Journal of Criminal Law and Criminology

Volume 103 | Issue 3 Article 1

Summer 2013

Foreword

Lily Katz

0091-4169/13/10303-0663
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3
 Printed in U.S.A.

SYMPOSIUM ON CYBERCRIME

FOREWORD

Lily Katz*

In the months leading up to our Symposium, held at Northwestern University School of Law on February 1, 2013, cybercrime dominated news headlines. Just weeks before the Symposium, federal prosecutors in the Southern District of New York charged three men with an elaborate bank-fraud conspiracy that stole tens of millions of dollars from personal and commercial bank accounts around the world.[1] However, this was no ordinary bank heist. The robbers used "neither a mask nor a gun, just a clever program and an Internet connection."[2] The "clever program" was a sophisticated malware code called the "Gozi Virus," which, through various methods including e-mailed .pdf attachments, infected more than 100,000 computers around the world and at least 25,000 computers in the United States. The virus collected private usernames, passwords, and other data that allowed the bank robbers to fraudulently transfer money out of the victims' bank accounts.[3]

---

* J.D., Northwestern University School of Law, 2013; Symposium Editor, *Journal of Criminal Law and Criminology*, vol. 103. The author—and the *Journal*—owe tremendous gratitude to various people who made this Symposium possible. Thank you to Jim McMasters, Jessica Clements, and the members of the marketing and communications departments at Northwestern University School of Law. We are also in debt to the *Journal*'s 2012–13 editorial board, particularly Caitlin Kovacs, Michael Krantz, Max Tanner, and Elie Zenner. Finally, thank you to all of the Symposium participants, including our illustrious authors and panelists.

[1] Information, United States v. Kuzmin at 1, No. 11 Cr. 387 (S.D.N.Y. Jan. 23, 2013) [hereinafter Information, *Kuzmin*]; *see also* Press Release, U.S. Attorney's Office for the S. Dist. of N.Y., Three Alleged International Cyber Criminals Responsible for Creating and Distributing Virus that Infected over One Million Computers and Caused Tens of Millions of Dollars in Losses Charged in Manhattan Federal Court (Jan. 23, 2013), *available at* http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusPR.php.

[2] Press Release, *supra* note 1 (quoting Manhattan U.S. Attorney Preet Bharara's statements on the case).

[3] Information, *Kuzmin*, *supra* note 1, at 1–2.

Cybercrime also landed in news headlines in the months before our Symposium following the death of twenty-five-year-old hacker Aaron Swartz. Swartz, a famed coder and online activist,[4] committed suicide in January 2013, just months before he was to face trial for numerous felony counts of violating the Computer Fraud and Abuse Act (CFAA).[5] Swartz's death has inspired a fresh critique of the CFAA, the primary federal antihacking statute, from legislators,[6] the online community,[7] legal academia,[8] and now the *Journal*.[9] The Gozi Virus bank-fraud conspiracy and the Swartz matter demonstrate how computers are changing the landscape of criminal law.

But cybercrime not only makes for interesting news stories, it also raises important conceptual, doctrinal, and empirical legal questions. Addressing those legal issues is the focus of this Symposium.

Questions about data security, Internet privacy, and law enforcement tactics in our ever-changing digital world abound. Digital networks are opening up new avenues for criminal activity, sparking fresh debate about whether our criminal law regime is equipped to handle emerging cyberthreats. And as technology creates new criminal threats—calling into question our law's response—it also provides law enforcement with novel techniques to combat and prevent crime. Therefore, even as this Symposium highlights some of the most nefarious uses of digital networks, we realize that technology creates other types of concerns when placed in

---

[4] *See* Michael Martinez, *Internet Prodigy, Activist Aaron Swartz Commits Suicide*, CNN.COM (Mar. 7, 2013, 11:41 AM), http://www.cnn.com/2013/01/12/us/new-york-reddit-founder-suicide.

[5] *See* David Kravets, *Feds Charge Activist with 13 Felonies for Rogue Downloading of Academic Articles*, WIRED.COM (Sept. 18, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/09/aaron-swartz-felony/all/.

[6] For example, California Congresswoman Zoe Lofgren recently proposed a revision to the CFAA. *See* Aarons's Law Act, H.R. 18, 113th Cong. (2013), *available at* http://www.lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf; *see also* Suzanne Choney, *'Aaron's Law' to Honor Internet Activist, Redefine Computer Fraud*, NBC NEWS (Jan. 16, 2013, 6:44 PM), http://www.nbcnews.com/technology/technolog/aarons-law-honor-internet-activist-redefine-computer-fraud-1B8005442; Kim Zetter, *'Aaron's Law' Proposes Reining in Federal Anti-Hacking Statute*, WIRED.COM (Feb. 1, 2013, 5:51 AM), http://www.wired.com/threatlevel/2013/02/aarons-law-amending-the-cfaa/.

[7] *See* Marcia Hofmann, *In the Wake of Aaron Swartz's Death, Let's Fix Draconian Computer Crime Law*, ELECTRONIC FRONTIER FOUND. (Jan. 14, 2013), https://www.eff.org/deeplinks/2013/01/aaron-swartz-fix-draconian-computer-crime-law.

[8] *See* Orin Kerr, *The Criminal Charges Against Aaron Swartz (Part 1: The Law)*, VOLOKH CONSPIRACY (Jan. 14, 2013, 2:50 AM), http://www.volokh.com/2013/01/14/aaron-swartz-charges/.

[9] David Thaw, *Criminalizing Hacking Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 909 (2013).

the hands of law enforcement. Several articles in this Issue identify and address lingering questions about permissible law enforcement tactics and Fourth Amendment protections after *United States v. Jones*.[10] In the hands of both criminals and law enforcement, computers challenge individuals' privacy and security, create new obstacles in trial practice for prosecutors and defense attorneys, and test the limits of our Constitution.

At this crossroads of technology and criminal law, our path is unknown. Challenges inherent to cybercrime evolve just as quickly as the technology that creates those challenges. In the face of this unpredictable future, our Symposium aims to capture and explore some of the unique debates within this field.

Further, the issues raised in this Symposium are everyone's concern. Cyberthreats implicate numerous practice areas within and outside of criminal law, including constitutional law, intellectual property law, international law, healthcare law, financial law, and sex crimes. They also affect a wide scope of entities and groups, including law enforcement, government agencies at the state and federal levels, foreign bodies, private for-profit companies, lawyers, and private citizens. Cybercrime is in all our futures, and, as such, the following articles carry weight for us all.

[10] 132 S. Ct. 945, 957 (2012).