THE PROBLEM OF **PERSPECTIVE** IN INTERNET LAW

Orin S. **Kerr** [FNa1]

91 Geo. L.J. 357 (2003)

INTRODUCTION

The lawyer's quintessential task is to apply legal rules to facts. [FN1] When we apply law to the Internet, however, a difficult question arises: What are the "facts" of the Internet? The Internet's facts depend on whether we look to physical reality or virtual reality for guidance. We can model the Internet's facts based on virtual reality, looking from the perspective of an Internet user who perceives the virtual world of cyberspace and analogizes Internet transactions to their equivalent in the physical world. [FN2] Alternatively, we can model the facts based on the physical reality of how the network operates. From this perspective, Internet transactions can be understood based on how the network actually works "behind the scenes," [FN3] regardless of the perceptions of a user. Because the Internet can generate a virtual reality, it offers two distinct sets of facts: one based on physical reality, the other based on virtual reality.

The Internet's ability to generate a virtual reality creates what I will call the problem of perspective in Internet law. The problem is that whenever we apply law to the Internet, we must first decide whether to apply the law to the facts as seen from the viewpoint of physical reality or virtual reality. In this Article, I will refer to the viewpoint of virtual reality as the "internal perspective" of the Internet, and the viewpoint of physical reality as the "external perspective."

This Article argues that the problem of perspective pervades Internet law, and that the nature and shape of Internet law depends upon how it is resolved in particular cases. In a surprising number of situations, we arrive at one result when applying law from an internal perspective and a different result when applying law from an external perspective. In fact, many of the major disputes within the field of "cyberlaw" [FN4] boil down to clashes between internal and external perspectives. To complicate matters, neither perspective holds an a priori claim to greater legitimacy. Both internal and external perspectives can appear perfectly viable depending on the circumstances, and courts and commentators***358** switch between them frequently without even recognizing the change. [FN5]

The goal of this Article is to explain the problem of perspective, to show its importance, and to offer an approach that can help lead to its solution. I argue that we need to be aware of the problem of perspective and develop legal tools that can help us choose between real and virtual understandings of the Internet when we apply law to it. I also contend that the problem of perspective is a new problem, or at least a new twist on an older one. Although prior technologies such as the telephone hinted at the clash in narrow ways, [FN6] computer networks and the Internet provide the first widespread technology that creates a virtual world for its users that can compete on

an equal footing with the real one. As a result, Internet law prompts us to confront the problem of perspective for the first time.

I. THE INTERNAL AND EXTERNAL PERSPECTIVES IN INTERNET LAW

A. THE PROBLEM OF PERSPECTIVE

In the 1999 science fiction thriller *The Matrix*, [FN7] Keanu Reeves plays a computer hacker named "Neo" who learns that the reality he has known since birth is merely a virtual reality created by a computer network known as the Matrix. The *real* Neo lies in a semicomatose state attached to the network, to which he and others have been connected by advanced computers that have taken over the world and sap energy from humans while occupying their minds with virtual reality. Neo ends up joining the rebel forces trying to destroy the Matrix, and the movie jumps several times between the virtual world inside the Matrix and the real world outside of the Matrix. The movie presents us with two different realities, two existing worlds. The first reality is the virtual world that we experience inside the Matrix, and the second is the "real" world that we experience outside the Matrix.

In addition to being a fun movie, *The Matrix* points out an important problem that arises when we try to understand the nature of computer networks in general and the Internet in particular. Like Neo confronting the Matrix, we can think about the Internet in two ways, virtual and real. The virtual perspective 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 only virtual. But as we try to make sense of what the Internet is, to understand what we experience online, we might decide to treat that virtual world as if it were real.

I will call this virtual point of view the internal perspective of the Internet. The internal perspective adopts the point of view of a user who is logged on to the Internet and chooses to accept the virtual world of cyberspace as a legitimate construct. [FN8] To this user, a computer connected to the Internet provides a window to a virtual world that is roughly analogous to the physical world of ***360** real space. The user can use her keyboard and mouse to go shopping, send mail, visit a chat room, participate in an online community, or do anything else she can find online. [FN9] 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 he or 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. I will call this the external perspective of the Internet. The external 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.

From this external viewpoint, the Internet is simply a network of computers located around

the world and connected by wires and cables. [FN10] The hardware sends, stores, and receives communications using a series of common protocols. [FN11] Keyboards provide sources of input to the network, and monitors provide destinations for output. When the Internet runs properly, trillions of zeros and ones zip around the world, sending and receiving communications that the computers connected to the network can translate into commands, text, sound, and pictures.

From the external perspective, the fact that Internet users may perceive that they have entered a virtual world of cyberspace has no particular relevance. These perceptions reflect the fact that software designers often garnish their applications with icons, labels, and graphics to help novices understand and use them—for example, by writing e-mail programs so that e-mail looks and feels like postal mail. [FN12] These superficialities have no deeper meaning from the external perspective. What matters is the physical network and the technical details of how it works, not the easily manipulated perceptions of Internet users.

Both internal and external understandings of the Internet should ring true to most of us. The Internet *is* a physical network, and it *can* create a virtual world for its users that can appear sufficiently realistic to its users to make a plausible claim for equal footing with the physical world. [FN13] But the key for us is that by ***361** generating a virtual reality, the technology in a sense leaves us with two Internets, rather than one. [FN14] We have an external version of the Internet, and also an internal one. One is physical, the other virtual. [FN15]

B. PERSPECTIVE AS A PROBLEM OF LAW

Why does this matter to lawyers and to the nature of Internet law? It matters because legal outcomes depend on facts, and the facts of the Internet depend on which perspective we choose. [FN16] This is a very practical problem. The basic task of a lawyer is to apply legal rules to facts—to apply law to an understanding of reality. In the case of the Internet, however, two competing understandings of reality exist. We have a virtual reality from the internal perspective and a physical reality from the external perspective. This means that we face a choice of which perspective to use when applying law to the Internet. Do we decide to follow the internal perspective of virtual reality or the external perspective of physical reality? Which version of the Internet should we pick before applying the law to it? By choosing the perspective, we choose the reality; by choosing the reality, we choose the facts; and by choosing the facts, we choose the law.

We can look at this another way by noting the differences between what happens when we apply law to the Internet from an internal versus an external perspective. From the internal perspective of an Internet user, the Internet is cyberspace, and we apply law to the Internet by trying to map the physical world of "realspace" onto the virtual world of cyberspace. [FN17] We look for analogies between cyberspace and realspace, and try to match the rules between them. [FN18] To the external observer, in contrast, the Internet is the physical network, and we apply law to the Internet by applying the law to the electronic transactions underlying the network's operation. This

does not necessarily mean that the Internet must be viewed only as 0s and 1s, any more than modeling the ***362** physical world requires us to model sounds as pressure waves or light as photons of energy. But it does mean that we look for analogies between realspace and the behind-the-scenes action that the computers connected to the Internet process and complete.

These two approaches are similar to each other and also quite different. In both the external and internal cases, we apply law to "the Internet." However, our model of what that Internet is—and therefore what Internet law is—varies dramatically depending on the perspective we choose. The law is contingent on the facts, and the facts are contingent on our perspective.

What makes this problem unusually interesting is that there is no particular correlation between internal and external renderings of the Internet's facts. The real produces the virtual, but the virtual need not reflect the real. Significant changes in the behind-the-scenes workings of the Internet can go entirely unnoticed by users. [FN19] At the same time, minor changes in computer code can have a dramatic impact on users' experiences. [FN20] A typical user immersed in the internal perspective can be blissfully unaware of the complex inner working of the Internet.

The lack of correlation between the real and the virtual has profound implications for Internet law. It means that the legal outcomes reached using an internal set of facts exist independently from outcomes reached with an external set of facts. When we apply the law to the facts, an internal perspective will take us down one path, and an external perspective will take us down another. The two paths may happen to converge, but there is no reason to think they will. In effect, we not only have two Internets, but two versions of Internet law. Every time we apply law to the Internet, we will have two possible outcomes: an internal outcome and an external outcome. The two outcomes may happen to match in some cases. In many cases, however, the choice of perspective proves outcome-determinative. Consequently, the shape of Internet law hinges on our choice of perspective.

C. AN EXAMPLE: SURFING THE WEB

All of this may seem rather abstract, so an example may help. Consider what happens when an Internet user surfs the web. Imagine that an Internet user opens up a web browser and types in "www.amazon.com," and moments later the homepage of Amazon.com appears on the viewer's screen. How might we model this event? How can we develop a factual picture of what has happened, so that we can later determine the legal consequences of accessing a webpage?

This is easy from an internal perspective. The user has visited Amazon.com's ***363** website, going to Amazon.com's home on the Internet. The user has visited Amazon.com's virtual store much like a person might visit a store in the physical world, traveling from one point in cyberspace to another. Of course, we realize that the user has not actually traveled anywhere. The user is just sitting in front of the screen. But from an internal perspective, the essential experience of surfing Amazon.com can be captured by comparing it to visiting a store.

From an external perspective, however, the event appears quite different—and significantly

more complicated. Behind the scenes, the simple act of typing "www.amazon.com" into a web browser triggers a series of responses from different computers connected to the Internet. The browser begins by sending out a request across the Internet to a special type of computer known as a Domain Name System (DNS) server. [FN21] The browser's request asks the DNS server to translate the letters of the website address "amazon.com" into an "Internet Protocol" or "IP" address, which is a series of numbers that computers connected to the Internet understand as an address akin to a phone number. [FN22] The DNS server will respond that "www.amazon.com" translates into the IP address "207.171.184.16." [FN23] The user's browser then issues another request, this time directed to "207.171.184.16," asking it to send a set of data files back to the browser. Amazon.com's computer will receive the request and then send data back to the browser. The browser will receive the data and display it on the user's screen. The resulting images and text appear in the form of the Amazon.com webpage that the user requested. [FN24]

Notice that the internal and external perspectives have produced two different accounts of the same event. One model of the facts follows the virtual perspective of the user, and another model follows the behind-the-scenes perspective of how the Internet actually works. From the internal perspective, visiting Amazon.com resembles visiting a store. The user types in the address, and a moment later is paying a virtual visit to Amazon.com's site. From the external perspective, visiting Amazon.com resembles calling Information and asking for Amazon.com's phone number, then dialing the number and asking the representative to send you the latest Amazon.com catalog. The single event of surfing the web produces two set of facts, one internal and the other external. As a result, when we need to apply law to the act of visiting a website, we can apply that law to two different sets of facts, which can produce two different outcomes. [FN25]

II. THE POWER OF PERSPECTIVE: EXAMPLES

A. THE FOURTH AMENDMENT IN CYBERSPACE

1. Do the Police Need a Warrant to Obtain E-mail?

Imagine that A sends an e-mail to his friend B. Two police officers learn about the e-mail and believe that it may reveal a nefarious criminal conspiracy. 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 follow to obtain the e-mail? Does the Fourth Amendment require them to obtain a search warrant? Or can they obtain the e-mail with less process than a search warrant? The answer depends largely upon whether they apply an internal or external perspective of the Internet.

Imagine that the first officer applies an internal perspective of the Internet. To him, e-mail is the cyberspace equivalent of old-fashioned postal mail. His computer announces, "You've got mail!" when an e-mail message arrives and shows him a closed envelope. [FN32] When he clicks

on the envelope, it opens, revealing the message. From his internal 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 then 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 therefore the officer must first obtain a warrant. [FN33] Because e-mail is the equivalent***366** of postal mail, the officer will conclude that the Fourth Amendment requires him to obtain a warrant before he can access the e-mail. [FN34]

Imagine that the second police office approaches the same problem from an external perspective. To him, the facts look quite different. Looking at how the Internet actually works, the second police officer sees that when A sent the e-mail to B, A was instructing his computer to send a message to his Internet Service Provider (ISP) directing the ISP to forward a text message to B's ISP. [FN35] To simplify matters, let's say that A's ISP is EarthLink, and B's ISP is America Online (AOL). EarthLink's computers received A's instructions, copied the text message, and then sent out another copy in the direction of the AOL server. That e-mail crossed the Internet until it arrived at the AOL mail server, which happens to be located in Virginia. [FN36] The next morning, when B sat at his desk and clicked on the icon to read the message from A, B was instructing his computer to send a request to the AOL server to run off a copy of the message and send it to him at his desk.

From the second officer's external perspective, obtaining the e-mail seems quite different from how it looked to the first officer. The second officer sees that he can obtain a copy of the e-mail from any one of four sources: A, who sent the e-mail; the Earth Link server located in California, which kept a copy before sending another copy to AOL; the AOL server in Virginia, which retained a copy in B's account; or B, who received a copy when he logged on and read the e-mail. To avoid tipping off A or B, the officer will probably want to go to the system administrator at EarthLink or AOL to get a copy of the message straight from their computers.

What process does the Fourth Amendment require? The second officer will reason that A sent a copy of the e-mail communication to a third party (the EarthLink computer), disclosing the communication to the third party and instructing it to send the communication to yet another third party (AOL). The officer will ask, what process does the Fourth Amendment require to obtain information that has been disclosed to a third party and is in the third party's possession? The officer will look in a Fourth Amendment treatise and locate to the black letter rule that the Fourth Amendment permits the government to ***367** obtain information disclosed to a third party using a mere subpoena. [FN37] The officer can simply subpoena the system administrator to compel him to produce the e-mails. No search warrant is required.

Who is right? The first officer or the second? The answer depends on whether you approach the Internet from an internal or external perspective. From an internal perspective, the officers need a search warrant; from the external perspective, they do not. [FN38]

2. Do Search Warrants Allow Remote Network Searches?

Let's consider a second example, one that reverses the implications of the internal and external approaches. Imagine that our two police officers give up on e-mail conspiracies and instead start investigating a local business that is a front for the mob in New York. The officers learn that the mob has stored a full set of records of the mob's illegal activities on the business's computer network. The officers obtain a search warrant to search the New York office of the business for the computer files. Importantly, the Fourth Amendment requires the warrant to be fairly narrow; the warrant must specifically name the place that will be searched ("the business offices of the Mob-front Company, 123 Pine Street, Suite 200") and name the evidence that will be seized ("computer files containing evidence of organized crime activity"). [FN39] The warrant gives the officers a limited grant of authority: It allows them to search the precise location of the business for the precise evidence described, and no more. [FN40]

Imagine that when the officers execute the search, they find several computer terminals inside the business offices that are connected to the network, but they cannot find the central computer server that stores the network's files. In fact, the network server is located hundreds or thousands of miles away, in another state, or perhaps even another country. The officers will face a question: Does ***368** their search warrant allow them to search the terminals inside the business and retrieve the information stored remotely on the network?

The first police officer, who prefers an internal perspective, will say "yes." This officer will approach the terminal and see various icons indicating the presence of the network's files. To him, the files listed are virtually present inside the terminal; he can access them from the network exactly as he would be able to access files stored on a local hard drive or floppy diskette. The first officer will look at the warrant, see that it authorizes him to search "123 Pine Street, Suite 200" for "computer files containing evidence of organized crime activity," and will conclude that the warrant authorizes him to search the terminal for the evidence.

The second police officer, who approaches the same problem from an external perspective, will disagree. He will reason that if he sits down at the terminal and starts looking through the files on the network, he will actually be instructing the terminal to send commands to the remote central server to run off copies of the files and send them back to him. Retrieving the files will not search "123 Pine Street, Suite 200," as his warrant allows, but rather will direct a search of the physical location of the server located hundreds or even thousands of miles away. If the server is located in California, he will be searching a place in California; if the server is in Canada, he will be searching a place in Canada. [FN41] The search warrant does not allow the officer to execute a search outside of "123 Pine Street, Suite 200," however, much less in another state or a foreign country. Accordingly, the second officer will conclude that the search warrant does not allow him to search the terminal for the network's remotely stored files. From an internal perspective, the search warrant authorizes the officers to search the terminal; from an external perspective, it does not.

Notably, the privacy implications of the two perspectives in this second hypothetical reverse

the implications of the first one. In the e-mail hypothetical, the internal perspective offers more privacy protection, whereas the opposite is true in the case of the remote network search. This should not surprise us. The internal and external perspectives offer two distinct and unrelated set of the Internet's facts, and the legal implications of the two perspectives should vary depending on the issue. In some cases the internal perspective will offer facts that lead to greater privacy protection, but in other cases the external perspective will be more protective.

C. COMPUTER CRIME

1. *United States v. Kammersell*

The Tenth Circuit's decision in *United States v. Kammersell* [FN76] provides a dramatic example of the importance of choosing between an internal and external perspective of the Internet. In this case, nineteen-year-old Matthew ***374** Kammersell used America Online's "instant message" service to send a bomb threat over the Internet from Riverdale, Utah (a suburb of Ogden, Utah) to his girlfriend's computer at work in downtown Ogden, a few miles away. [FN77] The government prosecuted Kammersell under 18 U.S.C. § 875(c), which makes it a federal felony to send an interstate communication "containing ... any threat to injure the person of another." [FN78]

The question facing the Court was whether Kammersell's instant message constituted an "interstate" threat. Kammersell argued that it did not. He offered an internal account of his conduct. From his perspective, he was located in Utah and had sent the threat to his girlfriend in Utah. His girlfriend was just a few miles away, in the same state. From Kammersell's perspective, there was nothing interstate about his threat, and the absence of a federal interstate nexus required the court to vacate his conviction. [FN79]

The government countered by approaching Kammersell's threat from an external perspective. Because America Online's servers are located in Virginia, the government noted, every AOL instant message must be routed from its point of origin to AOL's servers in Virginia, and then on to its destination. Unbeknownst to Kammersell, his instant message had traveled from Utah to Virginia, and then back to Utah. Kammersell's threat was in fact an "interstate" threat, as it had traveled most of the way across the country twice in the course of being delivered. [FN80]

Did Matthew Kammersell send an interstate threat? From an internal perspective, no; from an external perspective, yes. The Tenth Circuit adopted the government's external perspective and affirmed the conviction. [FN81]

2. *United States v. Thomas*

A 1996 obscenity case decided by the Sixth Circuit, *United States v. Thomas*, [FN82] provides a mirror image of *Kammersell*. As in *Kammersell*, the defendant's ***375** liability in *Thomas* hinged on whether the facts were approached internally or externally. Unlike *Kammersell*, however, the

defendant in *Thomas* asked the court to apply an external perspective, and the government advocated an internal perspective.

Robert and Carleen Thomas operated a computer bulletin board service from their home in California starting in 1991. [FN83] The bulletin board billed itself as "The Nastiest Place on Earth" and provided its paying customers with hard-core pornography. [FN84] Officials in Memphis, Tennessee began an investigation into whether the Thomases had violated federal obscenity laws. Eventually they set up an operation in which an undercover postal inspector in Memphis opened an account and used a computer to receive digital photographs formatted as GIF files from the Thomases' server. [FN85] The U.S. Attorney in Memphis charged the Thomases with almost a dozen violations of federal law, among them violations of 18 U.S.C. § 1465. [FN86] This statute makes it a federal crime to use a means of interstate commerce to transport an obscene "book, pamphlet, picture, film ... [or] image" in interstate commerce. [FN87] The government's theory was that the Thomases had used the Internet (a means of interstate commerce) to transport the GIF files (the images) in interstate commerce (from the server in California to the postal inspector in Tennessee). The jury convicted the Thomases on most of the counts, including six counts of violating 18 U.S.C. § 1465. [FN88]

On appeal, the Thomases argued that they had not violated the statute. They offered an external account of their conduct. They had not sent "images" to the undercover officer in Memphis, they reasoned, but merely had sent a "string of 0's and 1's" [FN89] from one computer to another. The fact that the "string of 0's and 1's" was a GIF file that could be translated by the postal inspector's computer into a visual image did not mean that the 0s and 1s were an "image" covered by ***376** the federal obscenity law. [FN90]

The Sixth Circuit rejected this external argument in favor of an internal description of the Thomases' conduct. According to the court, "the means by which the GIF files were transferred" did not matter so long as "the transmissions began with computer-generated images in California and ended with the same computer-generated images in Tennessee." [FN91] Because the data sent by the Thomases appeared as an image when "viewed on a computer screen" [FN92] by a computer user, it was an "image" according to federal obscenity law. From the court's internal perspective, technical details such as "[t]he manner in which the images moved" [FN93] seemed irrelevant. The court affirmed the conviction. [FN94]