Cybercrime 2020:
Revisiting the Future of Online Crime and Investigations

November 29, 2018

Co-sponsored by
Georgetown University Law Center and the
Criminal Division of the U.S. Department of Justice

Georgetown Law
Gewirz 12th Floor
120 F Street, NW
Washington, D.C. 20001

In December 2014, Georgetown University Law Center and the U.S. Department of Justice held *Cybercrime 2020*, an examination of where technology was headed, how it was likely to be exploited in the near future, and what law enforcement could do to address developing threats while balancing privacy and civil liberties. This year, *Cybercrime 2020: Revisiting the Future of Online Crime and Investigations* will reexamine the predictions made at our last symposium and explore how newly emerging cybercrime trends and the courts' latest technology-focused rulings are reshaping investigative techniques. The symposium's panels will explore how the courts and policymakers—in the U.S. and abroad—are likely to respond to recent advances in technology and evolving tech policy, and whether U.S. law enforcement's existing tools and capabilities are up to the challenges ahead. The conference will bring together experts from academia, the government, judiciary, and private industry to shed light on the future of online crime and investigations.

Welcome and Opening Remarks (9:00 am - 9:10 am):

- Professor Laura Donohue, Georgetown Law
- John P. Cronan, Principal Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice (DOJ)

Breakfast Address (9:10 am - 9:55 am):

- Peter Singer, Strategist and Senior Fellow, New America
- *In conversation with* Leonard Bailey, Head of Cybersecurity Unit, DOJ, Computer Crime & Intellectual Property Section (CCIPS)

Panel 1 – New Tech, New Crimes? (9:55 am - 11:10 am): How will tomorrow's cyber criminals exploit new technologies—from drones to "IoT" to cryptocurrencies—as consumers, businesses, and government begin adopting them? How might criminals use new attack vectors, like interference with GPS and cellphone signals? What technological challenges will law enforcement face in investigating these new means of committing cybercrime? Will new machine learning, artificial intelligence, and other cybersecurity technologies help thwart cybercrime, or might they be corrupted to become part of the problem?

Moderator: Michael Stawasz, Deputy Chief, DOJ, CCIPS
Discussants: Andrea Limbago, Chief Social Scientist, Virtru
Davi Ottenheimer, Founder, MongoDB
Trent Teyema, Senior VP and Chief Technology Officer, Parsons Corporation
Heather West, Senior Policy Manager, Mozilla

Break (11:10 am - 11:30 am)

Panel 2 – Legislating Future Crimes: Will New Prosecutorial Tools Be Necessary? (11:30 am – 12:45 pm): Are current laws "technology-neutral" enough to criminalize new cyber threats or do some criminal laws need to be amended—or new laws passed—to cover activities that may warrant prosecution in the future, such as communications jamming, "deep fake" video technology, invasive use of drones, and financial crimes involving crypto-currencies? Will federal laws need to be amended to incentivize victims to practice self-help to respond to cyber intrusions and attacks in recognition of limited government resources? Are we overlooking other gaps in the law?

Moderator: William Hall, Senior Counsel, DOJ, CCIPS
Discussants: Richard DiZinno, Chief Counsel for National Security and Crime, Senate Judiciary Committee
Professor Mary Anne Franks, University of Miami School of Law
Harley Geiger, Director of Public Policy, Rapid7
Professor Stephanie Pell, West Point's Army Cyber Institute

Lunch: (12:45 pm - 2:05 pm)

Keynote Address (1:00 pm - 1:30 pm):

- Deputy Attorney General Rod J. Rosenstein, DOJ

Break (1:40 pm – 2:05 pm)

Panel 3 – Investigative Tools and Techniques of Tomorrow: (2:05 pm – 3:20 pm): Emerging technology may provide law enforcement with new challenges as cyber criminals use them to mask their crimes and identities and to thwart surveillance, but it may also furnish law enforcement with new opportunities to amass new types of evidence from novel sources and to and sift through large caches of data to extract evidence. How suitable are current electronic surveillance statutes like the Stored Communications Act, Wiretap Statute, and Pen Register/Trap and Trace Act for the collection of data from likely future crimes scenes, like IoT devices and autonomous cars? What types of new investigative tools are needed for nefarious activities such as network intrusions, ransomware, network manipulation, and other types of technology-intensive crimes?

Moderator: Professor Jen Daskal, American University Washington College of Law
Discussants: Megan Brown, Wiley Rein LLP
Patrick Day, Senate Judiciary Committee, Senator Feinstein
Deputy Assistant Attorney General Richard Downing, DOJ, Criminal Division
Michele Korver, Digital Currency Counsel, DOJ

Break (3:20 pm - 3:40 pm)

Panel 4 – *Carpenter* and the Future of the Fourth Amendment: Where Do We Go from Here? (3:40 pm - 4:55 pm): The use of new investigative techniques will be tested by evolving Fourth Amendment jurisprudence. How do the prosecutorial tools and investigative techniques raised by the prior panels look in light of judicial doctrine? What constitutional issues do they raise? The Supreme Court's decision in *United States v. Carpenter* may end up being a lynchpin of future legal decisions; however, the Court's opinion raised as many questions as it answered. How will *Carpenter* shape surveillance and privacy laws? Will its reasoning be extended to areas other than location information? If so, under what rationale? How will it affect other Fourth Amendment jurisprudence, such as the third-party and private-search doctrines?

Moderator: Professor Laura Donohue, Georgetown Law
Discussants: April Falcon Doss, Saul Ewing Arnstein & Lehr LLP
Nathan Judish, Senior Counsel, DOJ, CCIPS
Professor Paul Ohm, Georgetown Law
Michelle Richardson, Director of the Data and Privacy Project, Center for Democracy & Technology

Concluding Remarks (4:55 pm - 5:00 pm): Leonard Bailey, Head of Cybersecurity Unit, DOJ, CCIPS