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: Jurisdiction and Procedure in Internet Law Cases

This 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.

Civil procedure has changed rapidly in the last few years as electronic court filing systems, electronic service, and electronic signatures have become more common. This brief discusses some of the common jurisdictional issues and how the Internet has affected legal procedure.

Contents

About The Internet and Public Policy Series

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

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

Service

Electronic service, either via electronic court software systems, e-mail, or even through social media, are relatively new avenues for providing proper service in courts in the United States. Traditional service was exclusively done personally through the U.S. Postal Service or via publications. The courts have recently found that service by e-mail could be reasonably calculated to give the party notice of the action.[1] Google and social media are also now considered important avenues for communication and, in some cases, may even be necessary avenues to exhaust a search for a party's contact information for service.[2]

The rules of service in many states are provided through the judiciary and are sometimes provided in statute. The Minnesota Rules of Civil Procedure and the Minnesota General Rules of Practice provide information about service requirements for civil cases in Minnesota. The new e-filing rules have removed some of the previous requirements for "conventional" service and do not require an affidavit to prove service when the e-filing system is used.[3]

Discovery and Evidence

Evidence for both civil and criminal matters can come from social media websites, commercial websites, and private and employer-owned e-mail accounts. This electronic content is now often included in discovery requests, and courts generally apply the same paper discovery rules to electronic discovery. Attorneys must advise their clients to preserve social media and e-mail and not to destroy evidence on computers or software applications.[4] Furthermore, social media content, even when made private, is not shielded from discovery.[5] According to the Federal Rules of Civil Procedure, a document request may specify the form in which the information should be produced. If a request does not specify the form, then the party is expected to produce the information in the form ordinarily maintained or reasonably usable. The same rules apply for information requested in a subpoena.

Because e-mails and social media accounts often have a great deal of personal information contained in them, people are hesitant to turn over copies or allow open-ended access of those

accounts to an opposing party. A party to an action can request a protective order to limit the scope of discoverable information and can sometimes include a "pull back" stipulation or court order in which the party can call back a privileged document that was inadvertently produced during a discovery request. In *Giacchetto v. Patchogue-Medford Union Free Sch. Dist.*, 293 F.R.D. 112 (E.D.N.Y. 2013), the court found that the plaintiff was only required to produce postings from a social media account with a specific reference to the claims, rather than exposing her entire social media account, regardless of whether the settings were public or private.

The responsibility to turn over electronic evidence falls on the parties to the case. Companies that manage intern services, provide devices, host e-mail, and run social media websites are not obligated to provide that information to third parties and generally will not do so because it has been viewed as a violation of the Stored Communications Act.[6] Wall postings are not protected as temporary or intermediate storage, but courts have found that some Facebook posts can be protected from disclosure, but usually not if the post on a website is completely public.[7] Some courts have allowed subpoenas to websites in civil matters.[8] Court decisions have not been consistent in permitting civil subpoenas of social media information. Generally, courts find subpoenas less likely for private messages between two parties and for information requests that are not likely to lead to discovering admissible evidence.

There are not a lot of resources for lost computer data beyond hiring a computer forensic expert to try to retrieve the information.[9] Computer forensic experts can usually retrieve information deleted from computers, e-mails, and servers. Experts make digital copies of the device that is then studied and use software to examine it, searching for deleted, encrypted, or damaged files. The cost varies depending on how big the drive is, the type of media, and operating system. For example, a small 80 GB hard drive could take between 15 and 35 hours to examine, costing $250 or more per hour. Some advantages of computer forensics include the ability to search large amounts of data quickly and recover lost or deleted data that can be used in court cases. But there are sometimes high costs to recover the data, including expert testimony to prove how the data was investigated, and tampered with or destroyed, along with the fact that the process may reveal some privileged data.

Federal and state rules of evidence are evolving to meet the demand for discovery of electronic materials. The Federal Rules of Evidence had "e-discovery" amendments that came into effect on December 1, 2006.[10] Minnesota adopted many of the federal changes regarding electronic discovery in 2007.[11]

Jurisdiction and Venue

Choosing where to file a case depends on which court has jurisdiction. Deciding whether a case is brought in federal or state court and which state the case is brought in will depend on which court has jurisdiction. The following discusses some of the common jurisdictional issues and how they are dealt with in Internet law cases, as well as policy considerations about Internet law and jurisdiction.

Most laws related to Internet activity are federal laws and provide for federal jurisdiction, and so it is common for many Internet cases, both civil and criminal, to end up in federal court. However, actions that are brought under state laws, both existing tort and contract law as well as recent legislation specifically related to Internet conduct, do occur. As states continue to pass more laws regarding online conduct and offer claimants an opportunity for relief in state courts, it is likely that more cases will be brought in state court.

Minnesota law provides jurisdiction for corporations or nonresidents when the act committed outside of Minnesota causes injury or property damage in Minnesota and when Minnesota's exercise of jurisdiction would not violate principles of fairness and substantial justice.[12] This personal jurisdiction standard over nonresidents is provided in Minnesota Statutes, section 543.19. This "long-arm statute" provides for jurisdiction in state court over a nonresident when the person or corporation owns or possesses real or personal property in Minnesota, transacts business in the state, or commits an act causing injury or property damage in the state. Jurisdiction can also extend to out-of-state people or corporations if they commit an act outside the state that causes personal injury or property damage in Minnesota, unless Minnesota has no substantial interest in providing a forum or the burden placed on the defendant would violate fairness and substantial justice. This last clause is the most likely to create the grounds for an extension of jurisdiction over someone outside Minnesota who may have harmed someone inside Minnesota through the use of the Internet.

The Due Process Clause in the Fourteenth Amendment to the U.S. Constitution provides that the state court's exercise of personal jurisdiction over nonresidents must require certain minimum contacts so that the exercise of jurisdiction does not violate traditional notions of fair play and substantial justice.[13] For both state court and federal court actions, the court has to determine if the court has jurisdiction over the parties in the case. In cases where a contract or service agreement has not determined jurisdiction, or where it is in dispute, the federal courts have found that Internet jurisdiction cases require the same personal jurisdiction analysis as other types of cases to find that the court has either general or specific jurisdiction. If the defendant raises the issue of inconvenient forum, then the *forum non-conveniens* analysis will also be applied to the case, which means the court will look at various factors to determine if that jurisdiction would be an appropriate forum.[14] While the courts have to grapple with new concepts in these Internet cases, the federal courts continue to apply the basic personal jurisdiction analysis that exists for other types of civil cases.

The federal courts will apply the general jurisdiction test to see if the person or company has many contacts with a state. As this is not often the case in Internet cases, the court often has to look to the long-arm statutes that allow the court to exert their jurisdiction over parties in other states to see if the requirements in statute have been met and whether or not the exercise of jurisdiction would violate the defendant's due process rights.

When the court cannot find general jurisdiction, the court will look to see if specific jurisdiction can be found. This requires that an actor directed their actions at the resident in the forum state and that the injury was related to that action.[15] Recent Internet cases have found that specific jurisdiction requires more than just feeling the effects in that forum but requires that the defendant "targeted" the forum.[16] The federal case law that developed over personal jurisdiction focuses on the amount of contact a person had with a district that is attempting to exert its

jurisdiction over that person. The court looks at whether or not the defendant purposefully established contacts with that state, often called "purposeful ailment."[17]

Operating a globally accessible website is not enough to create either general or specific jurisdiction. Instead, the courts have looked at whether or not a website is passive or active and specifically, if there are online commercial orders.[18] The courts have found that having an interactive website is also not enough to create jurisdiction. In *ALS Scan v. Digital Services Consultants, Inc.,* 293 F.3d 707 (4th Cir. 2002), the federal district court looked at whether or not a person "directed electronic activity into the state" to engage in business or another activity and that activity creates a cause of action.[19] Federal courts have found that the interactivity of a website and the ability to purchase from that website will not be enough to establish jurisdiction. The court noted the result that could occur, "If we were to conclude as a general principle . . . placing information on the Internet subjects a person to personal jurisdiction in each state in which the information is accessed, then the defense of personal jurisdiction, in the sense that a State has geographically limited judicial power, would no longer exist."[20]

Many terms of service and use agreements require the user to agree to choice of forum clauses, which means that the user has agreed to the jurisdiction identified by the contract, usually the state of incorporation or operation of the company.[21] These agreements are enforced by the federal court system, so when a company has included a "choice of forum" clause in the licensing or user agreement, it will dictate which federal or state court the case must be brought in.

There is no set international jurisdiction for cases regarding the Internet. U.S. courts make determinations impacting foreign companies and U.S. companies are regularly sued in foreign jurisdictions as well. The European Union has a regulation structure that affects all member countries and the companies and citizens in those countries. The Brussels Regulation provides the parameters of jurisdiction for companies doing business in those countries.[22] Because there is no uniformity worldwide and no international treaty to govern Internet law jurisdiction, there will continue to be many questions about where consumers and companies can sue and be sued.

States that are drafting new provisions on jurisdiction should consider their state rules of civil and criminal procedure for that state and how the long-arm personal jurisdiction statute has been interpreted. State court constitutions have vested the power to determine jurisdiction with different branches of government. In Minnesota, the court rules are determined by the judicial branch. In his textbook, *Global Internet Law*, Professor Michael Rustad notes that basing jurisdiction on the location of servers is not advisable because "it could make any Internet subscriber subject to personal jurisdiction."[23]

Venue in both civil and criminal cases related to Internet activity can be hard to determine. In civil cases, venue is usually where the cause of action arose or where the defendant to the action resides. In criminal cases, the venue is almost always where the crime occurred but criminal activity online can make that location difficult to determine.[24] Many of the early federal computer crimes did not specifically address venue and courts have found venue to be where the major loss or harm occurs, where the "transmission" occurs, and where the actor acted to enter a network or transferred files.[25]

Consumer protection advocates, and victim advocates in criminal cases, may encourage broad venue provisions to allow cases to occur wherever a victim resides or wherever an Internet transaction occurred. Legislation should take into consideration the constitutional requirements in criminal cases, as well as the existing state statutes related to criminal and civil venue.

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
- Privacy and consumer protection
- Cybertorts and property rights online
- Criminal activity on the Internet
- 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] *Snyder v. Energy Inc.*, 857 NY S 2nd 442 (2008), the court allowed service by e-mail when it appeared the defendant had read an e-mail sent to the known e-mail address, when multiple e-mails with service were sent for service, when the defendant was notified by telephone that service had been attempted, and when service was also sent to the defendant's last known address. See also, Jeffery Wolber, "Opening a Can of Worms and Viruses: The Impact of E-Service on E-Mail Users Everywhere," *New York Law School Law Review*, 61 (2016–2017): 449.

[2] *Munster v. Groce*, 829 NE 2d 52 (Ind. Ct. App. 2005), holding service was not proper when no real effort was documented on attempts to find the defendant's current address, which could have included searching the Internet to obtain his address; *Mpafe v. Mpafe*, Hennepin County Family Court, MN No. 27-FA-11-3453 (2011), the judge issued an order allowing service via social media sites and e-mail, indicating that traditional forms of service by publication were antiquated and unlikely to reach the defendant.

[3] See Minnesota Rules of Civil Procedure, Rule 4, Service; and Minnesota Rules of General Practice, Rule 7, Proof of Service.

[4] See *Allied Concrete Co. v. Lester*, 736 SE2d 699 (Va 2013), the trial court acted to mitigate the prejudice to the defendant caused by the plaintiff's deceptive actions, including destroying and altering his Facebook page after a discovery request was made.

[5] See *E.E.O.C. v. Simply Storage Mgmt*, 270. FRD 430 (S.D. Ind. May 11, 2010), holding that social network profiles were not protected from discovery merely because they are locked or private and that it had to be produced when relevant to a claim; *Reid v. Ingerman Smith LLP*, No. CV 2012-0307 (ILG)(MDG), 2012 U.S. Dist. LEXIS 182439 (E.D.N.Y. Dec. 27, 2012), the court affirmed the *E.E.O.C.* decision, noting that discovering private social media accounts parallels discovering personal diaries, as long as they are relevant.

[6] Relying on the SCA, 18 U.S.C. § 2701, most websites, e-mail hosts, and social media sites turn down subpoenas for information and discovery in civil matters. The SCA does provide specific procedures for government

agencies and law enforcement in criminal investigations to gain e-mail and messages from websites using court orders, warrants, and subpoenas. See 18 U.S.C. §§ 2701-2712. If a party does not comply in a civil case, the opposing party can get a court order for a signed release and sometimes obtain the information with the release from the account holder.

[7] See *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965 (2010), the court identified social media services as both an electronic communication service and a remote computing service. Unopened private messages make sites like Facebook an electronic communication service provider, while open messages make the entity a remote computing service provider and the court may treat these communications differently under the SCA.

[8] See *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (Sup. Ct. 2010), in which the court found the defendant's discovery request permissible and did not violate the plaintiff's right to privacy.

[9] The Wayback Machine is an example of an Internet archive that can be used to provide an authentic screen shot of the Internet on a specific date or time period. See James L. Quarles III, Richard A. Crudo, "[Way]Back to the Future: Using the Wayback Machine in Patent Litigation," *ABA Journal*, January/February 2014, https://www.americanbar.org/publications/landslide/2013-14/january-february/wayback_the_future.html.

[10] See Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, and 45. Subsequent notable updates to electronic discovery and discovery rules generally also occurred in 2015.

[11] See Minnesota Rules of Civil Procedure, Rules 16, 26, 34, 37, and 45.

[12] Minn. Stat. § 543.19.

[13] See *Pervasive Software Inc v. Lexware GMBH and Co.*, 688 F.3d 214, 220 (5th Cir. 2012), holding that Texas did not have jurisdiction over the contract dispute when the software at issue was purchased from a German company and none of the defendant's actions occurred in or were directed at Texas, the plaintiff could not establish the necessary contacts for specific jurisdiction.

[14] The *forum non-conveniens* analysis looks at access to evidence, witnesses, premises, the cost of trying the case in a certain place, and the public interest in where the case is tried. See Michael L. Rustad, *Global Internet Law*, St. Paul: West Academic Publishing, 2014, p. 144.

[15] Rustad, 156.

[16] Rustad, 157.

[17] Rustad, 157-158.

[18] Rustad, 142-144. See *Zippo Manufacturing Co. v. Zippo Dot Com*, Inc. 952 F. Supp. 1119 (W.D. Pa. 1997).

[19] Rustad, 161.

[20] Rustad, 161, quoting *ALS Scan v. Digital Services Consultants, Inc.*, 293 F.3d 707, 712 (2002).

[21] Rustad, 143.

[22] Rustad, 169.

[23] Rustad, 156.

[24] U.S. Const. art. III, § 2, cl. 3; U.S. Const. amend. VI.; see also Federal Rules of Criminal Procedure, Rule 18.

[25] Office of Legal Education Executive Office for United States Attorneys, "Prosecuting Computer Crimes" OLE Litigation Series (2015), pp. 116-120, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.