Deterring Cybercrime: The Focus on Intermediaries

April 25, 2017 in 2017 Online Forum: Platform Law

Aniket Kesari[1]

Amanda Maya[2]

Chris Hoofnagle[3]

Damon McCoy[4]

Precis for Platform Law: Public and Private Regulation of Online Platforms

April 2017

Keywords: Financially-motivated cybercrime, intermediary liability, CDA 230, deterrence by punishment, deterrence by denial, botnets, anti-counterfeiting, Rule 65, TRO, SDN, OFAC, hacking, DNS seizure

Businesses that sell illegal pharmaceuticals, pirated media, counterfeit goods, and computer attacks online have similar goals and needs as ordinary firms. Both kinds of enterprises must acquire new customers, have a supply chain, maintain a web presence, collect payments, deliver a product or service, and finally, cultivate a positive reputation to encourage repeat sales. In pursuit of profit, the legitimate and illegitimate alike depend on many third parties, including web hosts, payment providers, and shipping companies.

Licit businesses respond to traditional deterrence by punishment, through fines, threats, and regulatory actions. But enforcers often cannot use traditional deterrence against cybercriminals because of limits of law enforcement expertise and resources, competing enforcement priorities, and jurisdictional challenges. As a result, enforcers—both public and private—have turned to deterrence by denial approaches. Frustrated in attempts to reach the actual bad actor, enforcers focus on third parties critical to business operation. The Computer Science literature identifies attacks on service providers as an area of great vulnerability for financially-motivated cybercriminals.[5]

Yet, much of the legal academic scholarship on internet intermediaries focuses on their general immunity from state law actions under the Communications and Decency Act Section 230 (CDA 230). CDA 230 is interpreted to create broad immunity among internet intermediaries from the bad acts of their users.

For the Symposium, we have focused our lens on interventions unaffected by CDA 230. Specifically, we focus on the mechanisms that take advantage of intermediaries' role as gatekeepers. These include the use of Federal Rules of Civil Procedure Rule 65 by both private and public entities to seize domains used by botnet operators and by counterfeit good producers; the new emergence of Federal Rules of Criminal Procedure Rule 41 for anti-botnet takedowns; the expanded authorities to use the Department of the Treasury's Specially Designated Nationals list to block transactions with foreign cybercriminals; specialized domain name service take-down procedures used by the government; the attempts of law enforcement to leverage payment and banking systems as gatekeepers for illegal activities including platforms that promote "escort" services; and finally, we cover private-sector intermediary regulations, such as eBay's Verified Rights Online Program.

A focus on intermediaries raises due process and fairness concerns because such companies may not be aware of the criminal activity. Cybercriminals may use ordinary users' accounts and computers for attacks and monetization of crimes. Thus, when a victim of cybercrime investigates and makes interventions, legal demands may fall upon third parties, businesses that were merely used as a conduit by the suspect. These businesses themselves may have been hacked or otherwise believe that they are a victim of the cybercrime. Compliance may impose costs on intermediaries and costs to civil society in the form of censorship or in the erosion of internet anonymity as intermediaries demand that ordinary users provide documentation of their identity. The interventions we describe are often done *ex parte*, raising the risk that others' interests may not be fully considered by a neutral magistrate.

In sum, our work provides a classification of an understudied area of intermediary liability and regulation. While CDA 230 provides broad immunity for service providers in matters relating to privacy invasions, defamation and stalking, the same immunities are not present in other contexts. Specifically, when policing financially-motivated cybercrime, both public and private actors can subject intermediaries to costly, broad interventions. Our work highlights the current legal practices in this space, and evaluates their merits and demerits.

[1] UC Berkeley School of Law, Jurisprudence & Social Policy

[2] UC Berkeley School of Law

[3] UC Berkeley School of Law & School of Information

[4] New York University Tandon School of Engineering

[5] Zachary K. Goldman & Damon McCoy, Deterring Financially Motivated Cybercrime, 8 J. Nat'l Security L. & Pol'y 595 (2016), http://heinonline.org/HOL/Page?

handle=hein.journals/jnatselp8&g_sent=1&collection=journals&id=606; Chris Jay Hoofnagle, Ibrahim Altaweel, Jaime Cabrera, Hen Su Choi, Katie Ho, and Nathaniel Good, *Online Pharmacies and Technology Crime*, *in* The Handbook of Technology, Crime and Justice (Michael McGuire and Thomas J. Holt, eds.) (Routledge Press 2017).

CONTACT

Berkeley Technology Law Journal
U.C. Berkeley School of Law
Student Center, Ste. 3
Berkeley, California 94720-7200
btlj@law.berkeley.edu

JOIN BTLJ

Membership in BTLJ is open to all students at the University of California, Berkeley School of Law. Students interested in joining should e-mail btlj@law.berkeley.edu.