Congress in April 2017.[22]

In 2017, the FCC also announced it was considering modifying the current rules related to net neutrality after ISPs pushed to decrease federal regulations in this area. The comments and reply comments on the proposed changes to this rule were due by August 16, 2017.[23] In December 2017, the FCC voted to overturn the Open Internet rule and to return much of the jurisdiction related to Internet privacy and access to the FTC.[24] The new FCC regulation, referred to by the agency as "Restoring Internet Freedom," would also keep broadband and commercial mobile service providers from being treated like telephone companies, or "common carriers," under other federal regulatory laws.[25] The ISPs and broadband providers generally argue that their privacy policies that protect their consumers prevent unfair intrusions and that if there are unfair intrusions into consumers' privacy, that the FTC will investigate them just like they do to companies like Google and Facebook. Consumer privacy advocates argue that ISPs can see where their customers go on the Internet and what they look at, whereas a single website or web page does not have that ability, and therefore stronger privacy restrictions are appropriate for

ISPs. The FCC indicated the new plan to deregulate the Internet and move away from the previously adopted net neutrality position would preempt state action to try to impose similar regulations on service providers.

There was a strong reaction to the federal changes in 2017. In response to Congress overturning the FCC proposals in the spring of 2017, a number of state legislatures introduced legislation to impose rules similar to the FCC privacy rules. Only two states, Minnesota and Nevada, already had a law that imposed privacy restrictions on ISPs, but neither of those existing laws had the requirements in the overturned FCC rules. Many of the newly introduced state bills aimed to require ISPs to require consumer consent to collect, use, and sell consumer data, such as browsing history.[26] None of the proposed state legislation had passed at the end of 2017, except that Nevada's existing law on data privacy added additional provisions requiring websites and online consumer services to provide notice to users about information collected on users. The new law authorized the Nevada Attorney General to enforce the law and seek civil penalties against a website or online service who violates the act, which includes imposing a civil penalty of up to $5,000 for each violation.[27] A new proposal in Minnesota directed at ISPs did not pass[28] and the existing Minnesota law, passed in 2002, was not amended.

FTC Focuses on Consumer Protection

The FTC was created in 1914 to protect consumers and address unfair trade practices and consumer protection issues. For the last three decades, the FTC has also worked on consumer regulations and privacy issues related to Internet use. Generally, the FTC has had jurisdiction over the regulation of unfair and deceptive practices by businesses operating on the Internet and businesses providing Internet services, as well as consumer and privacy issues with websites and search engines.[29]

The FTC has rulemaking authority, as well as investigative and enforcement authority under the Federal Trade Commission Act (FTC Act).[30] The FTC Act regulates unfair acts or deceptive practices in commercial activity.

The FTC has investigated and taken action against a number of websites and search engines in recent years to enforce consumer protection issues. Using the FTC Act, the Gramm-Leach-Bliley Act (GLBA) regulating financial institutions, and other federal laws of general application, the FTC has conducted investigations and initiated lawsuits against companies for privacy violations and deceptive practices, largely mirroring the work that the FTC does against companies that are not Internet-based. One of the primary tools the FTC has is section 5a of the FTC Act,[31] which declares unfair and deceptive trade practices affecting commerce to be illegal. This broadly worded statute allows the FTC to investigate and fine large companies that engage in practices that hurt trade or affect many consumers in many different states. The definition of "unfair practices" requires a "substantial injury." Because of the resources required to undertake these cases, FTC actions tend to be against large national corporations in instances where the company's practices affect numerous consumers.

The FTC can also file complaints against companies that have violated other federal laws of general application including the Equal Credit Opportunity Act, Truth-in-Lending Act, Fair Credit Reporting Act, the Do-Not-Call Implementation Act of 2003, the Children's Online

Privacy Protection Act (COPA), Fair and Accurate Credit Transactions Act of 2003, and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM).[32] The FTC also issued a Health Breach Notification Rule, which covers entities outside the Health Insurance Portability and Accountability Act (HIPPA) to govern online health information stored by vendors of personal health records, personal health records-related entities, or third-party service provides for those vendors.[33]

Below are a few examples of the cases the FTC has brought in the last few years specifically addressing online commercial activities and privacy.

- In 2014, the FTC brought a complaint against Craig Brittain, an Internet site operator who posted nude photos of women without their consent, alleging that Brittain's actions constituted unfair or deceptive acts or practices in or affecting commerce in violation of section 5(a) of the FTC Act. Brittain reached an agreement with the FTC in 2015 to take down the website and cease any similar activities.[34]

- The FTC, along with 35 state attorneys general, brought a complaint against LifeLock, alleging deceptive trade practices for making promises about its identity theft protection services and settled with the company in 2010. The FTC then got a large monetary award when LifeLock later broke the terms of the settlement agreement for continuing to make deceptive claims and failing to safeguard users' privacy. In 2015, the FTC required LifeLock to pay $100 million dollars as a penalty for violating the previous settlement terms.[35]

- The FTC, along with a number of states and other countries, charged that the operators of the dating website AshleyMadison.com had deceived customers and failed to protect the private information of the website's users. Similar to previous cases, the settlement required the website to pay a large settlement fee and implement improved privacy provisions to protect consumer's data.[36]

- In 2017, the FTC reached a settlement with the online tax preparation company TaxSlayer for data breaches that violated the GLBA requirements that financial institutions follow security guidelines to keep customer information safe and provide customers with specific privacy notices.[37]

- The FTC reached a settlement with the television company Vizio in 2017 after filing a complaint along with the state of New Jersey, alleging the company violated consumers' privacy by tracking consumers' viewing history without their consent.[38]

- The FTC settled with Google for $22.5 million after its web browser placed advertising tracking cookies on customers' browsers after the company had erroneously informed customers that the default browser settings would block third-party cookies.[39]

- In 2011, the FTC reached an agreement with Facebook requiring it to provide accurate information to consumers about privacy and information sharing with third parties after Facebook allowed third-party applications to access information the website said they could not access, and incorrectly informed users that information that was deleted or

private was actually public and still saved by the company.[40] The settlement requires Facebook to provide users with accurate privacy information.

Similar to the role the FTC plays at a national level in enforcing consumer protection laws, state consumer protection acts can be enforced either by the state's attorney general or by individuals. These laws, sometimes called "little FTC Acts," are supplemental federal consumer protection laws and are broader than the federal laws. While these laws usually provide for enforcement through the state attorney general, many of them also allow a private cause of action by an individual. Minnesota law grants the attorney general the power to enforce the Act Against Unfair Discrimination and Competition,[41] the Unlawful Trade Practices Act,[42] the Antitrust Act,[43] and the Prevention of Consumer Fraud Act.[44]

Consumer Protection under Minnesota Law

The Minnesota Consumer Protection Act is primarily contained in Minnesota Statutes, sections 325F.68 to 325F.70, but the state also has a number of other consumer protection provisions in Minnesota Statutes, chapters 325D and 325F. Minnesota law does allow for individual causes of action, but the ability of an individual to sue for violations of these state provisions has been limited in some instances by Minnesota courts.[45] The Minnesota law specifically related to Internet privacy—Minnesota Statutes, chapter 325M—is not included in the Consumer Protection Act or in the statute that would allow for enforcement through the Minnesota Attorney General's Office.[46]

Some consumer advocacy groups have criticized existing laws for not providing enough protection to consumers and for failing to protect consumer privacy. Under the federal and state laws addressed in this section, consumers have to rely on the state's attorney general or the FTC to bring action against companies who violate privacy and consumer protection laws. Those actions are usually only brought when numerous consumers have been injured by the same policy or practice and rarely occur when only a small number of individuals are harmed by a company's actions. Further, because the common law causes of action for torts is also limited in privacy breaches, consumers often face many legal hurdles in trying to bring their own private action against large companies.

Federal and State Privacy Laws

This section addresses federal and state laws that have been enacted to protect personal data on individuals, such as personally identifiable information, health information, and financial information. These laws often apply to either data collected, stored, and retained by the government or data collected and held by private businesses, but in some cases the law applies broadly both to a government actor and to the private sector.

There are numerous federal laws that have emerged in the last few decades that require businesses, nonprofits, and anyone operating online to safeguard user's privacy. Some of these laws specifically apply to various sectors, such as the financial service industry or the health care industry. Other laws apply more generally, such as the Computer Fraud and Abuse Act, which applies to any person who illegally authorizes another person's computer or online passwords.[47]

The list below highlights the main purposes of each law designed to safeguard consumer privacy online.

Federal and State Law Regulate Government Data Practices

Federal and state laws require the government to keep individuals' data private, whether the information is electronic or on paper. Just like the private sector, these laws require the government to securely store personal information. Government data is generally governed by two types of laws. Record retention laws govern what data is collected, how long it is maintained, and when it is destroyed. Data privacy laws govern who can access the data and how it is protected as either private or public information.

The federal Privacy Act of 1974 governs how federal agencies can collect, maintain, and disseminate personal information about individuals, which includes information obtained electronically.[48] The E-Government Act of 2002[49] was passed to address the federal government's use of Internet technology and included the Federal Information Security Management Act of 2002 (FISMA),[50] which requires agencies to create data security policies for the information they maintain, and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), which created uniform confidentiality protections for statistical information. Updates to FISMA were passed in 2017 in the Federal Information Security Modernization Act of 2014.[51]

The Minnesota Data Practices Act (DPA) determines how Minnesota state agencies can collect and use personal information on individuals. The statute has many specific provisions related to data collected by state agencies and provides that certain types of data the state and political subdivisions[52] collect is kept private, including health records, schools records, law enforcement data, and welfare benefits and public assistance records.[53] The DPA does not differentiate between paper records or electronic records, and the data that is held electronically must be maintained and kept private in the same manner as any paper records.

The Minnesota Data Practices Act also classifies data that is collected when a person uses a government computer.[54] "Electronic access data" is data that a government entity creates when a person accesses a government entity's computer or database. Under current law, this data is classified as private or nonpublic. Minnesota law requires notice to an individual that the state website is collecting data on an individual. Minnesota law also requires individuals to be notified without reasonable delay when government data has been hacked and that all government entities complete a comprehensive security assessment annually.[55]

The Minnesota Department of Information Technology (MNIT) is a state agency charged with the coordination, procurement, and support of information technology systems in Minnesota government.[56] The agency has to create accessibility for Minnesota citizens and create and implement cybersecurity plans.[57] This agency develops and implements security plans to prevent cyberattacks that could cause "denial of service attacks," which keep users from accessing government services websites, as well as cyberattacks that destroy or hold state data hostage, and hacking attacks that leak private data. Along with developing cybersecurity guidelines and standards, this agency also installs and administers these policies on state computers to keep data

safe and comply with the state's data privacy act.[58] This agency is also required to make state information technology and electronic information accessible to people with disabilities.[59]

Federal Laws Include Privacy Protections for Electronic Communication

The Electronic Communication and Privacy Act (ECPA) was passed in 1986 to update the federal wiretapping statutes to include electronic communication. The law has been updated a number of times over the years, particularly regarding the process government law enforcement must use to intercept or track wire, oral, or electronic communications. The act contains three parts or titles. The first title relates to the ability of the government to intercept communications using a subpoena, a warrant, or a court order.[60] The third title is a prohibition on pen registers or trap-and-trace devices, which collect the numbers a person calls on his or her phone. The act allows those devices to be used only with a court order or under the Foreign Intelligence Surveillance Act.[61]

Title II of the ECPA is often referred to as the Stored Communications Act (SCA). This is the federal law that protects e-mails, telephone conversations, and electronic data communications when they are being made, in transit, or stored on a computer.[62] This law applies to both private and government entities and, along with the Fourth Amendment's protection from unlawful search and seizure, provides the primary source of privacy for online communication, including e-mail. Under the SCA, unauthorized access to e-mail and telephone communication can result in a prison sentence or fine. The law prohibits a company providing e-mail services from divulging the information to a third party or law enforcement, except in certain emergency situations or pursuant to a court order or warrant.[63] The SCA provides greater protection to communications that are less than 180 days old.[64] It also provides a civil cause of action to individuals harmed by violations of the law, which can include actual damages, punitive damages, court costs, and attorney fees.[65]

Courts have had to determine how to apply the ECPA and the SCA to various forms of electronic communication. The SCA prevents a provider of an electronic communication service from disclosing communication. The government can obtain subscriber information and the content of e-mail with a warrant, and in some cases with a subpoena or court order. An electronic communication service includes e-mail, but courts have also found that it can include private messages on social media, wall postings/comments on social media boards, and private YouTube videos.[66] The ECPA broadly includes text messages and Voice-over Internet Protocol (VoIP), however, the law has not been extended to cookies and user browser data.[67] Federal courts have also found that data held on a mobile phone or hard drive are also not covered by the SCA, including location data, because the law is specifically intended to relate to communication held by an e-mail provider or ISP, not information located on a device.[68] However, other laws and constitutional protections may protect information on a mobile phone or hard drive.

Courts have interpreted the SCA to determine how far the privacy restrictions go in protecting certain types of communication from government access, harmonizing the language in the statute with the Fourth Amendment protections against unreasonable search and seizure. While some private communication on social networking sites has been protected, courts have also found that simply because something is shared "privately" does not mean it cannot be accessed. In *U.S. v. Meregildo*,[69] the government was allowed to access Facebook posts while it was investigating

the suspect when the user's friends cooperated and provided the information. The court found that investigators did not need a warrant because the suspect had no expectation the suspect's friends would keep the information private. The Fourth Amendment has also been used to extend privacy protections, even where the SCA would have otherwise allowed e-mails to be obtained. In *U.S. v. Warshak,*[70] the court found that while the government obtained e-mails from an Internet service provider with a subpoena consistent with the provisions of the SCA, the suspect's privacy had been violated and the Fourth Amendment required a warrant to obtain those communications.[71]

While the SCA provides access to a government for the limited purpose of criminal prosecutions, it creates a total bar on disclosure for any other purpose. This means that a civil discovery request or subpoena would not allow dissemination of electronic communication from an electronic communication service provider. A private company or individual that wants to gain information can do so through the normal discovery process in civil litigation, by sending the request to the user and not the electronic communication service provider. Attorneys have been cautioned against obtaining discovery through deceitful means on social media sites, such as "friending" opposing parties; however, information that is available to the public on the Internet is not considered to give the user an expectation of privacy.[72]

The Computer Fraud and Abuse Act (CFAA) is the federal law that prevents the unauthorized access of a computer creating a crime for "computer trespassing" and damage to computers and systems via viruses and worms.[73] The law affects any computer used in or affecting interstate or foreign commerce, which is a broad definition allowing most computers to fall under the jurisdiction of the CFAA. The law makes it illegal to access federal government computers and computers used in the financial industry without authorization or without the proper level of authorization. In addition to criminalizing these acts, the CFAA also offers civil remedies for damages so that an individual can sue the perpetrator in some cases.[74] The FCAA covers:

- hacking and virus attacks to computers, including the threat to hack or attack a computer or conspiring to attack or hack a computer;
- trafficking in passwords;
- accessing a computer to gain information or to make a financial gain;
- negligently, recklessly, or intentionally damaging a computer through unauthorized access; and
- accessing a government computer or accessing a computer to gain national security information.[75]

The courts have found that nearly all computers, and particularly any computer that connects to the Internet, is covered by the CFAA.[76] Court cases have contemplated the broad definition of a computer in the CFAA and found that it applied to phones sending text messages.[77] The act applies both to an "insider" who accesses a computer beyond his or her authority and an outsider such as a hacker who accesses a computer.[78] The federal courts have looked at whether it constitutes a violation of the CFAA when individuals have violated a website's terms of service agreement. Courts have held that a user would not know that violating a contract would result in a criminal penalty under the CFAA but in other cases the courts have held that fraudulent activities violating the terms of service agreements can violate the CFAA and constitute a

crime.[79] These cases will likely continue to be prosecuted as unauthorized access to computers and computer networks occur in a variety of different ways.

The differing court interpretations, along with technology that is constantly evolving, have made it difficult to be certain how the law is applied. The CFAA has been criticized as outdated, and specifically, the difference in treatment between stored communication that is 180 days or older has been viewed as arbitrary. Many privacy advocates believe that stored electronic communication should be protected with better privacy regulations regardless of how long the information has been stored. Similarly, privacy advocates have argued that terms of service should not require users to allow their information to be scanned by the host, particularly for targeted advertising. In 2017, Google said it would stop scanning e-mails for targeted advertising in response to consumer privacy security concerns.[80] Google, like other e-mail providers, will continue to scan the e-mails for spam and phishing attacks.

One notable exception to privacy rights is when a person is at work. Individual rights related to computer content and electronic communications change when an employee is using an employer's computer or electronic device or an employer-issued e-mail. The courts have found that the Fourth Amendment protections that protect a person's home computer do not necessarily apply to individuals when the computer is owned by their employer, or when a person is using file-sharing software.[81] Courts have also ruled that e-mail accounts provided by an employer and used for employment purposes are not private to the individual employee, but may have some privacy protections when the employee is using a personal account incidentally at work.[82]

Similar to the issue of monitoring employee's behavior via computer and e-mail use, employees have seen retaliation in hiring and firing when employers monitor their social media activity. Federal legislation was introduced in 2013 to prohibit employers and institutions of higher education from requesting social media account information, but the bills did not pass through either the House of Representatives or the Senate.[83] Some states have passed legislation related to the ability of employers, and in some cases schools and higher education institutions, to access their employees' and students' social media accounts. While more than two dozen states have introduced legislation to limit employers from requesting social media names and passwords, only a few have a current law prohibiting the practice.[84] Legislation was introduced in Minnesota in 2016 and 2017 prohibiting schools and employers from requesting social media usernames and passwords, but no law has been enacted.[85]

Federal Laws Govern Privacy and Protection of Children

Children's Online Privacy Protection Act of 1998 (COPPA) is a federal law aimed at protecting the online privacy of children under the age of 13.[86] COPPA prohibits websites from collecting certain information from children covered under the act without parental consent and provides guidelines for how information can be deleted.[87] The FTC has accompanying rules for enforcement of COPPA. The FTC guidelines for websites and online services provides that websites must:

- post privacy policies consistent with COPPA;
- gain parental consent before collecting personal information about children;

- give parents the ability to view information collected on their children and delete the information that a company has on their children;
- take reasonable steps to maintain the confidentiality and security of children's personal information; and
- keep children's personal information only as long as reasonably necessary.

The FTC website indicates that COPPA applies to mobile apps, Internet gaming platforms, Internet-based location services, VoIP services, and toys that connect to the Internet.[88] The FTC prosecutes actions for COPPA violations as unfair trade practices.[89] COPPA also provides that state attorneys general can prosecute for COPPA violations and obtain damages for violations of the federal law. The New York State Attorney General investigated and found violations of COPPA by four children's toy companies in 2016.[90] While COPPA does not provide for a private right of action, in August 2017 class action cases were filed in a California federal district court against Viacom and the Walt Disney Company, alleging violations of COPPA and violations of state privacy laws, which raise questions about private claims of action for violations of COPPA.[91]

COPPA has been criticized for being difficult to use by businesses, who have to try to verify parental consent before collecting information from a child, which can be onerous. The FTC does have a "Safe Harbors" rule that allows industry groups to create guidelines and show compliance with COPPA, but generally the process to verify a parent's consent involves communicating individually with each parent, which then also requires additional personal information to be supplied by the parent.[92] COPPA has also been criticized for not having a private right of action, which means consumers need to rely on the FTC or a state's attorney general to bring an action and often means individual claims are left without redress.

The FTC has said that schools can also consent for youth covered under COPPA. Nothing in COPPA or the FTC rules specifically gives this permission to schools, but generally when the website is for the purposes of education, the school can act in lieu of the parents. When permission applies and what the schools need to communicate to parents to stay in compliance of COPPA causes some confusion.[93] Some state laws regulate student data privacy and student web access in addition to COPPA and may be more protective over student use of the Internet. It is unclear who would be in violation of COPPA (the website or the school) if a parent's permission was not provided consistent with what COPPA requires. It is also unclear if the school has the ability to request that data be deleted consistent with the requirements of COPPA, although it is likely a parent can still request that the student's data be deleted. Generally, school districts need to consider gaining parental consent for the websites their children are accessing online.

The Children's Internet Protection Act (CIPA) encourages public libraries to install software to block obscene or pornographic materials so that children do not access the material or are not exposed to it in public libraries and school libraries. The federal law allows libraries and schools that install the blocking software to access reduced rates to Internet services. The law requires blocking software that prevents obscene material and pornography from being accessed on the Internet,[94] but allows blocking software to be turned off if needed for an adult to do valid research. The law also requires the library or school library to adopt Internet safety and education policies, which include educating students about online safety and monitoring student Internet activities. CIPA was challenged shortly after it was enacted on First Amendment grounds, but

the Supreme Court ruled that CIPA did not violate the First Amendment rights of individuals and students.[95]

States have also passed laws similar to CIPA to require libraries or schools to install blocking software on public or school computers accessed by minors. The National Conference of State Legislatures has identified 25 states that have passed provisions similar to CIPA.[96] Some state laws require Internet service providers to allow customers the ability to install blocking software on home computers to protect minors.[97]

Minnesota law requires public libraries to use software to prevent minors who use the computers from being exposed to materials "reasonably believed to be obscene or child pornography or material harmful to minors under federal or state law."[98] Minnesota law also requires all public libraries that receive state funding to block access to child pornography or obscene materials to both children and adults.[99]

Critics of CIPA, and state laws similar to CIPA, have argued that it can be difficult for libraries to know which websites must be blocked under the law, and in an effort to comply with CIPA and similar state provisions, libraries may be blocking more websites than necessary or censoring information that would not otherwise be blocked from public access.

Student data privacy has been an important topic for many state legislatures in the last few years. Family Educational Rights and Privacy Act (FERPA) is the federal law on student data and covers the privacy of student records generally.[100] But the use of Internet sites, cloud computing, and many new software applications have raised issues about whether or not student data is protected when it is collected and retained by many third-party vendors that provide these new electronic services. Many states have introduced or enacted legislation to address concerns related to the data that schools, state agencies, and private third-party contractors collect on students.[101] These legislative proposals and new laws cover a variety of topics including the following:

- what data can be collected and shared by a school, school district, or state agency
- guidelines for contracts between schools and third-party vendors, including vendors who provide data storage (including cloud storage), electronic devices to the school and students, and education software applications
- limits on how student data is used by the school or third-party contractors, including prohibitions on targeted advertising or building student profiles for commercial purposes
- access to student data by the student, parent or guardian, or the state
- how student data can be used for longitudinal studies
- how and when student data must be kept or destroyed

Minnesota has not enacted a comprehensive student data privacy law but legislation has been introduced in recent years covering some of these topics.[102] Minnesota has specific student data provisions in the Minnesota Data Practices Act that govern the privacy requirements for student data collected by schools and state agencies.[103]

Federal Law Addresses Financial Data and Identity Theft

The Gramm-Leach-Bliley Act (GLBA) is a federal financial services privacy law enacted in 1999.[104] The law covers financial institutions, which includes companies that lend, borrow, or wire money, or who provide financial or investment services, including debt collectors. The GLBA limits when private personal financial information can be disclosed and requires customers to be notified of the privacy policies and information-sharing practices. It also requires financial institutions to advise customers of their right to opt out of having their financial information disclosed to any third parties. The law also requires third parties who obtain financial information from financial institutions to keep the data private. Financial services institutions covered by the GLBA must also have reasonable safeguards to protect their customers' information. Companies must also watch for security breaches and protect nonpublic information pursuant to a number of federal laws and agency rules.[105] The penalties for noncompliance on the part of financial institutions can result in millions of dollars in fines and criminal sentences of up to five years. The FTC and the Federal Deposit Insurance Corporation are just two of the many federal agencies that enforce the provisions of these federal financial services privacy laws.[106]

The Identity Theft and Assumption Deterrence Act makes it a federal crime to use false identification to commit a crime.[107] This law allows for criminal prosecution against individuals who use a stolen identity to commit a federal, state, or local crime.

Health Information Is Protected by Separate Laws

Electronic health records, similar to the financial sector, also have specific federal privacy laws. The major health privacy law, Health Insurance Portability and Accountability Act (HIPPA), regulates the privacy and disclosure of electronic health care records. HIPPA applies to hospitals, health care providers, health plans, health care clearinghouses, and can include universities and other facilities that provide health care services. HIPPA requires individually identifiable health information to be kept private, using technical and administrative safeguards.[108] Violations of HIPPA are investigated by the U.S. Department of Health and Human Services Office for Civil Rights, and criminal prosecution for more serious violations are handled by the U.S. Department of Justice.

The Health Breach Notification Rule is a federal regulation issued by the FTC and covers entities that offer services related to health records, but which are not covered by HIPPA. This FTC rule covers vendors who offer to maintain electronic personal health records and third parties who work with vendors of electronic personal health records; the rule requires those businesses to provide notice to consumers when health information from those electronic personal health records have been obtained without authorization.[109]

Individual State Laws Also Address Privacy

State Internet privacy laws broadly addressing ISPs and websites are rare. But unlike most states, Minnesota has a law specifically addressing Internet privacy. Minnesota Statutes, chapter 325M, was passed in 2002 and prohibits an ISP from knowingly disclosing the consumer's personal information, including browsing history, to a third party.[110] The law provides a number

of exceptions similar to the Stored Communication Act for subpoenas and law enforcement officers, as well as when the disclosure of information is part of the normal course of business for the ISP, or when the customer has given written or electronic authorization for the disclosure.[111] The law can be enforced by a consumer filing a civil lawsuit against the ISP, and a consumer who prevails can be awarded attorneys fees, court costs, and actual damages or $500, whichever is higher. The law does not provide for enforcement from the state attorney general and the law specifically prohibits class actions based on Minnesota Statutes, chapter 325M.[112]

Besides the rush of state legislation that was introduced after Congress overturned the proposed FCC privacy rules in 2017, there have been many other state initiatives to address online privacy. California passed the California's Privacy Rights for California Minors in the Digital World Act in 2014, which allows minors to request that their content be erased from websites and also limits some targeted advertising to minors based on user profiles.[113] States have also passed laws to limit access to individual's records for e-reader book purchases, as well as privacy laws that require conspicuous posting of privacy policies on websites that collect personal information, and laws that require notice to employees when their work e-mail is monitored.[114] A few states have passed legislation on specific privacy issues such as student data, and some of these laws specifically related to the use and distribution of electronic records.[115]

Industry Standards and Consumer Expectations

Many of the current privacy protections offered to consumers do not come from federal or state mandates, but are offered by websites, search engines, social media, e-mail providers, ISPs, and broadband providers to consumers based on consumer demands. Many of these companies provide privacy policies in the terms of service and service contracts they enter with consumers and users. Consumers can use these privacy policies to learn more about what companies do with the information they receive, and also can use this as a basis for consumer protection violations if a company does not follow the privacy policy or the terms of service contract it enters with the consumer.

These privacy policies and terms of service contracts have been criticized because they can be changed without notice to the consumer or user, and often do change without a renewed consent from a customer or user. Once a consumer agrees to a "click wrap" agreement, companies often fail to notify customers that they have updated their privacy provisions, or changed the terms of service, and the only way for the consumer to know the terms have changed would be to go back and look for new terms or contact the company.

While some companies may change their privacy policies without giving notice, others strive to provide greater privacy protections to consumers to win customers from competitors. As companies garner a reputation for having better privacy protections, their reputation may increase interest in their company. Some have argued that bad press, and a bad reputation for protecting consumer privacy, can hurt a company enough to make privacy controls part of a competitive field for various Internet-based services, web-browsing, and electronic communication companies. Costly litigation from suits by consumers over privacy torts, data breaches, or violations of state or federal law create incentives for companies to adopt and follow stricter privacy policies. Companies have to avoid running afoul of state and federal privacy and

consumer protection laws; not doing so could result in lawsuits filed by state attorneys general or federal agencies like the FTC, which can include millions of dollars in penalties.

Some industries have started to create privacy initiatives to help consumers find companies that are using higher privacy standards or providing more privacy options to users. The Digital Advertising Alliance (DAA) is made up of a group of advertising and marketing trade groups. One of their initiatives, the "YourAdChoice" icon, which appears as a small icon on participating websites, allows the consumer to learn more about what information is collected and control the collection of their personal information.[116] This is one example of businesses responding to consumers' concerns over targeted advertising and privacy, but many other companies have made policy changes to respond to consumers concerns over privacy.[117]

Emerging Technologies Present New Challenges

Emerging technologies create new opportunities for commerce and innovation while also raising new concerns over how they affect consumer privacy. The pace of innovation is much faster than state and federal legislation can address it, and consumers often turn to the legislature to examine the new technologies for perceived privacy issues, as consumers are not always aware of how their use of the technology affects their privacy, personal data, and financial information. While use of many of these new technologies on smartphones, tablets, and via software applications is becoming common and largely seen as beneficial, the outdated privacy regulations have not kept up with these emerging technologies; this has created a gap between existing technology and communication systems governed by older comprehensive privacy laws and emerging technologies, which are most often unregulated. Among the new technology that Congress and state legislatures have looked at recently include geolocation, biometrics, and blockchain technology.

Geolocation is the wireless detection of people's real-time locations through smartphones, tablets, and other electronic devices that connect with Global Positioning System (GPS) satellites and cell towers. As technology becomes increasingly sophisticated, it is easier for companies to obtain and use this information, which raises concerns as to whether legislation will regulate and define boundaries related to the collection, sale, and use of geolocation data.

There is currently no federal law that regulates geolocation data. One of the major issues that has emerged is whether or not geolocation data can be accessed by the government without a warrant. Recent federal legislation would require a warrant for cloud and geolocation data to be obtained by the government.[118] The Location Privacy Protection Act was introduced in November 2015 to prohibit sharing geolocation data except under certain circumstances in order to prevent cyberstalking and protect victims of stalking and domestic violence.[119]

State legislation has moved much more quickly and 18 states currently require probable cause warrants to access cellphone location information. Some of the legislation currently under consideration would require companies to disclose data they collect and share with third parties.[120]

A pending U.S. Supreme Court case, *Carpenter v. United States*,[121] looks directly at the ability of law enforcement to access location data without a warrant in light of Fourth Amendment

protections. The decision in this case may prompt federal regulations or may cause states to look more closely at their existing laws.

Location-based services and geolocation tracking allow businesses to retrieve individualized data in targeted areas for marketing and advertising as well as providing services to customers. This creates privacy concerns for consumers who may not be aware of how often their location is tracked and stored, or what companies do with the information, for example whether or not their location information is shared or sold to other third parties or when the information can be accessed by the government. The 2012 decision in *United States v. Jones*[122] held that installing a GPS tracking device on Jones's vehicle without a warrant was an unlawful search under the Fourth Amendment. The Court found that the Fourth Amendment offers some protection against trespassing onto personal property, including vehicles, and rejected the government's argument that there was no reasonable expectation of privacy in a person's movement on public roads.

Geofencing is a popular location-based service. When you enter a virtual boundary, an action is triggered, such as texts, push notifications, or ads for something within the boundary. For example, if you are in the geographical "fence" surrounding Macy's, ads for the store may pop up in open applications attracting you to shop at the store. Specific ads can be targeted towards your browsing history and application preferences. Geofences are also used to prevent drone-related accidents in sensitive areas, such as the White House and airports, where they present threats to public safety.

Popular location-based services include Uber, Yelp, Facebook, and Maps. Any application that asks permission to use your location may be sharing it with third parties. Although people can turn off location, (1) it prevents the app from working properly, and (2) locations are still tracked through GPS signals and cell tower triangulation. It is possible that in today's technological era, users implicitly consent to sharing location information for individualized advertisements and Internet usage despite some inherent privacy concerns.

Blockchain technology provides for safer and faster cryptocurrency transacting. Each transaction is encrypted and placed on the chain or a decentralized public ledger. Then, its code links to the code encrypting the blocks before and after it, creating a somewhat impenetrable "chain link fence." To break one block, a hacker essentially must decrypt all preceding and proceeding blocks, a daunting and unrealistic task. These are reasons that corporations, individuals, and governments are attracted to blockchain transacting, recordkeeping, and smart contracting. Smart contracting consists of self-executing code that helps limit breaches and protect party identities. With every transaction, an individual's public address generates a receiving address. Constantly changing addresses make it more difficult to track entire payment histories, which enhances individual privacy. While blockchain provides many benefits, it raises questions about standardizing development and privacy standards. Its open-source nature presents regulation challenges.

Federal agencies provide initiatives addressing transparency, efficiency, and trust in blockchain information sharing.[123] Although Congress has not passed legislation, state legislatures have proactively identified blockchain records under evidentiary standards. Other initiatives establish guidelines for smart contracting and shifting government and corporate recordkeeping to the chain. The active states include Vermont, Arizona, Delaware, Illinois, and Nevada.[124]

Adopting blockchain technology can enhance security but also presents privacy concerns. Since the chain crosses jurisdictional boundaries concerning the ease of national and international transacting, it may be addressed by federal legislation in the coming years but until then state legislatures are actively looking at the issue.

Biometrics, a comprehensive measurement of human physical and behavioral characteristics, is an increasingly popular business practice employing retina scans, fingerprint IDs, and facial recognition technology. Biometric information is popular for fraud detection and prevention, especially to enhance security. Using biometrics decreases the likelihood of forging passwords, fingerprints, or unique identities and increases the convenience of password upkeep along with creating stronger authenticity with a nontransferable and secure password. Some of the privacy risks associated with the use of biometric technology include:

- a failure to capture full and complete data, causing system failures;
- stolen and compromised personal identities if storage servers are hacked;
- false identification allowing unauthorized access, also false rejection of authorized users; and
- integrating security features beyond mere traditional password solution encryption.

In November 2017, Apple[125] was granted a patent to implement a secret biometric ID and tracking measure that secretly photographs and video-archives unauthorized device users. This presents some privacy and security concerns. A few states have passed laws which require businesses to gain consent from individuals before collecting their behavioral activity. Illinois[126] and Texas[127] were first to implement biometrics legislation, followed by Washington[128] in May 2017. Most legislation regulates business biometric information use via biometric identifiers. Several states, including California, Connecticut, Arizona, and New York, have proposed similar legislation but the bills have not passed.

Facebook has been sued under the Illinois law for using a deep-learning facial recognition system that can identify a user whose face is hidden, by drawing from identifiers such as body shape, hair, and posture. Facebook and retail shops use facial recognition to identify repeat customers and shoplifters, as well as to deliver ads based on perceived emotions. Even tagging a friend on Facebook can implicate a person's biometric data for targeted ads and potential tracking. In situations such as this, legislative action may be required to deter companies' use of biometric information if consumers perceive this identification to be compromising their privacy. Greater consumer awareness may help abate privacy and security concerns.

Conclusion

Consumer protection laws and privacy laws are being stretched to accommodate an evolving online marketplace and the never-before-seen privacy considerations that online banking, social media, and e-commerce have raised. Existing consumer protection and privacy laws have been criticized for being designed for the "brick and mortar" world and ineffective at reaching the new problems caused by e-commerce and Internet activity. States, and the federal government, are now faced with the challenge of updating existing laws to address the new harms caused by data

breeches, identity theft, and consumer tracking and profiling that did not exist when many of the currently applicable consumer protection and privacy laws were written. These emerging technologies are giving rise to new legislative considerations and a growing body of case law that helps navigate how new technologies are treated by existing consumer protection and privacy laws.

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:

- Challenges and policy consideration for state regulation
- 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] U.S. Constitution, Amendment IV, states, "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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." See also *Katz v. United States*, in which the Court concluded that the Fourth Amendment protects people, not only places, and that the physical intrusion into the plaintiff's area was unnecessary to create Amendment protection. 389 U.S. 347, 88 S. Ct. 507 (1967).

[2] U.S. Constitution, Amendment XIV, Section 1, states, "No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." See also *Meyer v. Nebraska*, 262 U.S. 390, 43 S. Ct. 625 (1923); *Griswold v. Connecticut*, 381 U.S. 479, 85 S. Ct. 1678 (1965); *Stanley v. Georgia*, 394 U.S. 557, 89 S. Ct. 1243 (1969); *Roe v. Wade* 410 U.S. 113, 93 S. Ct. 705 (1973).

[3] See National Conference of State Legislatures, "Privacy Protections in State Constitutions," May 5, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[4] The following ten states have a right to privacy in their state constitutions: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.

[5] *Hill v. National Collegiate Athletic Ass.*, 865 P.2d 633 (Cal. S.C. 1994).

[6] *United States v. Lifshitz*, 369 F.3d 173 (2d Cir. 2004). In the case, the defendant was convicted of child pornography offenses; probation terms that allowed monitoring his computer use was crucial as the computer was

his weapon, and the court determined that specific searches could be done without violating the defendant's Fourth Amendment rights. *Guest v. Leis,* 255 F.3d 325 (6th Cir. 2001). The court found no Fourth Amendment violation for capture of private bulletin board post, treating the post like a letter that had already been sent, or an e-mail that had been received by a third party.

[7] Missouri Constitution, Article 1, Section 15, states "That the people shall be secure in their persons, papers, homes, effects, and electronic communication and data, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, or access electronic data or communication shall issue without describing the place to be searched, or the person or thing to be seized, or the data or communication to be accessed, as nearly as may be; nor without probable cause, supported by written oath or affirmation."

[8] An effort to pass the Uniform Computer Information Transaction Act (UCITA), which would create more validity for "shrink wrap" and "click wrap" agreements has failed to gain traction in most states. Only Virginia and Maryland have approved UCITA. An effort to amend similar provisions to the Uniform Commercial Code through a proposed article 2B governing licensing and similar agreements has not been adopted.

[9] Michael L. Rustad, *Global Internet Law*, St. Paul: West Academic Publishing, 2014, p. 187.

[10] U.S. courts have found that an Internet agreement must be unconscionable both in how the contract was formed (procedural) and in the content of the contract (substantive), see Rustad at 206. This is in contrast to the European system, which often only upholds these provisions in contracts between commercial entities.

[11] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), was an early case upholding software "shrink wrap" licensing agreement terms; *Caspi v. Microsoft Network LLC,* 732 A.2d 528 (N.J. Super. 1999), held that contract provision requiring cases to be brought in Washington state was valid as was the entire "click wrap" contract, as the provisions were presented in a manner the purchaser could read in an online subscriber with an online service company.

[12] Rustad, 208.

[13] Ibid.

[14] Rustad, 354, see *Bragg v. Linden Research, Inc.*, 487 F.Supp. 2d (593) (E.D. Pa. 2007), finding that interaction with a person in a virtual world can satisfy a state's minimum contact requirement to have personal jurisdiction and that the defendant's mandatory arbitration provision was unenforceable; *Scarcella v. America Online*, 798 N.Y.S. 2d 348 (2004), in which the Court found the forum selection clause, to litigate any dispute against AOL in Virginia, in the electronic AOL membership "click wrap" agreement was unenforceable.

[15] Rustad, 354; while it is common for courts to uphold arbitration agreements in "click wrap" or "browser wrap" agreements, courts have found that some arbitration provisions will not be upheld, see *Brower v. Gateway 2000, Inc.*, 246 A.D.2d 246, 676 N.Y.S.2d 569 (1st Dep't 1998), finding the fee required for a consumer to arbitrate was unconscionable.

[16] See *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), finding that a shrink wrap license is valid and thus enforceable as a contract. The defendant accepted the offer by clicking through and could have rejected the contract terms by returning the software.

[17] *Hubbert v. Dell Corp.,* 359 Ill. App. 3d 976 (2005), holding that hyperlinks on Dell Computer's website that linked to the company's terms of service were conspicuous and part of the contract made between the company and the purchaser.

[18] See *Forrest v. Verizon Communications,* 805 A.2d 1007 (D.C. Ct. App. 2002), finding that the forum selection clause was reasonable and enforceable and that the attorney would have seen the clause had he read through the agreement before accepting it.

[19] *Tompkins v. 23andMe, Inc., 840 F. 3d 1016* (9th Cir. 2016), finding arbitration clause in a contract of adhesion was enforceable based on an analysis under state and federal law.

[20] See *In re Zappos.com, Inc., Customer Data Sec. Breach Litigation,* 893 F.Supp.2d 1058 (D. Nev. 2012), holding that the website made no affirmative requirement for the consumer to agree to the terms of service and that the terms were not obvious to the purchaser. This case upheld the holding in *Van Tassell v. United Mktg. Grp.,* 795 F.Supp.2d 770, 790 (N.D.Ill. 2011), in which a browse wrap contract is valid if the user has actual and/or constructive knowledge of the website's terms and conditions. See also Mark A. Lemley, *Terms of Use,* 90 Minn.

L.Rev. 459, 477 (2006), where it was determined a court may overlook the absence of assent when there are other reasons indicating the user is or should be aware of the website owner's terms.

[21] *In re Zappos.com, Inc., Customer Data Sec. Breach Litigation*, 893 F.Supp.2d 1058 (D. Nev. 2012).

[22] S.J. Res. 34, P.L. 115-22 (April 3, 2017).

[23] For more information on the 2017 FCC Net Neutrality proposals see: https://www.fcc.gov/restoring-Internet-freedom.

[24] See "FCC Restoring Internet Freedom," https://www.fcc.gov/restoring-Internet-freedom.

[25] See "FCC Restoring Internet Freedom," https://www.fcc.gov/restoring-Internet-freedom.

[26] See National Conference of State Legislatures, "Privacy Legislation Related to Internet Service Providers," August 4, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-Internet-service-providers.aspx.

[27] Nevada S.B. 538, Chapter 570 (2017 Regular Session), https://www.leg.state.nv.us/Session/79th2017/Bills/SB/SB538_EN.pdf.

[28] See H.F. 2579/S.F. 2309, H.F. 2642, H.F. 2606/S.F. 2323, S.F. 1937, and the Omnibus Jobs Bill, S.F. 1937, 2nd Unofficial Engrossment, Article 9, Section 4 (2017).

[29] In 2016, the FCC proposed new rules to expand the Communication Act of 1934 to apply to ISPs and would have broadened the FCC's regulatory control over Internet privacy issues. The rules were scheduled to go into effect in December 2017 but in April 2017, before the rules had taken effect, they were overturned by Congress pursuant to the Congressional Review Act.

[30] 5 U.S.C. §§ 41-58, as amended.

[31] 15 U.S.C. §§ 41-58. In 2006, the FTC Act was expanded to allow cooperation, information sharing, and investigation with foreign countries to deal with new problems arising from Internet use and e-commerce. See "Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers beyond Borders Act of 2006," Pub. L. No. 109-455, 120 Stat. 3372 (2006).

[32] See the FTC website for a list of statutes the agency enforces: https://www.ftc.gov/enforcement/statutes.

[33] 16 C.F.R. Part 318 (2009); requiring companies covered under the rule to notify consumers and the FTC when health information has been improperly disseminated or obtained.

[34] *In re the Matter of Craig Brittain*, USA Federal Trade Commission, https://www.ftc.gov/news-events/press-releases/2015/01/website-operator-banned-revenge-porn-business-after-ftc-charges.

[35] *Federal Trade Commission v. LifeLock, Inc.*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=lifelock&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation. Trade Regulation Reporter, LifeLock, Inc.—Stipulated Order Resolving FTC's Allegations of Contempt and Modifying Stipulated Final Judgment and Order for Permanent Injunction, Commission statement and dissenting statement, FTC File No. 072 3069, announced December 17, 2015, ¶17,427, Federal Trade Commission.

[36] *Federal Trade Commission v. Ruby Corp., et al*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=ashley+madison&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison, Trade Regulation Reporter, Ashley Madison—Court complaint and consent decree, FTC File No. 152 3284, announced December 14, 2016, ¶17,602, Federal Trade Commission.

[37] *FTC v. TaxSlayer*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=taxslayer&field_document_description= and https://www.ftc.gov/news-events/commission-actions?title=taxslayer&type=All&field_date_value_2%5Bvalue%5D%5Byear%5D=&field_date_value%5Bvalue%5D%5Bmonth%5D=&items_per_page=20; Trade Regulation Reporter, TaxSlayer, LLC—Complaint and consent order, FTC Dkt. C-4626, File No. 162 3063, announced August 29, 2017; issued October 20, 2017, ¶17,720, Federal Trade Commission.

[38] *Federal Trade Commission, Christopher S. Porrino, Attorney General of the State of New Jersey, and Steve C. Lee, Director of the New Jersey Division of Consumer Affairs, Plaintiffs, v. VIZIO, Inc.*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=vizio&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc; Trade Regulation Reporter, VIZIO, Inc. and VIZIO Inscape Services, LLC—Court complaint and stipulated order, FTC File No. 162 3024, announced February 6, 2017, ¶17,634, Federal Trade Commission.

[39] This settlement was the result of a violation of an earlier settlement agreement with Google, *In re the Matter of Google, USA Federal Trade Commission*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=google&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/122-3237/google-inc; Trade Regulation Reporter, Google, Inc.—Complaint and consent order, FTC Dkt. C-4499, File No. 122 3237, announced September 4, 2014; issued December 2, 2014, ¶17,178, Federal Trade Commission.

[40] *In re the Matter of Facebook, Inc., USA Federal Trade Commission*, https://www.ftc.gov/enforcement/cases-proceedings/case-document-search?title=facebook&field_document_description= and https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc; Trade Regulation Reporter, Facebook, Inc.—Consent order and complaint, Dkt. No. C-4365, FTC No. 092 3184, announced November 29, 2011, complaint and consent order issued July 27, 2012, ¶16,672, Federal Trade Commission.

[41] Minn. Stat. §§ 325D.01 to 325D.07.

[42] Minn. Stat. §§ 325D.09 to 325D.16.

[43] Minn. Stat. §§ 325D.49 to 325D.66.

[44] Minn. Stat. §§ 325F.68 to 325F.70.

[45] Minn. Stat. § 8.31, subd. 3a. See *Ly v. Nystrom,* 615 N.W.2d 302 (Minn. 2000), holding that an individual must demonstrate his or her cause of action benefits the public and that a single fraudulent misrepresentation in one instance was not a matter of public interest.

[46] See Minnesota Statutes, section 8.31, for a list of consumer protection statutes enforced by the Office of Minnesota Attorney General.

[47] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

[48] 5 U.S.C. § 552a; See the Department of Justice website for a detailed overview of the Privacy Act, https://www.justice.gov/opcl/file/793026/download.

[49] 44 U.S.C. § 3501.

[50] 44 U.S.C. § 3541.

[51] Pub. L. No. 113-283 (2014).

[52] The term "political subdivision" includes counties, cities, school districts, special districts, boards, and commissions created by law. "State agencies" include all state-level government offices and boards, as well as the University of Minnesota.

[53] Minnesota Data Practices Act, chapter 13, presumes most government data is public but creates numerous exceptions for data that is private. See Minn. Stat. §§ 13.01-13.90.

[54] Minn. Stat. § 13.15.

[55] Minn. Stat. § 13.055.

[56] Minn. Stat. § 16E.016.

[57] See the Minnesota IT Services website for more information: https://mn.gov/mnit/programs/security/cyber/.

[58] Minn. Stat. § 16E.03.

[59] Minnesota law generally requires the state's electronic information and IT services to be accessible to individuals with disabilities consistent with federal laws, including section 508 of the Rehabilitation Act, United

States Code, title 29, section 794d, as amended by the Workforce Investment Act of 1998, Public Law 105-220, August 7, 1998, and the Web Content Accessibility Guidelines, 2.0, with some exceptions where the accessibility would be unduly burdensome. See Minn. Stat. § 16E.03, subd. 9.

[60] 18 U.S.C. §§ 2510-22.

[61] 18 U.S.C. § 3121.

[62] 18 U.S.C. §§ 2701-12.

[63] 18 U.S.C. §§ 2802-03.

[64] The Secured Communication Act (SCA) only allows electronic communications less than 180 days to be accessed by a warrant but allows content that is older than 180 days to be accessed by a warrant, subpoena, or court order. 18 U.S.C. § 2703(d).

[65] 18 U.S.C. § 2707.

[66] See *Crispin v. Christian Audigier*, 717 F.Supp.2d (C.D. Cal. 2010), V*iacom Intern. Inc.*, *YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008).

[67] See *In re Facebook Internet Tracking Litigation*, 2017 WL 2834113 (N.D. Cal. 2017). The federal district court in California found that Facebook's tracking of browser data was not a violation of the SCA, the Wiretap Act, the California Invasion of Privacy Act, or California's Comprehensive Computer Data Access and Fraud Act.

[68] *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. 2012), holding that the Stored Communications Act does not apply to data stored in a personal cell phone; *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012), finding that disclosing a unique device identifying number, personal data, and/or geolocation information to third parties is not an egregious breach of privacy that would sustain a serious invasion of a privacy interest.

[69] *U.S. v. Meregildo*, 883 F.Supp.2d 523 (S.D.N.Y. 2012).

[70] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[71] Ibid.

[72] See *Disciplinary Counsel v. Brockler*, 145 Ohio St.3d 270, 2016-Ohio-657.

[73] 18 U.S.C. § 1030, Pub. L. No. 99-474 (Oct. 16, 1986).

[74] 18 U.S.C. § 1030(g).

[75] 18 U.S.C. § 1030.

[76] See 18 U.S.C. § 1030(e)(2)(B); *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009).

[77] See *U.S. v. Kramer*, 631 F.3d 900 (8th Cir. 2011), holding that a cell phone could be considered a computer based on the broad definition of computer in the CFAA.

[78] See *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007), Fifth Circuit Court of Appeals upheld the conviction against a university student for hacking into a university computer system and stealing Social Security numbers, finding that it was an unauthorized attack on the university's computers.

[79] See *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), after a young girl committed suicide from online bullying, prosecutors brought criminal charges under the CFAA against the adult who bullied the girl. The court found that the CFAA's "unauthorized use" provision could not extend to using MySpace's website in violation of the terms of service agreement because the average person would not know that violating a terms of use agreement with a website would be a crime, and the CFAA did not include a provision that indicated that contract violations were a crime. *U.S. v. Lowson*, 2010 WL 9552416 (Dist. N.J. 2010) found that a ticket-buying scheme in violation of Ticketmaster's terms of service could be prosecuted under the FCAA. *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016), found that a former employee who no longer had access to employer's computer system was in violation of CFAA when he used current employees' login information to gain access to his former employer's computer data.

[80] Daisuke Wakabayashi, "Google Will No Longer Scan Gmail for Ad Targeting" *The New York Times*, June

23, 2017.

[81] In *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002), the court found no reasonable expectation to privacy regarding an employer-owned computer in which there was also a clear policy that the computer and its contents were not confidential. In *United States v. Ganoe*, 538 F.3d 1117 (9th Cir. 2008) the court found no reasonable privacy expectation for computers that have active file-sharing software installed.

[82] *Ontario v. Quon*, 560 U.S. 746 (2010), holding that searching personal texts on government-issued cell phones was a proper work-related search and did not violate the employee's Fourth Amendment rights; *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N. J. S. 2010), holding that an employee had some expectation of privacy while using her personal e-mail account on a company computer; conversely, *McLauren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999) found that password-protected personal folders on the company network accessed via a company computer did not carry privacy expectations; *TBG Insurance Services Corp. v. Superior Ct.*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002) similarly found searching an employer-owned computer at the employee's home does not violate Fourth Amendment rights; and finally, *Garrity v. John Hancock Mutual Life Insurance Co.*, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) found no privacy rights regarding e-mails on the employer's computer network.

[83] Social Networking Online Protection Act, https://www.congress.gov/bill/113th-congress/house-bill/537/actions.

[84] The states with legislation prohibiting employers from obtaining current or prospective employees' usernames and passwords of social media accounts include: California, Illinois, Maryland, Michigan, Nevada, New Mexico, New Jersey, Utah, Washington, and Wisconsin; see ABA "Employee Monitoring and Workplace Privacy Law" for more information, https://www.americanbar.org/content/dam/aba/events/labor_law/2016/04/tech/papers/monitoring_ella.authcheckdam.pdf. Whereas 15 states considered legislation in 2016 prohibiting prospective or current employers or colleges/universities from accessing individual personal accounts, the following states enacted legislation: Illinois, Nebraska, Virginia, and West Virginia; see NCSL "Access to Social Media Usernames and Passwords" for more information on introduced legislation, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

[85] See Minnesota bills from the 2016 legislative session: H.F. 2385/S.F. 2703 and H.F. 2386/S.F. 2705; and the 2017 legislative session: H.F. 2116/S.F. 2038 and H.F. 2591/S.F. 2320.

[86] 15 U.S.C. §§ 6501-6506.

[87] Personal information for the purposes of COPPA can include a child's name, address, location, e-mail address, screen name, telephone number, Social Security number, photo/video/image, or parent's information.

[88] See FTC website on COPPA compliance for Internet businesses, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#step1.

[89] 16 C.F.R. § 312 (2013).

[90] Lily Hay Newman, "NY Cracks Down on Mattel and Hasbro for Tracking Kids Online," *Wired*, September 13, 2016, https://www.wired.com/2016/09/ny-cracks-mattel-hasbro-tracking-kids-online/.

[91] See *Rushing v. The Walt Disney Company*, Northern Dist. California, Case No. 3:17-cv-4419; *Rushing v. Viacom, Inc.*, Northern Dist. California, Case No. 3:17-cv-4492; see also *In re: Nickelodeon Consumer Privacy Litigation*, No. 15-1441 (3rd Cir. App. 2016) finding that a common law cause of action for privacy ("right of seclusion") was not preempted by COPPA.

[92] 16 C.F.R. Part 312; Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505; see the FTC website for a list of COPPA Safe Harbors programs, https://www.ftc.gov/safe-harbor-program.

[93] Benjamin Herold, "COPPA and Schools: The (Other) Federal Student Privacy Law, Explained," *Education Week*, July 28, 2017.

[94] 47 U.S.C. § 254(h)(5)(B) "[E]nforcing a policy of Internet safety for minors that includes monitoring the online activities of minors and the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are—(I) obscene; (II) child pornography; or (III) harmful to minors; (ii) is enforcing the operation of such technology protection

measure during any use of such computers by minors; and (iii) as part of its Internet safety policy is educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response." The term "harmful to minors" and other terms are defined in CIPA.

[95] *United States v. American Library Assn., Inc.*, 539 U.S. 194, 201 F. Supp. 2d 401 (2003), holding that Congress has the authority to require libraries to censor Internet content to receive federal funding under the CIPA without violating First Amendment rights.

[96] National Conference of State Legislatures, "Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries" November 6, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/state-Internet-filtering-laws.aspx.

[97] A number of states have passed laws that require Internet service providers to provide information or access to blocking and filtering products to allow customers to control children's access to the Internet. See La. Rev. Stat. § 51:1426; Md. Code § 14-3701 et seq., Nev. Rev. Stat. § 603.100 to 603.170, Tex. Bus. & Comm. Code §§ 35.101 to 35.103, Utah Code § 76-10-1231.

[98] Minn. Stat. § 134.50.

[99] *Ibid.*

[100] 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

[101] National Conference of State Legislatures, "Student Data Privacy," February 10, 2017, http://www.ncsl.org/research/education/student-data-privacy.aspx.

[102] See H.F. 1507 (2017), https://www.revisor.mn.gov/bills/text.php?session=ls90&number=HF1507&session_number=0&session_year=2017&version=list; S.F. 1980 (2017), https://www.revisor.mn.gov/bills/text.php?number=SF1980&version=0&session=ls90&session_year=2017&session_number=0 and H.F. 307, https://www.revisor.mn.gov/bills/text.php?number=HF307&version=0&session=ls90&session_year=2017&session_number=0.

[103] Minn. Stat. §§ 13.319 to 13.33.

[104] 15 U.S.C. §§ 6801-6809.

[105] The USA Patriot Act Section 314, FDIC Rules and Regulations, and the Sarbanes-Oxley Act all contain privacy provisions requiring monitoring and security requirements for personal information on financial accounts.

[106] 15 U.S.C. § 6805.

[107] 18 U.S.C. § 1028.

[108] 45 C.F.R. § 164.530(c).

[109] 16 C.F.R. Part 318.

[110] Minn. Stat. § 325M.02.

[111] Minn. Stat. §§ 325M.03 and 325M.04.

[112] Minn. Stat. § 325M.07.

[113] Calif. Bus. & Prof. Code §§ 22580-22582.

[114] See National Conference of State Legislatures, "State Laws Related to Internet Privacy," June 20, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-Internet-privacy.aspx#CollectPI.

[115] See National Conference of State Legislatures, "Student Data Privacy," February 10, 2017, http://www.ncsl.org/research/education/student-data-privacy.aspx.

[116] See YourAdChoice.com for more information, http://youradchoices.com/learn#learn-icon.

[117] Brian Fung, "Gmail Will No Longer Snoop on Your Emails for Advertising Purposes," *The Washington Post*, June 26, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/06/26/gmail-will-no-longer-snoop-on-your-emails-for-advertising-purposes/?utm_term=.10cbdff5606b.

[118] Federal legislation: Online Communications and Geolocation Protection Act, which was reintroduced in February 2015, places geolocation and cloud computing data in a similar position to e-mails under the SCA. This bill also updates the SCA making all e-mails, regardless of how old the e-mail is, accessible only with a warrant, https://www.congress.gov/bill/114th-congress/house-bill/656.

[119] Federal legislation: Location Privacy Protection Act, https://www.congress.gov/bill/112th-congress/senate-bill/1223.

[120] Illinois legislation: Still under consideration is Illinois's *Right to Know Act* which would require companies like Google and Facebook to disclose the data they collect and share with third parties, http://www.ilga.gov/legislation/billstatus.asp?DocNum=2774&GAID=14&GA=100&DocTypeID=HB&LegID=104098&SessionID=91.

[121] On appeal from the Sixth Circuit Court of Appeals, *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016).

[122] 565 U.S. 400, 132 S. Ct. 945 (2012).

[123] The U.S. federal blockchain program was recently launched by the Government Services Administration (GSA) to discuss blockchain features that federal agencies and U.S. businesses should be aware of. National Conference of State Legislatures, "Blockchain Technology: An Emerging Public Policy Issue," http://www.ncsl.org/documents/legisbriefs/2017/lb_2544.pdf.

[124] Vermont was the first in 2015-2016 to sign S.135, permitting broader business and legal application of blockchain technology to advance economic development, http://legislature.vermont.gov/assets/Documents/2018/Docs/ACTS/ACT069/ACT069%20Act%20Summary.pdf. In March 2017, Arizona enacted H.B. 2417 and H.B. 2216, which (1) establish guidelines for electronic signatures, smart contracts, and records, and (2) make it illegal to require someone to use or be subject to electronic firearm tracking technology, https://legiscan.com/AZ/text/HB2216/2017 and https://www.azleg.gov/legtext/53leg/1r/bills/hb2417p.pdf. In July 2017, Delaware enacted S.B. 69, giving corporations authority to use blockchain to create and maintain corporate records. The act protects corporations from lawsuits for storing information on the chain, https://legis.delaware.gov/BillDetail/24232. Illinois created the Illinois Blockchain Initiative and Illinois Legislative Blockchain and Distributed Ledger Task Force to analyze how governments could benefit from blockchain recordkeeping and service delivery. They also seek to support businesses to adopt chain use, https://illinoisblockchain.tech. Nevada enacted legislation recognizing blockchain and smart contracts as electronic records. It is also the first state to prohibit local governments from taxing and restricting their use, https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf.

[125] Apple Biometrics Patent, http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9,819,676.PN.&OS=PN/9,819,676&RS=PN/9,819,676.

[126] Illinois Biometric Information Privacy Act, passed in 2008, addresses the collection and storage of biometric identifiers and information. This act creates a private right of action for statutory violations and has led to an increase in lawsuits, specifically those in class action, http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[127] Texas Business and Commerce Code, Title 11, A. Ch. 503 Biometric Identifiers limits legal action to the state's attorney general, so that individuals cannot sue, http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.503.htm.

[128] Washington H.B. 1493 prohibits any person from using a biometric identifier in a database for commercial use without first providing notice, gaining consent, or creating a way to prevent subsequent use of the identifier commercially, http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/Session%20Laws/House/1493-S.SL.pdf#page=1.