What's So Special About Information Security

Author : Michael Madison

Date : December 13, 2013

Andrea M. Matwyshyn, *The Law of the Zebra*, 28 **Berkeley Tech. L.J.** 155 (2013).

A debate continues to brew about the proper interpretation of the Computer Fraud and Abuse Act (CFAA), the federal statute that imposes criminal penalties on individuals who access computer networks without authorization. For at least a decade, scholars and a growing number of courts have wondered whether the owner of a computer network could define "authorization" using form "terms and conditions" of the sort often presented to consumers who purchase or use digital services. If that strategy were successful, then someone who clicked "I Agree" on a digital form yet failed to comply with all of its terms might be accused – even convicted – of the federal crime specified by the CFAA.

Andrea Matwyshyn uses that apparently technical problem to revisit a much larger question: When, whether, and how the law should treat computers and computer networks as special in any way when dealing with a host of doctrinal and policy issues: commercial law, intellectual property law, telecommunications law, antitrust law, criminal law, and so on? This was the subject of a famous scholarly debate back at the turn of the 21st century between Lawrence Lessig, who argued that considering a "law of cyberspace" offered commentators access to potentially valuable insights about how people interact with each other[1], and Judge Frank Easterbrook, who accused cyberspace promoters of constructing an unworkable and unhelpful "law of the horse."[2] No one "won" the debate in its original form, but in the late 1990s the question was mostly academic, literally. Too few law and policy judgments turned on the answer to make the debate matter in any but a conceptual or theoretical sense.

Matwyshyn's "The Law of the Zebra" suggests that the answer does matter in a concrete set of cases, and she has the case reports to show it. Her answer is that both Lessig and Easterbrook were right: There is something special about computers and computer networks. But what's special about them is that judges should not be seduced into treating them as something new and strange. Most of the time, the common law deals with them, or should deal with them, just fine. Courts that fail to remember that fact are dealing in a "law of the zebra," an unusual creature, rather than a law of the horse (of course), an ordinary and more common animal.

In one sense, then, the article resumes a dialogue about metaphorical treatments of the Internet that captured the imaginations of a host of legal scholars a decade or so ago, including me. Is cyberspace a thing? A place? A frontier? A horse? A zebra?

That question has no single answer, and Matwyshyn is smart enough not to propose one. Instead, she wants to show how the alleged specialness of computer networks leads courts astray. The CFAA and breaches of relevant contracts form the doctrinal backbone of an inquiry into techno-exceptionalism.

She shows how courts have dealt with contract formation and breach of contract questions in computer access contexts in inconsistent ways, and how that inconsistency has affected application of the CFAA. She identifies her normative baseline – a series of related principles or propositions that define a common law contract framework – and argues that in contract formation questions, a degree of techno-exceptionalism is warranted; in contract interpretation and enforcement contexts, "regular" contract

law will do. Using four paradigmatic examples of "types" of computer hackers who might breach agreements with network providers – the sorts of people the CFAA was arguably drafted to deal with – she shows how her balanced form of "restrained technology exceptionalism" treats CFAA/contract law intersections. Ordinary contract remedies are sufficient to deal with the harms that result from most types of unauthorized network access linked to bypassing agreed-to terms and conditions. She argues that adding criminal liability under the CFAA to those remedies amounts to a sort of "weaponized" breach of contract that is warping basic contract law as applied in computer contexts, is bad policy, and arguably conflicts with Constitutional law prohibiting peonage. The proper way to look at the CFAA/contract interface, she argues, is through the prism of private ordering, a framework that is consistent both with Lessig's view of cyberspace law (in which computer networks present novel forms of private ordering for fresh normative evaluation) and Easterbrook's (in which existing doctrinal categories were more than adequate to that normative task).

On the doctrinal question, is she right? Possibly. But the doctrinal means are less important here than the policy ends. In effect, Matwyshyn argues that contract remedies should preempt CFAA liability where the two overlap. That sort of "reverse federalism" ("reverse" because, of course, we rarely think of state law preempting federal law) is, in a perverse way, quite consistent with a heterogeneous, anti-one-size-fits-all view of the Internet. Matwyshyn is not making an appeal to an idealized "information wants to be free" fantasy. Instead, she points out that the real policy at stake in interpretations of the CFAA, and in metaphorical debates about horses and zebras, is information security. Linking criminal liability under the CFAA to breaches of the standardized, form-based terms and conditions that are essentially ubiquitous on the Internet trivializes the idea of access and undermines incentives for network providers to care properly for information that they truly care about.

1. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 **Harv. L. Rev.** 501 (1999).
2. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 **U. Chi. L.F.** 207 (1996).

Cite as: Michael Madison, *What's So Special About Information Security*, JOTWELL (December 13, 2013) (reviewing Andrea M. Matwyshyn, *The Law of the Zebra*, 28 **Berkeley Tech. L.J.** 155 (2013)), https://cyber.jotwell.com/whats-so-special-about-information-security/.