ELEPHANTS AND MICE REVISITED: LAW AND CHOICE OF LAW ON THE INTERNET

PETER P. SWIRE[†]

By definition, an essential question of cyberlaw is to define when law will affect actions in cyberspace. Such law might be uniform, such as where nations have entered into a treaty or have adopted the same legal rule. Or, such law might be diverse, such as where nations adopt different legal rules.

Diversity of law often does not matter for physical acts, such as where the criminal law of one country simply does not apply to acts performed in a foreign country. On the Internet, however, diversity of law poses a fundamental challenge. Each surfer on a website might be from a foreign jurisdiction, with laws unknown to the owner of the site. Similarly, each website visited by a surfer might be hosted in a foreign jurisdiction, with laws unknown to the surfer. Every encounter in cyberspace, therefore, raises the possibility that diverse laws will apply. The rules for choosing among diverse laws—the subject of this part of the Symposium on "Choice of Law and Jurisdiction on the Internet"—thus appear uniquely important for cyberspace.

Surprisingly, however, the number of actual cases addressing choice of law on the Internet is far, far lower than the initial analysis would suggest. Although there is the *possibility* of diverse national laws in every Internet encounter, some mysterious mechanisms are reducing the *actual* conflicts to a handful of cases.

This Article seeks to explain those mysterious mechanisms. It does not primarily address the prescriptive task of saying what the optimal rules should be for resolving conflicting national laws that affect the Internet. Instead, it takes on a descriptive task. It treats choice of law on the Internet as a dependent variable; the task is to explain when and how choice-of-law rules actually matter on the Internet.

[†] Professor of Law and John Glenn Scholar of Public Policy Research, Moritz College of Law of the Ohio State University. My thanks for helpful comments from participants at the University of Pennsylvania Law Review Symposium on the Conflict of Laws, a workshop at the Moritz College of Law, and from students in my Law of Cyberspace seminar in the fall of 2004. My thanks also for helpful conversations with Jack Goldsmith, Bill Kovacic, and Joel Reidenberg, research support from the John Glenn Institute, and research assistance from Matthew Kleckner.

That choice-of-law question, in turn, overlaps considerably with the even broader question—when and how does *any* rule of law actually matter on the Internet?

In order to deepen our understanding of the effects of legal rules generally and of choice-of-law rules in particular, this Article compares current Internet legal issues with the list of issues described in my 1998 article, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*.[1] The historical comparison shows that most of the current choice-of-law topics were already identified in the earlier period. The chief exception concerns cybercrime and related computer security topics, which were only dimly seen on the horizon in 1998.

The discussion then turns to the mysterious mechanisms that have reduced the possibility of incessant choice-of-law disputes down to the actual handful of cases. Four significant filters exist before a court must choose among conflicting national laws: technology's ability to trump law; lack of jurisdiction over defendants; the harmonization of diverse laws; and the existence of self-regulatory and other systems that suppress choice-of-law conflicts for transactions. For a core concern of the earlier article—business sales to consumers over the Internet[2]—this last filter has proven decisive in avoiding choice-of-law conflicts.

Only a small subset of disputes makes it through all four filters. For those that do, this Article offers a new typology for the categories of residual disputes. First, harms can occur to third parties who are not bound by contracts between surfers and websites. Those harms can happen to owners of intellectual property, where laws have not been harmonized. They can also happen in tort, most prominently for the tort of defamation. Second, conflicts can occur for a limited number of issues involving significant moral, political, or constitutional differences among nations. To date, the most prominent disputes have involved speech protected by the First Amendment to the U.S. Constitution. In the future, we can expect occasional, albeit important, court decisions that seek to choose among national laws in the event of diverse laws.

---

[1] Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW. 991 (1998).

[2] *See id.* at 1016-17 (relating the importance of the Internet to international business and consumer sales).

I. THE TOPICS OF INTERNET LAW

Many of the major current topics of Internet law, which can lead to international choice-of-law disputes, were identified in the 1998 article.[3] A variety of consumer-protection and other issues can arise as individuals surf on foreign web pages or buy from foreign sites. Intellectual property disputes are manifest, notably for copyrights and trademarks. Privacy and data protection issues exist, such as when protective rules in Europe are not matched by laws in the United States and other countries. Content that is objectionable in some jurisdictions is legal in others. Notable examples include hate speech, pornography, and treasonable or politically censored speech. On the Internet, where everyone can be a publisher, digital defamation can easily occur.

In 1998, it was also possible to identify the types of business issues that would be troublesome on the Internet and potentially raise choice-of-law issues. Taxation becomes more complex as commerce shifts to the Net and away from identified import/export companies. Countries vary in their acceptance of gambling and other business activities. Looking ahead, in a world of outsourcing and offshoring, there will likely be increasing issues concerning professional licensing and the application of local labor laws to Internet activities.

Strikingly, the 1998 list missed a dark side of international Internet behavior. Even for those of us immersed in researching the Internet, there was little or no attention paid to the importance of computer security and cybercrime, much less to the potential use of the Internet for terrorist activity.[4] Since 1998, the Internet commu-

---

[3] *See id.* at 1017-19 (describing eleven areas where choice-of-law issues might arise on the Internet).

[4] The 1998 article was written after over two hundred interviews conducted for PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (1998).

There were, of course, experts involved in Internet security and cybercrime by the time of the 1998 article. The point here, which is striking in retrospect, is the very low level of awareness of those issues at the time even among Internet experts. A presentation on the National Cybercrime Training Partnership (NCTP) by a lawyer for the U.S. Department of Justice Computer Crime & Intellectual Property Section gives a sense of the initial phases of national and international awareness of cybercrime as of January 1999. *See* WAYNE P. WILLIAMS, NCTP VISION, MISSION, AND STRATEGY 13 (1999) (showing very early steps taken to address U.S. and international cybercrime from 1994 to 1998), *available at* http://www.wjin.net/Pubs/2476.pdf (last visited Mar. 21, 2005). My own education on these topics was accelerated during my time in government, when I participated in activities such as: the drafting of an interagency report on unlawful conduct on the Internet, THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT

nity has become far more aware of crime and security-related issues, which often occur across national borders. These issues include computer hacking, diffusion of computer viruses, identity theft, phishing,[5] and spyware. Another related topic that has expanded in importance concerns a different sort of unwanted intrusion into a user's computer, through spam.

In short, the Internet makes it easy and inexpensive for an actor in one country to affect another country. The number of potential transborder legal disputes, which contain choice-of-law issues, seems enormous.

II. DOES TECHNOLOGY TRUMP LAW? THE METAPHOR OF ELEPHANTS AND MICE

As discussed in the 1998 article,[6] the hope and belief of many Internet pioneers was that geography would prove "a virtually meaningless construct on the Internet."[7] In that early era, there were brave declarations that "the Internet treats censorship as damage, and routes around it," or "national borders aren't even speedbumps on the Information Highway."[8] For these Internet pioneers, the vision was that technology would trump law.

The 1998 article introduced the metaphor of elephants and mice to explain when that vision was provably false or else substantially held true.[9] In short, "elephants" are organizations that will be subject to

---

ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last visited Mar. 21, 2005); working on computer security issues for federal agency systems; and working in late 2000 on discussions concerning the Council of Europe Cybercrime Convention, Convention on Cybercrime, *opened for signature* Nov. 23, 2001, S. TREATY DOC. NO. 108-11 (2003), Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc.

[5] Phishing refers to the use of scam e-mails to acquire an individual's private information for identity theft. Webopedia Computer Dictionary, *Phishing*, *at* http://www.webopedia.com/Term/p/phishing.html (last modified Mar. 11, 2005).

[6] *See* Swire, *supra* note 1, at 991-92 (describing the shift from a romantic to a legalistic attitude toward the Internet).

[7] *Id.* at 991 (quoting Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997)).

[8] *Id.* at 991-92 (quoting Posting of Timothy C. May to owner-cypherpunks@toad.com (Feb. 13, 1997) and Posting of John Young to owner-cypherpunks@toad.com (Apr. 5, 1998)).

[9] See *id.* at 1019-22 for an explanation of the metaphor of elephants and mice and how legal rules affect each.

the law, while "mice" can hope to ignore it. Elephants are large companies or other organizations that have major operations in a country. Elephants are powerful and have a thick skin, but are impossible to hide. They are undoubtedly subject to a country's jurisdiction. Once laws are enacted, they likely will have to comply. By contrast, mice are small and mobile actors, such as pornography sites or copyright violators, who can reopen immediately after being kicked off of a server or can move offshore. Mice breed annoyingly quickly—new sites can open at any time. Where harm over the Internet is caused by mice, hidden in crannies in the network, traditional legal enforcement is more difficult.

Applied to choice of law, the earlier article explained how the metaphor of elephants and mice suggests where international choice-of-law rules are most likely to be important:

> Elephants are often subject to jurisdiction in multiple countries. When disputes arise, the issue quickly becomes which sovereign's rules will apply—the classic choice of law question. As international sales to consumers become more prominent, choice of law disputes will often arise between the seller's country and the individual's national consumer protection law. On the other hand, the legal regulation of mice will more rarely implicate choice of law issues. The mice will disguise their identity, dispute jurisdiction, and hide their assets from judgment. Only rarely will they emerge into the light of open court to assert a defense based on choice of law.[10]

The activities of mice, I believe, were what the early Internet pioneers were implicitly assuming when they claimed that national laws would have little effect on cyberspace. There are two key features to violations of law caused by mice—it is hard to stop one mouse, and there is rarely only one mouse. Think about the difficulty in tracking one virus writer or one person who illegally distributes copyrighted songs and pictures over the Internet. Next, think about how much more difficult it is to try to stop all virus writers or all those who illegally distribute copyrighted material.

There are strategies in the physical world for catching mice and stopping them (or at least most of them) from getting at the food in the pantry. Analogous strategies exist for the virtual world, and are discussed further in the Conclusion. Where those strategies are not in place, however, mice will often be able to evade the effects of law. Current examples include: hackers who attack systems remotely; virus writers; sites that show content that is illegal locally (such as pornog-

---

[10] *Id.* at 1025.

raphy, hate speech, or speech otherwise censored by the local regime); Internet scams, including phishing; and illegal copying of copyrighted songs, photos, and other material. One current example that is causing particular problems for the Internet is the flood of unauthorized commercial e-mail, or spam. The (perhaps rabid) mice who send spam go to great lengths to stay hidden, and often operate offshore to make tracing and enforcement more difficult.[11]

By contrast, elephants have to be much more mindful of the law. They may use their bulk and strength to lobby and otherwise help shape the law. Elephants also have thick hides, as they deploy legal counsel, public relations agencies, and other means to defend themselves in court and otherwise to discourage regulatory actions. When a serious legal regime exists, however, elephants will find it expensive to ignore it. For instance, a large company will have to pay large penalties if it violates copyright law on its website. For privacy, companies with large databases, such as credit card companies and airline reservation systems, will not escape the regulators' notice. In general, it will be difficult to ignore a local sovereign if the elephant has employees and assets in that jurisdiction. In these instances, technology will not trump law, even when activities are conducted via the Internet. Where multiple countries have jurisdiction over an elephant, then choice-of-law rules can indeed dictate the outcome of a dispute.

---

[11] According to then-Federal Trade Commission Chairman Timothy J. Muris:

> Even with incredibly painstaking, expensive, and time-consuming investigation, it is often impossible to determine where spam originates. Spammers are extremely adroit at concealing the paths that their messages travel to get to recipients' in-boxes. Typically, the most that can be ascertained with certainty is the last computer through which the spam traversed immediately before arriving at its final destination. To frustrate law enforcers, clever spammers may arrange for this penultimate computer to be outside the country where the spam's ultimate recipient is located.

Timothy J. Muris, FTC, Unsolicited Commercial Email, Prepared Statement Before the Senate Committee on Commerce, Science and Transportation (May 20, 2004), *available at* http://www.ftc.gov/speeches/muris/040520spamemailtest.pdf (last visited Mar. 21, 2005). Chairman Muris also commented specifically on "spammers' willingness to ignore the law." *Id.* A spammer's willingness to ignore the law in general reinforces the conclusion that choice-of-law rules in particular will have little relevance to deterring spammers.

III. IS THERE JURISDICTION?

Where technology does not provide immunity, potential defendants can hope that jurisdiction does not apply. Courts who lack jurisdiction—literally, the ability to "say the law"—never get to the subsequent topic of choosing which law to apply. A possible explanation for the paucity of conflicts cases, therefore, would be if jurisdiction is lacking for Internet activities.

That explanation, however, does not work well. At least for commercial actors who use the Internet to sell into another country, there will very often be jurisdiction both in the country of the seller and the buyer. The country of the seller will typically be a place of business, with "continuous and systematic" contacts, so the seller's country will have general jurisdiction.[12] Controversy has centered on when there is also jurisdiction in the country of the surfer or buyer. The United States has been more hesitant to find such jurisdiction than have European countries.

Even under U.S. law as it has developed, however, typical commercial activities on the Internet are sufficient to create jurisdiction in the state or nation of the buyer. The early Internet cases often used the so-called *Zippo* test, which found jurisdiction for "interactive" websites but not for "passive" ones.[13] Over time, the position of U.S. courts has evolved. Jurisdiction scholar Allan Stein sums up the current state of the law: "[T]here must be evidence that the defendant 'purposefully availed' itself of conducting activity in the forum state, by directly targeting its web site to the state, knowingly interacting with residents of the forum state via its web site, or through sufficient other related contacts."[14] In the European Union, the revisions to the Brussels Convention have clarified the law for business-to-consumer transactions over the Internet: jurisdiction will generally exist in the buyer's country, and judgments from that country will generally be enforced in other European countries.[15]

---

[12] Int'l Shoe Co. v. Washington, 326 U.S. 310, 317 (1945).

[13] *See* Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) ("A passive Web site . . . is not grounds for the exercise [of] personal jurisdiction.").

[14] Allan R. Stein, *Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision*, 98 NW. U. L. REV. 411, 432 (2004) (quoting Toys "R" Us, Inc. v. Step Two, S.A., 318 F.3d 446, 454 (3d Cir. 2003)).

[15] Council Regulation 44/2001, arts. 5, 38, 2001 O.J. (L 12) 1, 4, 11. For a discussion of the revisions to the Brussels Convention, see Cindy Chen, Comment, *United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce*, 25 U. PA. J. INT'L ECON. L. 423 (2004).

These legal rules make it quite likely that Internet vendors will be subject to jurisdiction in the country of the buyer. A leader in the American Bar Association working on this topic expressed the resulting concern: "Businesses may forgo the efficiency and accessibility of electronic commerce if faced with the 'litigious nightmare' of being subject to suit in every jurisdiction on the globe."[16] In response, there are some steps that e-commerce companies are taking to reduce the risk of being haled into court in some distant and perhaps unknown jurisdiction. A useful study led by Professor Michael Geist found:

> Some companies, particularly those situated in North America, seek to influence jurisdictional outcomes by using both technological and legal approaches to mitigate risk. The most common methods to achieve this include the insertion of legal terms on websites, the use of a local server, the use of a national (country-code) top domain name, or the posting of local content.[17]

The use of a local server, a local domain name, and local content all would help prove that only the local market was being targeted for business by that website. Such strategies might help convince a court that the site is not meeting the U.S. test for "purposely availing" itself of other markets. It is far less clear, however, that such strategies would create a defense against jurisdiction under the law of the European Union or other nations that follow the country of destination approach.

Perhaps these strategies, however, serve as practical rather than legal defenses against lawsuits in foreign jurisdictions. There is evidence from the Geist survey that supports this view. For companies that adjusted their business operations in response to Internet jurisdiction risk, as many targeted lower-risk jurisdictions as sought to reduce activity in higher-risk jurisdictions.[18] Targeting lower-risk jurisdictions does not create a legal barrier to other buyers. It does, however, reduce the practical likelihood of suit in unexpected countries. As discussed further below,[19] the transaction patterns that sur-

---

[16] Thomas P. Vartanian, *A U.S. Perspective on the Global Jurisdictional Checkpoints in Cyberspace* (1999), *available at* http://www.ilpf.org/events/jurisdiction/presentations/vartanianpr.htm (last visited Mar. 21, 2005).

[17] MICHAEL GEIST, INTERNET JURISDICTION SUB-COMM., AM. BAR ASS'N, GLOBAL INTERNET JURISDICTION: THE ABA/ICC SURVEY 3 (2004), *available at* http://www.mgblog.com/resc/Global%20Internet%20Survey.pdf.

[18] *See id.* at 14 (noting that roughly twelve percent of companies surveyed were in each category).

[19] *See infra* Part V.

vive on the Internet seem to be those that reduce the risk of jurisdictional and choice-of-law disputes.

For the elephants of Internet commerce, then, jurisdiction will rarely be a successful defense. Noncommercial activities, which merely announce information through a website, have a stronger likelihood of a successful defense to jurisdiction, under the U.S. if not the European approach. For the mice, their strategy of hiding entirely will often be more effective than denying jurisdiction. If they create significant harms in another jurisdiction, then the courts of that nation are likely to strive mightily to find a way to state the law.

IV. IS THERE HARMONIZATION AS A MATTER OF LAW?

If technology does not trump law, and there is jurisdiction, then there may be no conflicts among national laws due to harmonization of the applicable legal rules. Scholars including Colin Bennett[20] and Justin Hughes[21] have emphasized how convergence of legal rules, or in some instances complete harmonization, is the central way that nations have avoided conflicts on data protection, intellectual property, and other cyberlaw areas.

In partial disagreement with Professors Bennett and Hughes, my own view is that formal adoption of harmonized legal rules has not been especially widespread for the troublesome topics of cyberlaw. Professor Hughes, who participated in World Intellectual Property Organization negotiations, has correctly highlighted the effectiveness of WIPO in harmonizing important parts of copyright and other intellectual property law. Professor Bennett, a data protection expert, has correctly described privacy harmonization that developed for some countries, notably for members of the European Union under the Data Protection Directive. With that said, formal, multinational institutions designed to harmonize law have not been largely successful for cyberlaw topics. Professor Hughes himself admits that the set of issues protected by the First Amendment to the U.S. Constitution is a major exception to his otherwise optimistic view of convergence of legal systems.[22] This Article will briefly examine four topics of proposed harmonization, in roughly descending order of the success at getting global agreement: cybercrime, data protection, enforcement of con-

---

[20] COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES (1992).

[21] Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. REV. 359 (2003).

[22] *Id.* at 391-93.

sumer-protection laws, and jurisdiction and enforcement of judgments.

A. *The Council of Europe Cybercrime Convention*

There has been one prominent harmonization effort in the area of Internet-related criminal law. The Council of Europe Cybercrime Convention was signed by over thirty countries, including the United States, in 2001.[23] As stated by the U.S. Department of Justice, the Convention is:

> [T]he first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. . . . (1) requiring signatory countries to establish certain substantive offenses in the area of computer crime, (2) requiring Parties to adopt domestic procedural laws to investigate computer crimes, and (3) providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems.[24]

The Convention has come under sharp attack, often justifiably, on a number of fronts.[25] Notably, the Convention calls for increased surveillance powers with no similarly detailed standards to protect privacy and limit governmental use of such powers. With that said, my view is that it is important to adapt law enforcement investigations to the reality that many cybercrimes involve communications that pass through multiple countries. The Convention seeks to harmonize domestic definitions of cybercrime, so that similar behavior is considered

---

[23] For the text and commentary of the Convention, see Convention on Cybercrime, *supra* note 4. Signatories are listed on the Council of Europe's website, at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (last visited Mar. 21, 2005). Ten additional countries have signed on since November 2001. *Id.*

[24] U.S. DEP'T OF JUSTICE, FREQUENTLY ASKED QUESTIONS AND ANSWERS: COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, *at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (last modified Nov. 10, 2003).

[25] I agree with many of the points in CTR. FOR DEMOCRACY & TECH., COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY ON THE COUNCIL OF EUROPE DRAFT "CONVENTION ON CYBER-CRIME" (DRAFT NO. 25) (2001), *at* http://www.cdt.org/international/cybercrime/010206cdt.shtml (critiquing the expansive reach of the Convention, with the potential for violations of privacy). For an extensive history and critique of the Convention, see YAMAN AKDENIZ, AN ADVOCACY HANDBOOK FOR THE NON GOVERNMENTAL ORGANISATIONS: THE COUNCIL OF EUROPE'S CYBER-CRIME CONVENTION 2001 AND THE ADDITIONAL PROTOCOL ON THE CRIMINALIZATION OF ACTS OF A RACIST OR XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS (rev. ed. 2004), *at* http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.

criminal.[26] It also aims to achieve fast and effective international cooperation to investigate and deter cybercrime.[27] As has been seen in some major computer attacks to date, the absence of international agreement on these topics has permitted clearly criminal behavior to go unpunished.[28]

Despite these goals of harmonizing cybercrime law and procedures for pursuing joint investigations, only nine countries had ratified the Convention as of the time of this writing.[29] It is doubtful that sanctions will be enforced against countries that fail to enact conforming substantive law or fail to cooperate in investigations.

B. *Data Protection Harmonization and the Safe Harbor*

The 1998 article had an extensive discussion of choice-of-law issues under the European Union Data Protection Directive.[30] That discussion highlighted the potential that E.U. Member States would interpret Article 4 of the Directive broadly, to apply even to websites in the United States and elsewhere that did not sell any products inside the E.U. Although there has been no formal statement by regulators forswearing that broad reading, actual enforcement has not been nearly so broad. Instead, I believe that all of the privacy enforcement actions by E.U. Member States have been predicated on activity that took place within the E.U.

One reason for the lack of extraterritorial enforcement (and the consequent lack of authoritative resolution of choice-of-law issues) has been the Safe Harbor agreement reached between the United States and the European Union in 2000.[31] The Safe Harbor created a lim-

---

[26] Convention on Cybercrime, *supra* note 4, arts. 2-13, Europ. T.S. No. 185 at 4-8.

[27] For a generally favorable review of the Convention, including analysis of cross-border remote searches, see Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 106-07.

[28] *Cf. 'Love Bug' Virus Case Dropped in Philippines; No Legal Grounds for Trial of Student*, WASH. POST, Aug. 22, 2000, at A12 (reporting the dismissal of charges against a defendant because the Philippines did not have a criminal statute covering computer hacking).

[29] See the list of signatories on the Council of Europe's website, *supra* note 23, for their ratification status.

[30] *See* Swire, *supra* note 1, at 998-1015 (analyzing harmonization under the Directive).

[31] *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45,665, 45,665-86 (July 24, 2000) (providing the Safe Harbor Principles and a set of frequently asked questions for consideration by the European Commission); Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided

ited, but significant, degree of harmonization of privacy standards between the level required under the E.U. Data Protection Directive and that provided under U.S. law. Organizations that subscribe to the seven Safe Harbor Principles of notice, choice, onward transfer, access, security, data integrity, and enforcement are considered to provide adequate privacy protection and thus may export personal data from the European Union to the United States. These seven principles are not identical to the protections required within the European Union, but do track the key fair information principles protected under European law.

There has been substantial criticism of the Safe Harbor. Privacy supporters have criticized it for not being protective enough of privacy.[32] Detractors have noted the relatively small number of organizations that have formally enrolled in the Safe Harbor program.[33] A lingering concern is that the entire financial services sector, which is central to transborder data flows, is excluded from the scope of the Safe Harbor.[34]

---

by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7, 7-9 (declaring that organizations that adopt the Safe Harbor Principles provide adequate protection of personal data for the purposes of the Directive). *See generally* U.S. Dep't of Commerce, *Welcome to the Safe Harbor*, *at* http://www.export.gov/safeharbor (last modified Mar. 2, 2005) (providing complete information and documents on the Safe Harbor). In my position as Chief Counselor for Privacy in the Clinton Administration, I was involved in the negotiations of the Safe Harbor, supporting the efforts of David Aaron and the late Barbara Wellbery.

[32] *See, e.g.*, Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 719 (2001) (arguing that the Safe Harbor "is only a weak, seriously flawed solution for e-commerce"). For the 2004 review by the European Commission of the operation of the Safe Harbor, see Comm'n of the Eur. Communities, *The Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce* (Comm'n Staff, Working Doc. No. SEC(04)1323, 2004) [hereinafter Commission Staff Working Document], *available at* http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/sec-2004-1323_en.pdf (last visited Mar. 21, 2005).

For an analysis of how the E.U. data protection laws have exerted pressure to harmonize to a stricter level of privacy protection, see Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 55-88 (2000).

[33] The number has grown over time, however, with 401 in November 2003 and 688 as of March 22, 2005, although not all organizations have kept their certifications current. Commission Staff Working Document, *supra* note 32, at 5 (citing the 401 figure). Current registrants are available at http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (last visited Mar. 21, 2005).

[34] The Safe Harbor applies to organizations under the jurisdiction of the Federal Trade Commission and the U.S. Department of Transportation, but not to organiza-

With that said, my own view is that the Safe Harbor has been fairly successful at meeting two strategic goals: avoiding a trans-Atlantic trade war and providing a reasonable baseline for privacy protection in transborder activities. Agreement on the Safe Harbor succeeded on a political level, allowing the Europeans to point to agreement on significant privacy protections on data transferred to the United States, and allowing the United States to point to the relatively manageable compliance costs of the Safe Harbor principles. Agreement on the Safe Harbor can also be defended as a "soft" harmonization of privacy law.[35] Both for organizations who have formally enrolled in the Safe Harbor, and for the larger group of organizations who are aware of the Safe Harbor, the Safe Harbor principles give a widely known set of rules for what is considered appropriate corporate action. Even though most companies will never face an enforcement action or a privacy audit, any organization that deviates substantially from the Safe Harbor principles runs the risk of exposure and enforcement. The potential number of choice-of-law cases involving privacy is greatly reduced under this soft version of harmonization that gives notice to organizations about key, expected privacy protections.

C. *Harmonized Consumer-Protection Enforcement*

An even softer form of harmonization is seen with regard to consumer protection for cross-border transactions. The International Consumer Protection and Enforcement Network (ICPEN) was founded in 1992 and now includes the U.S. Federal Trade Commission and agencies from twenty-eight other countries.[36] Much of ICPEN's work to date has been to share information about common problems facing enforcement agencies, and to spread better practices for en-

---

tions governed by financial regulatory agencies such as the Federal Reserve, the Securities and Exchange Commission, and the Office of the Comptroller of the Currency. For a discussion of the complex jurisdictional and substantive issues that have prevented use of the Safe Harbor for financial institutions, see Kyle Thomas Sammin, Note, *Any Port in a Storm: The Safe Harbor, the Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, 36 GEO. WASH. INT'L L. REV. 653, 657-71 (2004).

[35] *See generally* Andrew T. Guzman, *A Compliance-Based Theory of International Law*, 90 CAL. L. REV. 1823, 1872-73 (2002) (defining "soft law" in relation to the traditional sources of international law, such as treaties and customary international law).

[36] Int'l Consumer Prot. & Enforcement Network (ICPEN), *About ICPEN*, *at* http://www.icpen.org/imsn/abouticpen.htm (last visited Mar. 21, 2005).

forcement activities.[37] To promote consistent international enforcement, member agencies have participated in "sweep days" that target a specific category of Internet scams in different countries on the same day.[38] In 2000, member agencies issued findings on cross-border remedies, identifying areas "where the ability of IMSN members collectively to protect consumers and foster consumer confidence is limited. Members expect that the growth of e-commerce will make these limitations increasingly problematic."[39] For the foreseeable future, harmonization is likely to proceed in the areas of information sharing and some extension of cross-border remedies, but not through adoption of harmonized substantive law for consumer protection.

D. *The Hague Convention on Jurisdiction and Enforcement of Judgments*

A major harmonization effort in the area of jurisdiction and enforcement of judgments has thus far stalled. The proposed Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters was designed, among other things, to set up harmonized rules for determining which jurisdiction's laws should apply to business-to-consumer transactions over the Internet.[40] Particular controversy has accompanied Article 7 of the proposed Convention. Negotiators have put forward a number of variations that seek to compromise between the country-of-destination rule (favored

---

[37] Interview with William Kovacic, former General Counsel of the Federal Trade Commission (Jan. 21, 2005). Another cross-border forum for developing best practices for consumer issues is the Committee on Consumer Policy of the Organization of Economic Cooperation and Development. Org. for Econ. Co-operation & Dev., *Consumer Policy*, *at* http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html (last visited Mar. 21, 2005).

[38] *See* ICPEN, *Activities*, *at* http://www.icpen.org/imsn/activities.htm (last visited Mar. 21, 2005) (describing sweep days and the success of Sweep Day 2004).

[39] INT'L MKTG. SUPERVISION NETWORK (IMSN), FINDINGS ON CROSS-BORDER REMEDIES, *at* http://www.icpen.org/imsn/cross%20border%20findings.htm (last visited Mar. 21, 2005). (IMSN is the former name of ICPEN.)

[40] There has been considerable writing about the proposed Convention. For one recent article that collects sources, see Timothy P. Lester, *Globalized Automatic Choice of Forum: Where Do Internet Consumers Sue? Proposed Article 7 of the Hague Convention on International Jurisdiction and Foreign Judgments in Civil and Commercial Matters and Its Possible Effects on e-Commerce*, 9 NEW ENG. J. INT'L & COMP. L. 431 (2003). For a discussion highlighting controversial aspects of the proposed Convention other than choice of forum, see Stephen B. Burbank, *Jurisdictional Equilibration, the Proposed Hague Convention and Progress in National Law*, 49 AM. J. COMP. L. 203 (2001). The working documents of the proposed Hague Convention can be accessed at http://hcch.e-vision.nl/index_en.php?act=progress.listing&cat=4.

by European countries and consumer advocates) and rules that give more weight to the seller's country of origin (favored by the United States and e-commerce companies). One area of possible eventual compromise would be to give country-of-origin treatment to transactions where the seller does not have notice of the location of the buyer.[41] Until this issue is resolved, it appears highly unlikely that there will be formal harmonization for jurisdiction and enforcement of judgments.

V. STRUCTURING TRANSACTIONS TO AVOID CHOICE-OF-LAW PROBLEMS

The three previous filters have given limited protection to elephants against facing choice-of-law disputes: the ability of technology to trump law applies primarily to mice; jurisdiction is likely to exist in both the country of origin and the country of destination for many consumer transactions; and effective harmonization exists in only a limited subset of areas of law. This Part argues that a fourth filter screens out the bulk of potential disputes—the structuring of online transactions in ways that avoid choice-of-law problems.

For business-to-business transactions over the Internet, this screening process is rarely controversial. Legal regimes, including the U.N. Convention on Contracts for the International Sale of Goods, generally allow the parties to select by contract which forum's law will apply.[42]

For business-to-consumer transactions, however, the growth of e-commerce has been influenced by the risks introduced at the begin-

---

[41] *See* Lester, *supra* note 40, app. II at 479-89 (providing multiple proposed variants of Article 7). At the risk of stepping on a hornet's nest, my own view is that it likely makes sense to have country-of-origin treatment for some categories of transactions where the seller does not have notice of the buyer's jurisdiction. In many transactions, the seller learns the buyer's delivery address or other information that gives notice of the buyer's jurisdiction. From the seller's side, much of the perceived jurisdictional risk of participating in e-commerce would be eliminated if the seller could develop good information about the buyer's jurisdiction and then decide whether to do business in that jurisdiction. By reducing the total risk to both sellers and buyers, this approach is quite possibly the best in terms of encouraging e-commerce. The sellers can reduce much of the perceived jurisdictional risk, while ordinary consumers can have confidence that the transaction will be governed by the familiar law of their home country.

[42] United Nations Convention on Contracts for the International Sale of Goods, *done* Apr. 11, 1980, S. TREATY DOC. NO. 98-9 (1983), 1489 U.N.T.S. 3 (entered into force Jan. 1, 1988); *see also* Swire, *supra* note 1, at 993-98 (describing relevant EU law and the Convention's place within it).

ning of the Article—the fear by the surfer that the website will impose unfamiliar laws and the fear by the seller that the buyer comes from a jurisdiction that imposes unfamiliar laws. With the breakdown of talks in the Hague Convention,[43] we are likely to continue to have legal uncertainty about precisely which laws will apply to which sorts of transactions.

The result, I suggest, has been the migration of online transactions to largely unforeseen structures that greatly reduce the risk of choice-of-law disputes. I explored three major examples of these structures in a 2003 article called *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*.[44] That article described three early beliefs about how commerce would take place on the Internet.[45] First, payments would be made with new e-cash systems. Second, new "pure play" Internet retailers would defeat the stodgy companies that had physical stores. Third, using the wonderful power of search engines, buyers and sellers would interact directly and without the need for intermediaries.

Each of these predictions has turned out to be wrong, and in ways that greatly reduce the number of choice-of-law disputes. Merchants have learned to build "trustwrap" into each transaction—to find ways to demonstrate to consumers that an online purchase is safe. First, e-cash systems have failed to become widespread. Instead, credit card purchases (and systems such as PayPal that are based on credit and debit card accounts) have become the dominant means of payment over the Internet.[46] Sellers and buyers are subject to the elaborate rules of the credit card payment system, and so there is relatively little recourse to national courts. Credit cards have two decisive consumer protections compared with e-cash systems. If there is unauthorized use of the credit or debit card, the individual's loss is limited by U.S. statute, usually to $50.[47] In addition, the credit card brings with it an already-functioning dispute resolution system. If a merchant claims

---

[43] *See supra* Part IV.D.

[44] Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847 (2003).

[45] *See id.* at 850-51 (concluding that "vision of the New Economy" in the mid-1990s "foretold a future of E-cash, of nimble Internet companies destroying physical retailers, and an end to intermediaries between sellers and buyers").

[46] *See id.* at 851-54 (describing the advantages of the debit and credit card payment systems for online transactions).

[47] *See generally* Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181 (1996) (analyzing consumer-protection rules applying to unauthorized use of credit cards, debit cards, and checks).

that a customer has spent $200 on software, and the customer disagrees, then the customer is not charged for the $200 while the dispute is in process.[48] With these ready-made ways to protect customers against unauthorized use and to resolve disputes, the credit card system inspires trust in consumers, creates effective dispute resolution mechanisms, and avoids the need for recourse to national courts.

Second, the early predictions of "pure play" Internet sellers envisioned that online commerce would take place between one site for each seller and buyers who might exist anywhere in the world. Over time, the major pure Internet sites have gone international, with separate sites in markets such as France and Germany. Thus, those national sites are likely to be subject to that nation's laws.[49] More broadly, with time we have seen the rapid growth of "clicks and bricks" retailers, where the seller has physical locations in addition to websites.[50] Having physical stores inspires trust in the solidity of known brands. Having physical stores adds value to an online transaction, because the physical location can provide in-person services such as exchanges, repairs, and demonstrations about how to use a product. Of greatest relevance to choice-of-law rules, the existence of a physical retailer in the jurisdiction makes it overwhelmingly likely that local consumer laws will apply. The consumer, in essence, gets insurance against unfamiliar consumer-protection rules.

The third early prediction about e-commerce was that search engines and the global reach of the Internet would eliminate the need for wholesalers and other intermediaries. Consumers can feel that it is very risky, however, to buy from a website they have never heard of, in a country far away. One major cure for this problem has been the phenomenal growth of auction sites, especially the Internet intermediary eBay. Listings in 2004 reached 1.4 billion, up 45% from 971 mil-

---

[48] For further discussion of the chargeback dispute resolution mechanism in e-commerce, including ways that protections often apply outside of the United States, see Lester, *supra* note 40, at 461-64.

[49] Two of the leading "pure play" Internet sites are Amazon.com and Yahoo!. Both now have separate sites for France and Germany. *See* http://www.amazon.fr; http://www.amazon.de; http://fr.yahoo.com; http://de.yahoo.com.

[50] *See* Swire, *supra* note 44, at 854-56. For one analysis of the business and infrastructure advantages of the approach, see Anne Stuart, *Clicks and Bricks*, CIO, Mar. 15, 2000, at 76, *available at* http://www.cio.com/archive/031500/click.html (last visited Mar. 21, 2005).

lion in 2003.[51] An important achievement of eBay is that it has created a mechanism for matching individual buyers and sellers, even when they have never transacted with each other before and are in different countries. The international reach of eBay is apparent from the front page of www.ebay.com, which provides targeted pages for twenty-five different countries.

Although it was likely not a major goal of eBay's managers to avoid conflict-of-laws disputes, that has been one effect of the business model. Initially, trust on eBay was supposed to result from feedback ratings that customers gave to each other. Over time, however, eBay has created an entire legal system that accompanies each sale.[52] The system contains at least a dozen consumer protections, including fraud protection for the buyer, an escrow service so that buyers can examine an item before payment goes to the seller, a verified identity program, and a system for fraud enforcement including referrals if necessary for criminal activity. In essence, buyers and sellers do not have to trust in mice—the other individuals with whom they transact. They can trust instead in an elephant, eBay. Although eBay initially became famous for small purchases, such as hobbyist collectibles, today's eBay includes numerous auctions for valuable items such as diamonds. Even these large consumer transactions appear to be conducted without recourse to national courts, avoiding judicial pronouncements about which jurisdiction's laws apply.

Taken together, the winning business models for e-commerce all have the effect of reducing the number of court cases that choose which laws to apply. Credit cards and eBay have become the dominant dispute resolution systems. "Clicks and bricks" retailers are subject to local law, making it unlikely that the online seller can seek to apply the laws of a distant country. Conflict-of-laws issues do not arise, even for international sales where the nations have different laws, because the transactions take place inside structures that avoid the conflicts.

---

[51] Press Release, eBay, eBay Inc. Announces Fourth Quarter and Full Year 2004 Financial Results 1 (Jan. 19, 2005), *available at* http://investor.ebay.com/releases.cfm?Year=2005 (last visited Mar. 21, 2005).

[52] eBay, *Rules & Safety Overview (SafeHarbor)*, *at* http://pages.ebay.com/help/community/index.html (last visited Mar. 21, 2005). For analysis of these safeguards, see Swire, *supra* note 44, at 856-58.

These business models have successfully facilitated the growth of e-commerce even after the Internet bubble burst.[53] That does not mean, however, that the current business models and legal rules are the best ones possible. Professor Erin O'Hara, in her article in this Symposium, expresses concern that transaction fees for eBay transactions can exceed ten percent of the value of the sale (although fees drop below three percent for value over $25).[54] Professor Clay Gillette has critiqued some aspects of the eBay system.[55] There may be legal rules, including choice-of-law rules, that would do an even better job at inspiring trust and encouraging international e-commerce. With that said, however, the recent business models have been accompanied by the spread of e-commerce and avoidance of choice-of-law cases in the courts.

VI. WHERE INTERNATIONAL CHOICE-OF-LAW RULES MAY AFFECT INTERNET ACTIVITIES

We are now in a better position to describe when choice-of-law rules will affect Internet activity. Such rules will be most important when three conditions are present: (i) where there is activity by elephants; (ii) where there has not been harmonization; and (iii) where the structure of transactions does not prevent the dispute. The remaining international choice-of-law disputes occur in two contexts. The first is for financial harms suffered by third parties, especially for intellectual property and tort claims. The second is for a limited set of issues that involve significant moral, political, or constitutional differences.

---

[53] Estimates of the size and growth of e-commerce have varied enormously, due in part to the lack of standardized definitions of what counts as business-to-consumer and business-to-business e-commerce. With that said, one careful survey of the estimates in 2003 concluded that the "value of e-commerce transactions, while still small relative to the size of the U.S. economy, continues to show strong growth despite a recent economic downturn." RITA TEHAN, CONG. RESEARCH SERV., E-COMMERCE STATISTICS: EXPLANATION AND SOURCES 1 (rev. ed. 2003), *available at* http://www.usembassy.it/pdf/other/RL31293.pdf (last visited Mar. 21, 2005).

[54] Erin Ann O'Hara, *Choice of Law for Internet Transactions: The Uneasy Case for Online Consumer Protection*, 153 U. PA. L. REV. 1883, 1908 & n.85 (2005).

[55] *See* Clayton P. Gillette, *Reputation and Intermediaries in Electronic Commerce*, 62 LA. L. REV. 1165, 1177-92 (2002) (questioning the efficacy of eBay's feedback forum as a contract enforcement tool).

A. *Financial Harms Suffered by Third Parties*

The previous section discussed how Internet transactions can generally be structured to avoid choice-of-law disputes, for both business-to-business transactions and business-to-consumer transactions. There are certain harms, however, that are suffered by parties who are not subject to the contract. Harms can exist under property or tort law.

Physical items do not transfer over the Internet. The harms to property that occur in connection with the Internet thus involve intellectual property. The potential scope of choice-of-law disputes for intellectual property is greatly narrowed by the territorial nature of much of intellectual property law. Even today, patent[56] and trademark[57] law are overwhelmingly understood to apply within each sovereign territory, so that a separate patent or trademark must be secured in each country in which infringement is alleged.

Disputes over domain names have tested this territorial approach. For domain names, the two parties to the relevant contract are the current owner of the name and the registrar who provides the name. Two recent choice-of-law disputes arose when a third party claimed that the domain name, used worldwide, violated a trademark. In both *Globalsantafe Corp. v. Globalsantafe.com*[58] and *Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona*,[59] U.S. courts decided to apply U.S. law even in the face of numerous foreign contacts. Professor Paul Schiff Berman's article in this Symposium provides extensive analysis of the two cases, and reaches a normative conclusion: "[W]e need to

---

[56] For new research underscoring the territorial reach of patent law, and specific gaps in patent protection that thus result, see Mark A. Lemley et al., *Divided Infringement Claims*, 33 AM. INTELL. PROP. L. ASS'N Q.J. (forthcoming 2005).

[57] For a history and defense of territoriality in trademark law, see Curtis A. Bradley, *Territorial Intellectual Property Rights in an Age of Globalism*, 37 VA. J. INT'L L. 505 (1997). For a critique that advocates a limited extraterritorial reach of U.S. trademark law, see Roger E. Schechter, *The Case for Limited Extraterritorial Reach of the Lanham Act*, 37 VA. J. INT'L L. 619 (1997) (advocating extraterritorial application of trademark law for a limited set of well-known marks). *See generally* Graeme B. Dinwoodie, *Trademarks and Territory: Detaching Trademark Law From the Nation-State*, 41 HOUS. L. REV. 885 (2004) (criticizing exclusively territorial basis of trademark law).

[58] 250 F. Supp. 2d 610 (E.D. Va. 2003) (establishing in rem jurisdiction under the Anticybersquatting Consumer Protection Act, and applying U.S. law according to the *Princess Lida* doctrine).

[59] 330 F.3d 617 (4th Cir. 2003) (holding that the application of United States trademark law is consistent with the fundamental doctrine of territoriality).

reconsider the traditional assumption that trademark disputes must always be resolved by applying the law of the forum country."[60]

For purposes of this paper, which addresses the descriptive question of when choice-of-law disputes arise from the Internet, the point is to show why this category of case gives rise to choice-of-law problems. The substantial financial stakes in ownership of a domain name, and the fact that harms can fall on third parties, gives those third parties an incentive to bring the case that results in a choice-of-law judgment. If and only if the territorial tradition of trademark law becomes weaker, then we may see a significant number of trademark court decisions delineating which nation's laws should apply.[61]

Although the territorial tradition of trademark and patent laws thus remains strong, the current approach for copyright is different. As described by Professor Justin Hughes, there has been significant harmonization of copyright laws.[62] Where this harmonization exists, choice-of-law disputes are minimized because the same substantive rule applies under the law of the various jurisdictions. The remaining disputes occur in situations where harmonization has not been achieved. A prominent example of lack of harmonization occurred in the case of *Twentieth Century Fox Film Corp. v. iCraveTV*.[63] In that case, streaming of video material by a Canadian company to Canadian residents was lawful in Canada. The film studio, however, succeeded in getting an injunction under U.S. law, due to access to the content by some U.S. users. The principal source of choice-of-law judicial decisions for copyright issues, therefore, would seem likely to occur for specific situations where harmonization has not taken place. These situations may individually be very important, but it conceptually makes sense to think of them as a relatively finite number of particular

---

[60] Paul Schiff Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 U. PA. L. REV. 1819, 1834 (2005).

[61] The number of conflicts for domain names is also reduced by the alternative dispute resolution mechanism of the Uniform Domain Name Dispute Resolution Program (UDRP), established by the Internet Corporation for Assigned Names and Numbers (ICANN). The rules for that program are set forth at http://www.icann.org/dndr/udrp/uniform-rules.htm. For comprehensive commentary and citations concerning ICANN and the UDRP, see the site created by Professor A. Michael Froomkin, http://www.icannwatch.org.

[62] *See* Hughes, *supra* note 21, at 363 (noting that the 1996 World Intellectual Property Organization copyright treaties are "a successful example of top-down convergence").

[63] Nos. Civ.A. 00-120, Civ.A. 00-121, 2000 WL 255989 (W.D. Pa. Feb. 8, 2000).

conflicts, rather than a potentially limitless universe of potential conflicts that arise from the global nature of the Internet.[64]

In addition to contract-based claims (largely avoided by the structure of transactions) and property-based claims (largely avoided by territoriality and harmonization), there can be tort-based claims that arise from Internet conduct. The most prominent Internet-based tort to date is defamation. The tort of defamation has been a fertile source of choice-of-laws cases in the United States.[65] The leading edge of potential Internet defamation cases is *Gutnick v. Dow Jones & Co.*[66] In that case, the High Court of Australia permitted a defamation action by an Australian to proceed based on publication over the Internet by a U.S. company using a U.S.-based server. The number of defamation disputes could climb substantially if any major jurisdiction became noticeably favorable to plaintiffs in awarding judgments. Publishers on the Internet might seek to prevent their statements from reaching that jurisdiction, but it would be difficult for such limits to succeed.

Other tortious harms to third parties might become more prominent in the future. Intentional attacks on a computer system are treated as crimes in a growing number of countries, as discussed above in connection with the Council of Europe Cybercrime Convention.[67] Tort actions, such as trespass to chattels, may then be pursued in the relatively limited subset of cases where the attacker is identified and has enough assets to be worth pursuing.[68] A potentially important type of claim in the future may be a claim that a software producer or system owner provided tortiously weak computer security, such as failure to fix a known vulnerability.[69] For these and other torts, choice-of-

---

[64] For a detailed analysis of international conflict-of-laws issues in copyright, see Paul Edward Geller, *Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues*, 51 J. COPYRIGHT SOC'Y U.S.A. 315 (2004).

[65] Prominent examples include *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) (applying the First Amendment to prevent application of an Alabama defamation claim), and *Calder v. Jones*, 465 U.S. 783 (1984) (permitting a California defamation claim to proceed against Florida persons).

[66] (2002) 210 C.L.R. 575 (Austl.).

[67] *See supra* Part IV.A.

[68] For a recent article collecting sources, see Daniel Kearney, Note, *Network Effects and the Emerging Doctrine of Cybertrespass*, 23 YALE L. & POL'Y REV. 313 (2005).

[69] There has been a paucity to date of scholarship on how the tort system should assess claims for weak computer security. There are intricate legal issues that deserve fuller attention, including the application of the tort system to purely economic losses and the question of how (and whether) to levy damages for harms that are highly networked and affect a potentially enormous number of people. For one article that col-

law decisions thus might be made in the courts when at least one jurisdiction permits plaintiffs to win on such claims, and there are identified defendants who have significant assets.

In terms of quantity of choice-of-law cases, there are specific intellectual property and tort situations where third parties might seek court resolution of issues arising from the Internet. The most likely categories thus far for court decisions include: areas where trademark or patent law depart from the territorial tradition; areas of copyright law that have not been harmonized; defamation; and other torts if at least one jurisdiction adopts plaintiff-friendly rules for liability.

B. *Issues Involving Significant Moral, Political, or Constitutional Differences*

The remaining category of potential choice-of-law cases is more elusive to define. The suggestion here is that there is a fairly limited number of disputes concerning the Internet where nations have significant moral, political, or constitutional differences. To date, the bulk of these disputes have involved the First Amendment to the U.S. Constitution. The structure of the disputes is that the First Amendment protects publication within the United States of material that is unlawful in another country.

The most famous recent example is *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme.*[70] French law prohibits the display of Nazi paraphernalia, but the First Amendment protects a speaker's right to display it. The corporation Yahoo!-France had to comply with French law, but the separate corporation Yahoo!, Inc., operating in the United States, was held in U.S. court not to have to satisfy the French judgment against it.

Similar First Amendment conflicts can exist for topics other than hate speech. In *Reno v. American Civil Liberties Union*,[71] the U.S. Supreme Court struck down a federal anti-pornography statute, holding that First Amendment speech protections apply to Internet content. There are several concerns regarding the effect of this decision. For

---

lects sources, see Kevin R. Pinkney, *Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure*, 13 ALB. L.J. SCI. & TECH. 43 (2002).

[70] 169 F. Supp. 2d 1181 (N.D. Cal. 2001), *rev'd on other grounds*, 379 F.3d 1120 (9th Cir. 2004), *reh'g granted en banc*, 399 F.3d 1010 (9th Cir. 2005). The underlying French judgment is T.G.I. Paris, Nov. 20, 2000, *available at* http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf (last visited Mar. 21, 2005).

[71] 521 U.S. 844 (1997).

example, anti-pornography laws in other countries may thus be unenforceable against U.S. websites. In the area of political speech, nations including China and Singapore may seek to censor critics of their respective governments. Once again, however, the First Amendment would likely shield persons in the United States who make those criticisms. Electronic Frontier Foundation cofounder John Perry Barlow is credited with the aphorism that "[i]n Cyberspace, the First Amendment is a local ordinance."[72] As just a "local ordinance," the First Amendment is a fertile source for potential conflicts with other ordinances. To the frustration of other countries who wish to enforce their laws, however, this ordinance is written into the U.S. Constitution and thus is highly resistant to change.

Clashes of moral values exist outside of the First Amendment realm. One current example concerns the legality of U.S. laws banning Internet gambling. A panel of the World Trade Organization has upheld the complaint of Antigua and Barbuda against the United States for the latter's ban on Internet gambling.[73] The case represents the first time that the WTO has ruled on the scope of the "public morals" exception to obligations to permit free trade in services.[74] The United States has announced that it will appeal the panel ruling, arguing among other points that cross-border gambling was never included within the scope of international free trade obligations.[75]

---

[72] JOSEPH REAGLE, WHY THE INTERNET IS GOOD: COMMUNITY GOVERNANCE THAT WORKS WELL app. 1 (Berkman Ctr. Working Draft, 1998), *available at* http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html (last visited Mar. 21, 2005).

[73] GEN. AGREEMENT ON TRADE IN SERVS. (GATS) DISPUTE PANEL, WORLD TRADE ORG., UNITED STATES—MEASURES AFFECTING THE CROSS-BORDER SUPPLY OF GAMBLING AND BETTING SERVICES, Doc. WT/DS285/R, at 272 (2004) (concluding that the commitments of the United States against gambling and betting services are in violation of GATS), *available at* http://www.wto.org/english/tratop_e/dispu_e/285r_e.pdf.

[74] This point is made as part of a clear explication of the dispute in Joost Pauwelyn, *ASIL Insight: WTO Condemnation of U.S. Ban on Internet Gambling Pits Free Trade Against Moral Values*, *available at* http://www.asil.org/insights/2004/11/insight041117.html (Nov. 2004).

[75] *See* United States Trade Representative, Statement from USTR Spokesman Richard Mills Regarding the WTO Gambling Dispute with Antigua and Barbuda, Nov. 10, 2004 (explaining that WTO members are not required to seek approval from their trading partners on matters designed to "protect public morals and public order"), *available at* http://www.ustr.gov/Document_Library/Spokesperson_Statements/Statement_from_USTR_Spokesman_Richard_Mills_Regarding_the_WTO_Gambling_dispute_with_Antigua_Barbuda.html.

CONCLUSION

A chief task of this Article has been to treat international choice of law on the Internet as a dependent variable, and to explain the conditions under which such cases arise. A second task, addressed briefly here, is to consider the existence of mice as a dependent variable; that is, what measures can affect the prevalence of mice, and thus the persistence of actors on the Internet who can act outside of the law.

A. *Summary on the Frequency and Type of Choice-of-Law Cases*

The prominence of the Yahoo! and Internet gambling cases is not matched by their frequency. There is a limited subset of important clashes of moral, political, or constitutional values. The Internet heightens the conflict between nations because individual citizens can so easily "cross" borders to interact with websites in other countries.

Despite the importance of such clashes, the number of choice-of-law cases arising from the Internet is far less than is suggested by the image of each surfer potentially having an international dispute with each website. As a descriptive matter, two filters are especially effective in reducing the number of choice-of-law cases from the potentially infinite down to a handful—only elephants pay much attention to choice-of-law issues, and successful business models on the web are effective at avoiding choice-of-law disputes. Two other filters also could reduce the number of disputes. Jurisdictional limitations could do so, but sellers on the Internet will come under the jurisdiction of the buyer's country in almost all settings. Harmonization can also reduce conflicts, but only limited harmonization has been implemented at the global level.

The analysis here also suggests a hitherto undescribed category as the area where the number of choice-of-law cases could become numerous—claims brought by third parties that involve substantial potential damages. Defamation claims and disputes over the scope of intellectual property rights are the chief candidates for such claims.

B. *Surveillance as a Way to Try to Stop the Mice*

To this point, this Article has treated the prevalence of mice as a given. As discussed in the 1998 article, however, there are strategies

for nations that wish to address the perceived harms caused by mice.[76] Nations can focus their attention on alternative targets of enforcement, including the payments system, Internet Service Providers, and other gatekeepers such as Yahoo! through whom the bits flow between the mouse (creator of the harm) and the user. Nations can also seek to apply pressure to the other countries that serve as safe dens for the mice. Finally, the users themselves, such as those who download music or pornography, might be the target of enforcement.

All of these strategies could reduce current illegal activity, and all have been used to some extent. One general theme that was not developed in the 1998 article, however, is the possibility that increased surveillance could be a general-purpose tool for increasing the enforceability of law on the Internet. "Data retention" rules might be imposed on Internet Service Providers so that the providers would retain records of where their customers surfed on the web. Stronger authentication could become a precondition for sending emails or doing other web activity. Most generally, there are temptations in the post-9/11 world to minimize anonymity and increase traceability for essentially all web activity. In addition, many Internet users are especially irritated by spam, and would welcome a revised Internet that effectively tracks spammers back to their nests.

This Article will not attempt to set forth a general theory of when increased surveillance over the Internet is desirable. Many of my previous writings have addressed aspects of that broader inquiry.[77] The point here, instead, is to highlight that the degree to which mice exist is contingent upon the technological and legal choices we will make in the coming years. A determined enough effort can greatly reduce the number of mice. To extend the metaphor, we can put out poisoned cheese and take other strong measures to attack the mice. But the same poison might also kill our house pets and have other bad consequences. The desire to increase surveillance and hunt down the

---

[76] *See* Swire, *supra* note 1, at 1021-22 (offering several approaches that countries can employ to reduce harm caused by mice).

[77] *See, e.g.*, Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 493-507 (1999) (addressing the issues that could arise if all of an individual's purchases were known by government); *see also* Declaration of Peter P. Swire ¶¶ 5-9, *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24 (D.D.C. 2003) (No. CIV.A.02-MS-0323(JDB)) (explaining due process and privacy problems with the Recording Industry Association of America's attempt to use subpoenas under the 1998 Digital Millennium Copyright Act, 17 U.S.C. § 512(h) (2000), to reveal the identity of Verizon customers), *available at* http://newscenter.verizon.com/kit/riaa/swire_declaration_013003.pdf (last visited Mar. 21, 2005).

mice must be balanced by thoughtful inquiry about the many other consequences of such actions.