

Computer Crime Seminar
Fall 2006

Supplemental Reading 1
August 28, 2006

Paul Ohm

The Importance and Limits of Metaphor and Analogy

Orin Kerr, *Seeing it Both Ways*, Legal Affairs (July/August 2003).

The virtual perspective of the Internet is like the perspective inside the Matrix: It accepts the virtual world of cyberspace as akin to a reality. Of course, unlike Neo, we know all along that the virtual world that the computer generates is just that. But as we try to envision what we experience online, we might decide to treat that virtual world as if it were real. From this perspective, a computer connected to the Internet provides a window to a virtual world of cyberspace that is roughly analogous to the physical world of real space. The user can employ her keyboard and mouse to "go shopping" or "send mail." She can "visit" a chat room, participate in an online community, or conduct any number of other everyday activities online, all without moving from the computer. The technical details of what the computers attached to the Internet actually do "behind the scenes" don't particularly matter. What matters is the virtual world of cyberspace that the user encounters and interacts with when she goes online.

We can also understand the Internet from a different perspective. Like Neo when he is outside the Matrix, we can look at the Internet from the point of view of the physical world, rather than the virtual one. The physical perspective adopts the viewpoint of an outsider concerned with the functioning of the network in the physical world rather than the perceptions of a user. The physical perspective treats the Internet as a physical network of computers located around the world and connected by wires and cables. The hardware sends, stores, and receives data in the form of digital ones and zeroes using a series of common protocols. Keyboards provide sources of input to the network, and monitors provide destinations for output. When the network runs properly, trillions of ones and zeroes zip around the world, sending and receiving electrical impulses that the computers connected to the network can translate into commands, text, sound, and pictures.

* * *

Imagine you send an e-mail to me, and two police officers learn about the e-mail and believe that it might reveal a nefarious criminal conspiracy between us. The officers agree that they should try to obtain a copy of the e-mail to prove the conspiracy. They confront a legal question: What kind of legal process must they undertake in order to obtain the e-mail? Does the Fourth Amendment require them to obtain a search warrant?

Imagine that the first officer applies the virtual perspective of the Internet. To him, my e-mail is the cyberspace equivalent of old-fashioned postal mail. After all, my computer announces "You've got mail!" and displays a closed envelope when an e-mail message arrives. When the officer clicks on the envelope, it opens, revealing the message. From his virtual perspective, the officer is likely to conclude that the Fourth Amendment places the same restriction on government access to e-mail that it places on government access to ordinary postal mail. He will look in a Fourth Amendment treatise for the black-letter rule on accessing postal mail. That treatise will tell him that accessing a suspect's mail ordinarily violates the suspect's "reasonable expectation of privacy" and that the officer must first obtain a warrant. Viewing e-mail as analogous to postal mail, the officer will conclude that the Fourth Amendment requires him to obtain a warrant before he can access the e-mail you send me.

Imagine that the second police officer approaches the same problem from a physical perspective. To him, the facts look quite different. Looking at how the Internet actually works, he argues that when you sent the e-mail to me, you allowed several intermediaries to observe the content of the message. After all, by sending the e-mail you gave an instruction to your computer to send a message to your Internet service provider directing your ISP to forward a text message to my ISP. Your ISP received the instructions, and the e-mail crossed the Internet until it arrived at my ISP's mail server. The next morning, when I sat at my desk and clicked on the icon to read your message, I asked my ISP's mail server to run off a copy of the message—the server retains the original—and send it to me at my desk.

The second officer will reason that you disclosed the contents of the e-mail to your ISP, with instructions to disclose the contents of the e-mail again to my ISP, before finally relaying the message to me. The second officer will look in the same Fourth Amendment treatise and find the black-letter rule that the government requires only a subpoena—not a warrant—to obtain information that's already been disclosed to a third party.

Who is right? The first officer or the second? It all depends on your perspective. Accept the virtual facts and the officers need a search warrant; accept the physical facts and they don't.

* * *

Internet law's dependence on perspective is not only a Fourth Amendment problem. The choice between virtual and physical facts pervades the law of the Internet, arising every time a judge relates the facts of the Internet to the law. Consider the Tenth Circuit's decision in *United States v. Kammersell*. In this case, a 19-year-old named Matthew Kammersell used America Online's instant message service to send a bomb threat from his home in Riverdale, Utah, to his girlfriend's computer in nearby Ogden, Utah. The government prosecuted Kammersell under a law that makes it a federal crime to send interstate communication containing a "threat to injure."

Kammersell's lawyers argued that no interstate communication took place when he sent a message to his girlfriend, who was just a few miles away in the same state. The government countered with a physical perspective, noting that because America Online's servers are located in Virginia, every AOL instant message must be routed there first, and then sent to its destination. Unbeknownst to Kammersell, his instant message had traveled from Utah to Virginia, and then back to Utah.

Did Matthew Kammersell send an interstate threat? From a virtual perspective, no; from a physical perspective, yes. The Tenth Circuit adopted the government's physical perspective and affirmed the conviction.

Michael Fromkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Penn. L. Rev. 709 (1995).

It is old news that common-law legal reasoning is both analogical and taxonomical, [FN663] and that metaphor is a powerful tool for both. [FN664] Nevertheless, the observation that "the power of a metaphor is that it colors and controls our subsequent thinking about its subject" [FN665] is particularly relevant and powerful when the law encounters a new technology. [FN666] The law's first reaction to a *861 new technology is to reach for analogies and to explain why the new technology can be treated identically to an earlier technology. Railroads, for example, could be slotted into the existing legal categories created to deal with highways, collisions, and freight tariffs. [FN667] In contrast, airplanes—a technological advance on the same order as the railroad—required a significant change in the law because to be useful the airplane must fly over land, a classical trespass, without a right of way. [FN668]

* * *

By their nature, balancing tests almost demand that courts give some play to the judge's hopes and, especially, fears. A mandatory key escrow statute would evoke two conflicting sets of fears, one over control and the other over lawlessness, symbolized by the archetypes of Big Brother and the criminal cabal. In the end, the conflict may be decided by the way the courts characterize cryptography. Just as the cryptographic "key" is a metaphor, so too may the choice among possible metaphors determine how much constitutional protection an encrypted message gets. If the courts treat a ciphertext as if it had been written in a foreign language, it will trigger a First Amendment analysis that will result in giving cryptography more protection than if the courts focus on the place where the message is encrypted. If encryption is considered no more than the outer envelope in a message transmission system—essentially a "car" on the information superhighway—it is likely to receive the lowest level of protection.

Why Study "Computer Crime"?

Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207

When he was dean of this law school, Gerhard Casper was proud that the University of Chicago did not offer a course in "The Law of the Horse." He did not mean by this that Illinois specializes in grain rather than livestock. His point, rather, was that "Law and . . ." courses should be limited to subjects that could illuminate the entire law. Instead of offering courses suited to dilettantes, [FN1] the University of Chicago offered courses in Law and Economics, and Law and Literature, taught by people who could be appointed to the world's top economics and literature departments--even win the Nobel Prize in economics, as Ronald Coase has done.

I regret to report that no one at this Symposium is going to win a Nobel Prize any time soon for advances in computer science. We are at risk of multidisciplinary dilettantism, or, as one of my mentors called it, the cross-sterilization of ideas. Put together two fields about which you know little and get the worst of both worlds. Well, let me be modest. I am at risk of dilettantism, and I suspect that I am not alone. Beliefs lawyers hold about computers, and predictions they make about new technology, are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers.

Dean Casper's remark had a second meaning--that the best way to learn the law applicable to specialized endeavors is to study general rules. Lots of cases deal with sales of horses; others deal with people kicked by horses; still more deal with the licensing and racing of horses, or with the care veterinarians give to horses, or with prizes at horse shows. Any effort to collect these strands into a course on "The Law of the Horse" is doomed to be shallow and to miss unifying principles. Teaching 100 *208 percent of the cases on people kicked by horses will not convey the law of torts very well. Far better for most students--better, even, for those who plan to go into the horse trade--to take courses in property, torts, commercial transactions, and the like, adding to the diet of horse cases a smattering of transactions in cucumbers, cats, coal, and cribs. Only by putting the law of the horse in the context of broader rules about commercial endeavors could one really understand the law about horses.

Now you can see the meaning of my title. When asked to talk about "Property in Cyberspace," my immediate reaction was, "Isn't this just the law of the horse?" I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile. And if I did know something about computer networks, all I could do in discussing "Property in Cyberspace" would be to isolate the subject from the rest of the law of intellectual property, making the assessment weaker.

Lawrence Lessig, Commentaries, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501 (1999).

I agree that our aim should be courses that 'illuminate the entire law,' but unlike Easterbrook, I believe that there is an important general point that comes from thinking in particular about how law and cyberspace connect.

This general point is about the limits on law as a regulator and about the techniques for escaping those limits. This escape, both in real space and in cyberspace, [FN5] comes from recognizing the collection of tools that a society has at hand for affecting constraints upon behavior. Law in its traditional sense--an order backed by a threat directed at primary behavior [FN6]--is just one of these tools. The general point is that law can affect these other tools--that they constrain behavior themselves, and can function as tools of the law. The choice among tools obviously depends upon their efficacy. But importantly, the choice will also raise a question about values. By working through these examples of law interacting with cyberspace, we will throw into relief a set of general questions about law's regulation outside of cyberspace.

I do not argue that any specialized area of law would produce the same insight. I am not defending the law of the horse. My claim is specific to cyberspace. We see something when we think about the regulation of cyberspace that other areas would not show us.

Technological Primer

IP address

From Wikipedia, the free encyclopedia (visited August 14, 2006).

An IP address (Internet Protocol address) is a unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any participating network device — including routers, computers, time-servers, printers, Internet fax machines, and some telephones — must have its own unique address. An IP address can also be thought of as the equivalent of a street address or a phone number (compare: VoIP) for a computer or other network device on the internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network.

An IP address can appear to be shared by multiple client devices either because they are part of a shared hosting web server environment or because a proxy server (e.g. an ISP or anonymizer service) acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. The analogy to telephone systems would be the use of pre-dial numbers (proxy) and extensions (shared).

Domain names

A network lookup service, the Domain Name System (DNS), provides the ability to map hostnames to an IP address. This allows humans to easily remember a name and not a series of numbers. DNS allows multiple addresses and names to point to one Internet resource.

Another reason for DNS is to allow, for example, a web site to be hosted on multiple servers (each with its own IP address) to provide rudimentary load balancing.

For example, www.wikipedia.org resolves to 207.142.131.248.

Dynamic and static IP addresses

IP addresses may either be assigned permanently (for example, to a server which is always found at the same address) or temporarily from a pool of available addresses. [edit]

Dynamic

Dynamic IP addresses are issued to identify non-permanent devices such as personal computers or clients. Internet Service Providers (ISPs) use dynamic allocation to assign addresses from a small pool to a larger number of customers. This is used for dial-up access, WiFi and other temporary connections, allowing a portable computer user to automatically connect to a variety of services without needing to know the addressing details of each network.

* * *

It is common to use dynamic allocation for private networks. Since private networks rarely have an address shortage, it is possible to assign the same address to the same computer on each request or to define an extended lease time. These two methods simulate static IP address assignment.

Static

Static IP addresses are used to identify semi-permanent devices with constant IP addresses. Servers typically use static IP addresses. * * *