

Computer Crime

Professor Ohm

Supplemental Reading for Monday, August 24, 2009

List of Included Readings

1. Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 2007 (excerpt).
2. Larry Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (excerpt).
3. Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED MAGAZINE THREAT LEVEL BLOG, Sept. 18, 2008, <http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/>. *Note: this article contains strong language.*
4. Jenna Wortham & Andrew E. Kramer, *Professor Main Target of Assault on Twitter*, N.Y. TIMES, Aug. 8, 2009, <http://www.nytimes.com/2009/08/08/technology/internet/08twitter.htm>.

Readings

1. Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 2007 (excerpt).

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.”

...

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 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 I don't know much about cyberspace; what I do know will be outdated in five years (if not five months!); and my predictions about the direction of change are worthless, making any effort to tailor the law to the subject futile.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.

...

If we are so far behind in matching law to a well-understood technology such as photocopiers--if we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth-- what chance do we have for a technology such as computers that is mutating faster than the virus in *The Andromeda Strain*?

Well, then, what can we do? By and large, nothing. If you don't know what is best, let people make their own arrangements.

Next after nothing is: keep doing what you have been doing. Most behavior in cyberspace is easy to classify under current property principles. What people freely make available is freely copyable. When people attach strings, they must be respected, and the tough question when someone copies commercial software will be whether the person making copies is a direct infringer or only a contributory infringer, and whether the remedy should be civil damages or time in prison. Lower costs of copying may make violations of the law more attractive, which suggests the allocation of additional prosecutorial resources, but movement along a cost continuum does not call for change in legal substance.

-
2. Larry Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (excerpt).

Introduction

A few years ago, at a conference on the ‘Law of Cyberspace’ held at the University of Chicago, Judge Frank Easterbrook told the assembled listeners, a room packed with ‘cyberlaw’ devotees (and worse), that there was no more a ‘law of cyberspace’ than there was a ‘Law of the Horse’; [FN1] that the effort to speak as if there were such a law would just muddle rather than clarify; and that legal academics (‘dilettantes’) should just stand aside as judges and lawyers and technologists worked through the quotidian problems that this souped-up telephone would present. ‘Go home,’ in effect, was Judge Easterbrook's welcome.

...

Easterbrook's concern is a fair one. Courses in law school, Easterbrook argued, 'should be limited to subjects that could illuminate the entire law.' [FN3] '[T]he best way to learn the law applicable to specialized endeavors,' he argued, 'is to study general rules.' [FN4] This 'the law of cyberspace,' conceived of as torts in cyberspace, contracts in cyberspace, property in cyberspace, etc., was not.

My claim is to the contrary. 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.

...

I. Regulatory Spaces, Real and 'Cyber'

Consider two cyber-spaces, and the problems that each creates for two different social goals. Both spaces have different problems of 'information'-- in the first, there is not enough; in the second, too much. Both problems come from a fact about code--about the software and hardware that make each cyber-space the way it is. As I argue more fully in the sections below, the central regulatory challenge in the context of cyberspace is how to make sense of this effect of code.

...

*507 B. Modalities of Regulation

1. Four Modalities of Regulation in Real Space and Cyberspace.--Behavior, we might say, is regulated by four kinds of constraints. [FN16] Law is just one of those constraints. Law (in at least one of its aspects) orders people to behave in certain ways; it threatens punishment if they do not obey. [FN17] The law tells me not to buy certain drugs, not to sell cigarettes without a license, and not to trade across

international borders without first filing a customs form. It promises strict punishments if these orders are not followed. In this way, we say that law regulates.

But not only law regulates in this sense. Social norms do as well. Norms control where I can smoke; they affect how I behave with members of the opposite sex; they limit what I may wear; they influence whether I will pay my taxes. Like law, norms regulate by threatening punishment *ex post*. But unlike law, the punishments of norms are not centralized. Norms are enforced (if at all) by a community, not by a government. In this way, norms constrain, and therefore regulate.

Markets, too, regulate. They regulate by price. The price of gasoline limits the amount one drives--more so in Europe than in the United States. The price of subway tickets affects the use of public transportation--more so in Europe than in the United States. Of course the market is able to constrain in this manner only because of other constraints of law and social norms: property and contract law govern markets; markets operate within the domain permitted by social norms. But given these norms, and given this law, the market presents another set of constraints on individual and collective behavior.

And finally, there is a fourth feature of real space that regulates behavior--'architecture.' By 'architecture' I mean the physical world as we find it, even if 'as we find it' is simply how it has already been made. That a highway divides two neighborhoods limits the extent to which the neighborhoods integrate. That a town has a square, easily *508 accessible with a diversity of shops, increases the integration of residents in that town. That Paris has large boulevards limits the ability of revolutionaries to protest. [FN18] That the Constitutional Court in Germany is in Karlsruhe, while the capital is in Berlin, limits the influence of one branch of government over the other. These constraints function in a way that shapes behavior. In this way, they too regulate.

These four modalities regulate together. The 'net regulation' of any particular policy is the sum of the regulatory effects of the four modalities together. A policy trades off among these four regulatory tools. It selects its tool depending upon what works best.

So understood, this model describes the regulation of cyberspace as well. There, too, we can describe four modalities of constraint.

Law regulates behavior in cyberspace--copyright, defamation, and obscenity law all continue to threaten *ex post* sanctions for violations. How efficiently law regulates behavior in cyberspace is a separate question--in some cases it does so more efficiently, in others not. Better or not, law continues to threaten an expected return. Legislatures enact, [FN19] prosecutors threaten, [FN20] courts convict. [FN21]

Norms regulate behavior in cyberspace as well: talk about democratic politics in the alt.knitting newsgroup, and you open yourself up to 'flaming' (an angry, text-based response). 'Spoof' another's identity in a 'MUD' (a text-based virtual reality), and you may find yourself 'toaded' (your character removed). [FN22] Talk too much on a discussion list, and you are likely to wind up on a common 'bozo' filter (blocking messages from you). In each case norms constrain behavior, and, as in real space, the threat of *ex post* (but decentralized) sanctions enforce these norms.

Markets regulate behavior in cyberspace too. Prices structures often constrain access, and if they do not, then busy signals do. (America Online (AOL) learned this lesson when it shifted from an hourly to *509 a flat-rate pricing plan. [FN23]) Some sites on the web charge for access, as on-line services like AOL have for some time. Advertisers reward popular sites; on-line services drop unpopular forums. These behaviors are all a function of market constraints and market opportunity, and they all reflect the regulatory role of the market.

And finally the architecture of cyberspace, or its code, regulates behavior in cyberspace. The code, or the software and hardware that make cyberspace the way it is, constitutes a set of constraints on how one can behave. [FN24] The substance of these constraints varies--cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space-- railroad tracks that divide neighborhoods, bridges that block the access of buses, constitutional courts located miles from the seat of the government-- they are experienced as conditions on one's access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password before one gains access; [FN25] in other places, one can enter whether identified or not. [FN26] In some places, the transactions that one engages in produce traces, or 'mouse droppings,' that link the transactions back to the individual; [FN27] in other places, this link is achieved only if the individual consents. [FN28] In some places, one can elect to speak a language that only the recipient can understand (through encryption); [FN29] *510 in other places, encryption is not an option. [FN30] Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates. [FN31]

These four constraints--both in real space and in cyberspace--operate together. For any given policy, their interaction may be cooperative, or competitive. [FN32] Thus, to understand how a regulation might succeed, we must view these four modalities as acting on the same field, and understand how they interact.

...

Conclusion

At the center of any lesson about cyberspace is an understanding of the role of law. We must make a choice about life in cyberspace--about whether the values embedded there will be the values we want. [FN140] The code of cyberspace constitutes those values; it can be made to constitute values that resonate with our tradition, just as it can be made to reflect values inconsistent with our tradition.

As the Net grows, as its regulatory power increases, as its power as a source of values becomes established, the values of real-space sovereigns will at first lose out. In many cases, no doubt, that is a very good thing. But there is no reason to believe

that it will be a good thing generally or indefinitely. There is nothing to guarantee that the regime of values constituted by code will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction. Indeed, to the extent that code writers respond to the wishes of commerce, a power to control may well be the tilt that this code begins to take. [FN141] Understanding this tilt will be a continuing project of the ‘law of cyberspace.’

Nevertheless, Judge Easterbrook argued that there was no reason to teach the ‘law of cyberspace,’ any more than there was reason to teach the ‘law of the horse,’ because neither, he suggested, would ‘illuminate the entire law.’ [FN142] This essay has been a respectful disagreement. The threats to values implicit in the law--threats raised by changes in the architecture of code--are just particular examples of a more general point: that more than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators--code, but also norms and the market--that must be addressed. Cyberspace makes plain not just how this interaction takes place, but also the urgency of understanding how to affect it.

-
3. Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED MAGAZINE THREAT LEVEL BLOG, Sept. 18, 2008, <http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/>. *Note: this article contains strong language.*

A person claiming to be the hacker who obtained access to Alaska Gov. Sarah Palin’s private Yahoo e-mail on Tuesday has posted a supposed first-person account of the hack, revealing the relatively simple steps he says he took to crack the private e-mail of the Republican vice-presidential candidate.

The story was briefly posted Wednesday to the 4chan forum where the hack first surfaced. Bloggers have connected the handle of the poster, "Rubico," to an e-mail address, and tentatively identified the owner as a college student in Tennessee.

Threat Level was unable to reach the student by phone because his number is unlisted. A person who identified himself as the student’s father, when reached at home, said he could not talk about the matter and would have no comment. The father is a Democratic state representative in Tennessee. Threat Level is not identifying them by name because authorities have not identified any suspects in the case, and the link to the student so far is tenuous. The father, in a second call with Threat Level late Thursday afternoon, said that neither he nor his son has been contacted by any law enforcement authorities. A local Tennessee paper had erroneously reported that his son had been contacted by authorities, he told Threat Level.

As detailed in the postings, the Palin hack didn’t require any real skill. Instead, the hacker simply reset Palin’s password using her birthdate, ZIP code and information about where she met her spouse — the security question on her Yahoo account, which was answered (Wasilla High) by a simple Google search.

The simplicity of the attack, of course, makes it no less illegal.

The hacker said that he read all of the e-mails in the Palin account and found "nothing incriminating, nothing that would derail her campaign as I had hoped. All I saw was personal stuff, some clerical stuff from when she was governor.... And pictures of her family."

Once the hacker had read the e-mails in Palin's account, he said he suddenly realized what he'd done and how vulnerable he was to being caught, since he'd used only a single proxy service to hide his IP address.

yes I was behind a proxy, only one, if this shit ever got to the FBI I was fucked, I panicked, i still wanted the stuff out there but I didn't know how to rapidshit all that stuff, so I posted the pass on /b/, and then promptly deleted everything, and unplugged my internet and just sat there in a comatose state

Once he posted the information to 4chan — the stronghold of the Anonymous griever collective — a good Samaritan tried to step in to protect Palin by resetting her password and sending an e-mail to one of her aides, Ivy Frye. But the white hat posted a screen shot of that e-mail to 4chan, and it included the new password. That triggered a feeding frenzy on the forum, as legions of channers competed to log in and reset Palin's password again.

That flurry of activity triggered a security feature that froze Palin's account for 24 hours, which was long enough for the information to hit the media. Palin, or someone in her camp, closed the account early Wednesday morning.

The postings telling the story have been deleted from 4chan, so I've included them below.

rubico 09/17/08(Wed)12:57:22 No.85782652

Hello, /b/ as many of you might already know, last night sarah palin's yahoo was "hacked" and caps were posted on /b/, i am the lurker who did it, and i would like to tell the story.

In the past couple days news had come to light about palin using a yahoo mail account, it was in news stories and such, a thread was started full of newfags trying to do something that would not get this off the ground, for the next 2 hours the acct was locked from password recovery presumably from all this bullshit spamming.

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower...

>> rubico 09/17/08(Wed)12:58:04 No.85782727

this is all verifiable if some anal /b/tard wants to think Im a troll, and there isn't any hard proof to the contrary, but anyone who had followed the thread from the beginning to the 404 will know I probably am not, the picture I posted this topic with is the same one as the original thread.

I read though the emails... ALL OF THEM... before I posted, and what I concluded was anticlimactic, there was nothing there, nothing incriminating, nothing that would derail her campaign as I had hoped, all I saw was personal stuff, some clerical stuff from when she was governor.... And pictures of her family

I then started a topic on /b/, peeps asked for pics or gtfo and I obliged, then it started to get big

Earlier it was just some prank to me, I really wanted to get something incriminating which I was sure there would be, just like all of you anon out there that you think there was some missed opportunity of glory, well there WAS NOTHING, I read everything, every little blackberry confirmation... all the pictures, and there was nothing, and it finally set in, THIS internet was serious business, yes I was behind a proxy, only one, if this shit ever got to the FBI I was fucked, I panicked, i still wanted the stuff out there but I didn't know how to rapidshit all that stuff, so I posted the pass on /b/, and then promptly deleted everything, and unplugged my internet and just sat there in a comatose state

Then the white knight fucker came along, and did it in for everyone, I trusted /b/ with that email password, I had gotten done what I could do well, then passed the torch , all to be let down by the douchebaggery, good job /b/, this is why we cant have nice things.

Gabriel Ramuglia who operates Ctunnel, the internet anonymizing service the hacker used to post the information from Palin's account to the 4chan forum, told Threat Level this morning that the FBI had contacted him yesterday to obtain his traffic logs. Ramuglia said he had about 80 gigabytes of logs to process and hadn't yet looked for the information the FBI was seeking but planned to be in touch with the agents today.

Ramuglia said the screenshots of Palin's e-mail account, which the hacker posted online, will help him narrow his search, since they revealed most of the Ctunnel URL that was at the top of the hacker's browser when he took the screen shot.

-
4. Jenna Wortham & Andrew E. Kramer, *Professor Main Target of Assault on Twitter*, N.Y. TIMES, Aug. 8, 2009, <http://www.nytimes.com/2009/08/08/technology/internet/08twitter.htm>.

The cyberattacks Thursday and Friday on Twitter and other popular Web services disrupted the lives of hundreds of millions of Internet users, but the principal target appeared to be one man: a 34-year-old economics professor from the republic of Georgia.

During the assault — the latest eruption in a yearlong skirmish between nationalistic hackers in Russia and Georgia — unidentified attackers sent millions of spam e-mail messages and bombarded Twitter, Facebook and other services with junk messages. The blitz was an attempt to block the professor's Web pages, where he was revisiting the events leading up to the brief territorial war between Russia and Georgia that began a year ago.

The attacks were “the equivalent of bombing a TV station because you don't like one of the newscasters,” Mikko Hyppönen, chief research officer of the Internet security firm F-Secure, said in a blog post. “The amount of collateral damage is huge. Millions of users of Twitter, LiveJournal and Facebook have been experiencing problems because of this attack.”

The blogger, a refugee from the Abkhazia region, a territory on the Black Sea disputed between Russia and Georgia, writes under the name Cyxymu, but identified himself only by the name Giorgi in a telephone interview. Giorgi, who said he taught at Sukhumi State University, first noticed Thursday afternoon that LiveJournal, a popular blogging platform, was not working for him. “I decided to go to Facebook,” he said. “And Facebook didn't work. Then I went to Twitter, and Twitter didn't work. ‘How strange,’ I thought, ‘What a coincidence they all don't work at once.’”

Security experts say that it is nearly impossible to determine who exactly is behind the attack, which disrupted access to Twitter, Facebook, LiveJournal and some Google sites on Thursday and continued to affect many Twitter users into Friday evening.

But Beth Jones, an analyst with the Internet security firm Sophos, said the assault occurred in two stages.

Early Thursday, the attackers sent out a wave of spam under the name Cyxymu, which is a Latin transliteration of the Cyrillic name of the capital of Abkhazia, Sukhumi. This technique, a “joe job,” is intended to discredit a Web user by making him appear to be the source of a large amount of junk e-mail. “These hackers wanted to make him look responsible for millions of spam e-mails,” said Ms. Jones.

The messages contained links to Giorgi's accounts on several social networks and Web sites, including Twitter.

The next leg of the attack, Ms. Jones said, was a distributed denial of service, or D.D.O.S., attack aimed at knocking Giorgi off the Web. The hackers used a botnet, a network of thousands of malware-infected personal computers, to direct huge amounts of junk traffic to Cyxymu's pages on Twitter, LiveJournal, YouTube and Facebook in an attempt to disable them, Ms. Jones said.

The junk messages overwhelmed the services, slowing them, and in the case of Twitter and LiveJournal, shutting them down entirely for a time.

Giorgi said his pages were providing a place for refugees from Abkhazia to exchange memories of their home. The Twitter page had a sepia photograph of a palm-lined city street. “It was nostalgia,” he said.

This week, he began posting day-by-day accounts of the run-up to the conflict that drew partly on posts from his readers inside of Abkhazia, who he said had been describing how the Russian army staged its forces in the region in early August 2008.

“I feel a bit ashamed for the people who lost service because my blog was blocked,” said Giorgi.

The hundreds of millions of Internet users affected were simply “collateral damage,” said Ms. Jones.

The attacks and their aftermath show just how vital Web tools and services are becoming to political discourse — and how vulnerable they are to disruption.

“They aren’t set up to play the role of a global communications network, but very quickly they’ve come to represent that,” said John Palfrey, a law professor and co-director of Harvard University’s Berkman Center for Internet and Society.

The attacks that felled Twitter shed light on the fragility of the popular microblogging service, especially compared to its competitor Facebook, which quickly recovered from the pummeling, said Stefan Tanase, a researcher at Kaspersky Lab, an Internet security firm. Twitter, a small San Francisco company, has been struggling to improve its security even as it tries to manage hypergrowth in the number of users and messages it handles.

But, Mr. Tanase said, “Twitter is definitely a company that is learning fast and reacting fast.”

The outage frustrated many Twitter users. Some migrated over to better-functioning social networks like Facebook and FriendFeed to send messages and follow conversations, said Jeremiah Owyang, an analyst at Forrester Research and a prolific tweeter.

“If Twitter goes down or shuts down permanently, the conversation just shifts somewhere else,” he said.

...