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. Today, *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. Today's conference brings together experts from academia, government, Congress, 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: A Conversation with Peter Singer about "LikeWar: The Weaponization of Social Media" (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, 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

Luncheon (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: Patrick Day, Senate Judiciary Committee, Senator Feinstein

Deputy Assistant Attorney General Richard Downing, DOJ, Criminal Division

Matthew Gardner, Wiley Rein LLP

Louisa Marion, DOJ, CCIPS

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

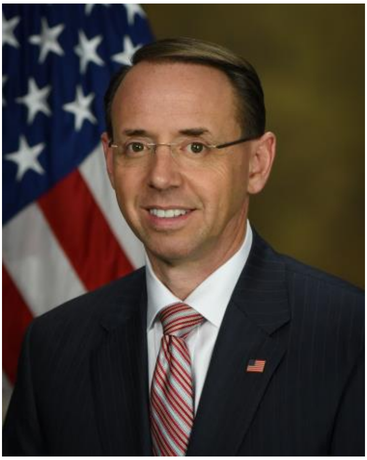
KEYNOTE ADDRESS BIOGRAPHIES

PETER WARREN SINGER
Strategist and Senior Fellow,
New America

Peter Warren Singer has been named by the Smithsonian as one of the nation's 100 leading innovators, by Defense News as one of the 100 most influential people in defense issues, by Foreign Policy to their Top 100 Global Thinkers List, as an official "Mad Scientist" for the U.S. Army's Training and Doctrine Command, and by Onalytica social media data analysis as one of the ten most influential voices in the world on cybersecurity and 25th most influential in the field of robotics. Peter's award winning books include *Corporate Warriors: The Rise of the Privatized Military Industry*, *Children at War*, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*; and *Cybersecurity and Cyberwar: What Everyone Needs to Know* and *Ghost Fleet: A Novel of the Next World War*, a technothriller crossed with nonfiction research, which has been endorsed by people who range from the Chairman of the Joint Chiefs to the co-inventor of the Internet to the writer of HBO Game of Thrones. His upcoming nonfiction book, *LikeWar*, was released in October 2018 and explores how social media has changed war and politics, and war and politics has changed social media.

His past work include serving at the Office of the Secretary of Defense, Harvard University, and as the founding director of the Center for 21st Century Security and Intelligence at Brookings, where he was the youngest person named senior fellow in its 100 year history.

ROD J. ROSENSTEIN
Deputy Attorney General,
U.S. Department of Justice



Rod J. Rosenstein was sworn in as the 37th Deputy Attorney General of the United States on April 26, 2017, by Attorney General Jeff Sessions.

Mr. Rosenstein graduated from the Wharton School of the University of Pennsylvania, with a B.S. in Economics, summa cum laude, in 1986. He earned his J.D. *cum laude* in 1989 from Harvard Law School, where he was an editor of the Harvard Law Review. Upon graduation, he served as a law clerk to Judge Douglas H. Ginsburg of the U.S. Court of Appeals for the District of Columbia Circuit.

After joining the U.S. Department of Justice through the Attorney General's Honors Program in 1990, Mr. Rosenstein prosecuted public corruption cases as a trial attorney with the Public Integrity Section of the Criminal Division. He then served as Counsel to the Deputy Attorney General (1993 - 1994), Special Assistant to the Criminal Division's Assistant Attorney General (1994 - 1995), and Associate Independent Counsel (1995 - 1997).

In 1997, Mr. Rosenstein became an Assistant U.S. Attorney in Maryland. He prosecuted cases in the U.S. District Court and briefed and argued appeals in the U.S. Court of Appeals for the Fourth Circuit. He also coordinated the credit card fraud and international assistance programs.

From 2001 to 2005, Mr. Rosenstein served as Principal Deputy Assistant Attorney General for the Tax Division of the U.S. Department of Justice. He supervised the Division's criminal sections and coordinated the tax enforcement activities of the Tax Division, the U.S. Attorney's Offices and the Internal Revenue Service. He also oversaw civil litigation and served as the acting head of the Tax Division when the Assistant Attorney General was unavailable, and he personally briefed and argued federal civil appeals.

Mr. Rosenstein served as the United States Attorney for the District of Maryland from 2005 to 2017. He oversaw federal criminal and civil litigation and developed and implemented federal law enforcement strategies in Maryland. During his tenure as U.S. Attorney, Mr. Rosenstein served on the Washington/Baltimore High-Intensity Drug Trafficking Area Task Force and on the Attorney General's Advisory Committee. He also personally litigated cases in the U.S. District Court and in the U.S. Court of Appeals for the Fourth Circuit.

President Donald J. Trump announced his intention to nominate Mr. Rosenstein on January 31, 2017. The Senate confirmed his nomination on April 25, 2017.

PARTICIPANT BIOGRAPHIES

LEONARD BAILEY, *Special Counsel for National Security, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice; Head of CCIPS' Cybersecurity Unit, U.S. Department of Justice*

Leonard Bailey joined DOJ's Terrorism and Violent Crime Section in 1991. In the late 1990's, he served as Special Counsel and Special Investigative Counsel to DOJ's Inspector General and supervised sensitive investigations of Department officials and programs. In 2000, he joined CCIPS where he has prosecuted computer crime and intellectual property cases; advised on matters related to searching and seizing electronic evidence and conducting electronic surveillance; and chaired the Organization of American States' Group of Government Experts on Cybercrime.

In 2009, he moved to DOJ's National Security Division. As Senior Counselor to the Assistant Attorney General for National Security, he focused on critical infrastructure protection, offensive and defensive cyber policy, and application of national security cyber authorities in criminal matters. He next served as an Associate Deputy Attorney General in the Office of the Deputy Attorney General, where he coordinated DOJ's cyber policy and initiatives and its cyber-related work with the National Security Council. He returned to CCIPS in 2013 where he currently leads their work on cybersecurity policy.

Leonard is a graduate of Yale University and Yale Law School. He has taught courses on cybersecurity and cybercrime at Georgetown Law School and Columbus School of Law in Washington, D.C.

JOHN P. CRONAN, *Principal Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice*

John P. Cronan participates in the supervision of the Criminal Division's more than 600 attorneys who prosecute financial crimes and fraud, money laundering, public corruption, cybercrime, intellectual property theft, organized and transnational crime, child exploitation, international narcotics trafficking, human rights violations, and other crimes. From November 2017 to July 2018, John also served as the Acting Assistant Attorney General of the Criminal Division. Prior to joining the Criminal Division, John supervised the Terrorism and International Narcotics Unit of the U.S. Attorney's Office for the Southern District of New York, where he oversaw the investigation and prosecution of international and domestic terrorism offenses, large-scale international drug trafficking, espionage, and export violations. John graduated from Georgetown University and Yale Law School, and clerked for the Honorable Robert A. Katzmann and the Honorable Barrington D. Parker, Jr. on the U.S. Court of Appeals for the Second Circuit.

JENNIFER DASKAL, *Associate Professor of Law, American University Washington College of Law*

Jennifer Daskal teaches and writes in the fields of criminal, national security, and constitutional law. From 2009 to 2011, Daskal was counsel to the Assistant Attorney General for National Security at the Department of Justice. Prior to joining DOJ, Daskal was senior counterterrorism counsel at Human Rights Watch, worked as a staff attorney for the Public Defender Service for the District of Columbia, and clerked for the Honorable Jed S. Rakof in the Southern District of New York. She also spent two years as a national security law fellow and adjunct professor at Georgetown Law Center. From 2016 to 2017, she was an Open Society Institute Fellow working on issues related to privacy and law enforcement access to data across borders.

Daskal is a graduate of Brown University, Harvard Law School, and Cambridge University, where she was a Marshall Scholar. Recent publications include *Borders and Bits* (Vanderbilt Law Review 2018); *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues* (Journal of National Security Law and Policy 2016); *The Un-Territoriality of Data* (Yale Law Journal 2015); *Pre-Crime Restraints: The Explosion of Targeted, Non-Custodial Prevention* (Cornell Law Review 2014); and *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone* (University of Pennsylvania Law Review 2013). Daskal has published op-eds in the NEW YORK TIMES, WASHINGTON POST, and INTERNATIONAL HERALD TRIBUNE and has appeared on BBC, C-

Span, MSNBC, and NPR, among other media outlets. She is an Executive Editor of and regular contributor to the Just Security blog.

PATRICK DAY, *Counsel, U.S. Senate Committee on the Judiciary, Ranking Member Dianne Feinstein*

Patrick Day serves as Counsel for national security issues for Ranking Member Dianne Feinstein (D-CA) on the Senate Judiciary Committee. He is responsible for advising the Senator on a variety of issues including the Foreign Intelligence Surveillance Act (FISA) and Electronic Communications Privacy Act, as well as general policies regarding counterterrorism, counterintelligence and cybersecurity. Patrick has spent the last 10 years working in national security policy in the U.S. Senate. Prior to his current position, he represented Senators Jeanne Shaheen (D-NH) and Jim Webb (D-VA) on the Senate Armed Services Committee. Patrick is a graduate of the University of Tennessee, has an M.A. from the College of International Security Affairs at the National Defense University in Washington D.C., and has a J.D. from the Washington College of Law at American University.

RICHARD DIZINNO, *Chief Counsel for National Security and Crime, Senate Judiciary Committee*

Richard DiZinno works on national security policy, including 702 reauthorization, USA Freedom Act, and issues involving Foreign Agents Registration Act, Economic Espionage Act, Authorization of Use of Force, counterintelligence, counterterrorism, and sanctions. He also works on cybersecurity policy and issues involving access to electronic data, including Computer Fraud and Abuse Act, Electronic Communications Privacy Act, CLOUD Act, encryption, and counter drone authorities. From 2009 through 2017, was an Assistant U.S. Attorney with the U.S. Attorney's Office for the District of Columbia, where he tried over 50 bench and jury trials. While with the U.S. Attorney's Office, he worked in the Homicide, Fraud, and Public Corruption sections, and he served as a senior AUSA in the National Security Section before leaving for the Senate. From 2005 to 2009, he worked in private practice at Howrey LLP handling criminal and civil litigation in antitrust and general commercial cases. From 2002 to 2003, he served as a Judicial Assistant for Chief Judge Hogan in the *In Re Vitamins Antitrust Litigation*. Richard graduated from George Washington University Law School in 2004, where he was a member of the Phi Delta Phi Legal Honor Society, and the Moot Court Board. He earned a B.A. in Economics and French from College of the Holy Cross in 1996.

LAURA K. DONOHUE, *Professor of Law, Georgetown Law, Director of Georgetown's Center on National Security and the Law, Director of the Center on Privacy and Technology*

Laura K. Donohue writes on constitutional law, legal history, emerging technologies, and national security law. Her most recent book, *The Future of Foreign Intelligence: Privacy and Surveillance in a Digital Age* (Oxford University Press, 2016), was awarded the 2016 IIT Chicago-Kent College of Law/Roy C. Palmer Civil Liberties Prize. She also has written *The Cost of Counterterrorism: Power, Politics, and Liberty* (Cambridge University Press, 2008); and *Counterterrorist Law and Emergency Law in the United Kingdom 1922-2000* (Irish Academic Press, 2007).

Professor Donohue's articles have been published by California Law Review, University of Chicago Law Review, Stanford Law Review, University of Pennsylvania Law Review, Harvard Journal of Law and Public Policy, and numerous other scholarly journals.

In November 2015, the U.S. Foreign Intelligence Surveillance Court appointed her as one of five amici curiae under the 2015 USA FREEDOM Act.

Professor Donohue is a Life Member of the Council on Foreign Relations; an Advisory Board Member of the Electronic Privacy Information Center; and Reporter for the American Bar Association's Criminal Justice Section Task Force on Border Searches of Electronic Devices. She has served on the Board of the American Bar Association's Standing Committee on Law and National Security and is a Senior Scholar at Georgetown Law's Center for the Constitution.

Donohue obtained her AB in Philosophy (with Honors) from Dartmouth College; her MA in Peace Studies (with Distinction) from the University of Ulster, Northern Ireland; her JD (with Distinction) from Stanford Law School; and her PhD in History from the University of Cambridge, England.

APRIL DOSS, *Partner, Saul Ewing Arnstein & Lehr LLP*

April Doss is a seasoned litigator with extensive in-house experience who offers clients significant insight on data privacy and cybersecurity based on her years of service in high-level government jobs connected to the intelligence community. Her knowledge about cybersecurity and data privacy is informed by her tenure as the senior minority counsel for the Russia Investigation in the Senate Select Committee on Intelligence (SSCI), as well as her many years at the National Security Agency (NSA), where she was associate general counsel for intelligence law.

In her year-long role advising the Senate committee, April served as lead minority counsel for all facets of the SSCI investigation into Russia's interference in the 2016 U.S. elections. At the NSA, she gained significant experience with legal issues relating to big data, including privacy and compliance programs, particularly within the telecommunications, technology and defense sectors of the economy. Over the course of her career at the NSA, April managed operations; oversaw a complex, multi-site compliance program; and served as part of the senior management team for the NSA's new technology development. Prior to her federal government service, April tried both criminal and civil cases, first as a public defender and later as a law firm litigator. She also served as assistant and acting general counsel of a private college prior to her federal service.

April is a regular commentator and contributor on national security, privacy, and cybersecurity issues. She has appeared on CNN, MSNBC and NewsOneNow. April's articles have been published in a wide range of publications, including the *Washington Post*, *The Atlantic*, *The Weekly Standard*, *Lawfare*, the American Bar Association's *SciTech Lawyer*, the *IAPP Privacy Advisor* and Law360. She has been quoted in *WIRED*, *Axios*, *Reuters*, and *The Hill*, among others.

RICHARD W. DOWNING, *Acting Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice*

Richard W. Downing has served as Acting Deputy Assistant Attorney General for the Criminal Division at the DOJ since September 2015. Downing previously served as Principal Deputy Chief of the Computer Crime and Intellectual Property Section. During his tenure, he supervised the prosecution of cybercrimes, oversaw policy and litigation of constitutional and statutory rules for the collection of electronic evidence, and supervised the development of international law enforcement cooperation related to cybercrime. Downing joined the DOJ in 1999. Prior to that, he was an Assistant District Attorney in Philadelphia for seven years. He graduated with a J.D. from Stanford Law School in 1992 and received a B.A. in political science, *summa cum laude*, from Yale University in 1989.

MARY ANNE FRANKS, *Professor of Law, University of Miami School of Law*

Professor Franks teaches criminal law, criminal procedure, First Amendment law, and Law, Policy, and Technology. She is also the President and Legislative & Tech Policy Director of the Cyber Civil Rights Initiative, a nonprofit organization dedicated to combating online abuse and discrimination.

In 2013, Professor Franks drafted the first model criminal statute on nonconsensual pornography (sometimes referred to as "revenge porn"), which has been used as the template for multiple state laws and for pending federal legislation on the issue. She also served as the reporter for the Uniform Law Commission's 2018 Uniform Civil Remedies for the Unauthorized Disclosure of Intimate Images Act. She regularly advises legislators and tech industry leaders, including Google, Facebook, Twitter, and Microsoft, on issues relating to online privacy, extortion, harassment, and threats.

Professor Franks is the author of *The Cult of the Constitution: Guns, Speech, and the Internet* (Stanford University Press, forthcoming 2019). Her legal scholarship has appeared in publications such as the Harvard Law Review, the California Law Review, and the UCLA Law Review. She has also authored numerous articles for the popular press, including THE ATLANTIC, THE GUARDIAN, and TIME MAGAZINE. Professor Franks has delivered more than a hundred lectures to a range of audiences in the U.S. and internationally, including law schools, domestic violence organizations, law firms, and tech companies.

Professor Franks holds a J.D. from Harvard Law School as well as doctorate and master's degrees from Oxford University, where she studied as a Rhodes Scholar. Before she began teaching at the University of Miami, Professor Franks was a Bigelow Fellow and Lecturer in Law at the University of Chicago Law School and taught social studies and philosophy at Harvard University. In 2013, she was a Visiting Professor at the University of Navarra in Pamplona, Spain.

MATTHEW GARDNER, *Of Counsel, Wiley Rein LLP*
Matt advises clients on a wide range of cybersecurity issues, including preparing for and responding to cyber incidents and interacting with regulators and law enforcement. He has extensive experience working with critical infrastructure companies to manage cyber risk, and he routinely advises clients on complicated issues involving the intersection of law and emerging technologies. Matt frequently helps clients prepare for and respond to network vulnerabilities, including working with the U.S. Departments of Justice (DOJ) and Homeland Security (DHS) to find creative solutions to challenging security issues.

HARLEY GEIGER, *Director of Public Policy, Rapid7*

Harley Geiger is Director of Public Policy at Rapid7, where he leads the company's public policy and government affairs activities on cybersecurity, digital trade, exports and encryption issues. Prior to working a Rapid7, Geiger was Advocacy Director at the Center for Democracy & Technology (CDT), where he worked on issues related to government surveillance, privacy and computer crime. Prior to that, Geiger was Senior Legislative Counsel for US Representative Zoe Lofgren of California, serving as lead staffer for technology and intellectual property issues. Geiger is an Attorney and is CIPP/US certified.

WILLIAM A. HALL, JR., *Senior Counsel, Computer Crime and Intellectual Property Section, U.S. Department of Justice*

Bill Hall specializes in the investigation and prosecution of computer crime cases, particularly those involving computer intrusions, fraud, and threats to national security. Prior to joining CCIPS, Bill served as Counsel on the Judiciary Committee of the U.S. Senate, where he specialized in crime and terrorism issues; as an Assistant U.S. Attorney in San Diego, California, where he handled computer, white collar, and child exploitation cases; as a Trial Attorney in the Child Exploitation and Obscenity Section of DOJ; and, as an Assistant District Attorney in Philadelphia, Pennsylvania. He also clerked for Judge Danny Boggs of the U.S. Court of Appeals for the Sixth Circuit. He is a graduate of Dartmouth College and Harvard Law School.

NATHAN JUDISH, *Senior Counsel, Computer Crime and Intellectual Property Section, U.S. Department of Justice*

Nathan Judish specializes in issues related to obtaining electronic evidence in criminal investigations, including the Fourth and Fifth Amendments, the Stored Communications Act, the Wiretap Act, and the Pen Register statute. His appellate litigation includes: the compelled decryption case *United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017); the cell-site simulator case *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016); and the historical cell phone location case *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013). He also assisted with drafting and defending the 2016 amendment to Rule 41 of the Federal Rules of Criminal Procedure for remote access search warrants in investigations involving Internet anonymizing technologies or botnets. Mr. Judish received a B.S. in Electrical Engineering and an A.B. in History from Washington University in St. Louis, an M.S. in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology, and a J.D., *magna cum laude*, from the Harvard Law School.

ANDREA LITTLE LIMBAGO, *Chief Social Scientist, Virtru*

Dr. Andrea Little Limbago is a computational social scientist specializing in the intersection of technology, national security, and society. She currently is the Chief Social Scientist at Virtru, an encryption and data privacy software company, where she researches and writes on the geopolitics of cybersecurity, global data protection and privacy trends, and usable security. Her writing has been featured in numerous outlets, including Politico, the Hill, Business Insider, War on the Rocks, and Forbes. Andrea frequently presents on a range of cybersecurity topics such as digital norms, attacker trends, computational propaganda, data protection, and workforce development. Andrea is also a Senior Fellow and Program Director for the Emerging Technologies Law and Policy Program at the National Security Institute at George Mason, and contributes to numerous security conference program review committees. She previously was the Chief Social Scientist at Endgame. Prior to that, Andrea taught in academia and was a technical lead at the Department of Defense, where she earned a top award for technical excellence. Andrea earned a PhD in Political Science from the University of Colorado at Boulder.

LOUISA MARION, *Trial Attorney, DOJ, CCIPS*

Louisa K. Marion is a Senior Counsel at the Computer Crime and Intellectual Property Section at the U.S. Department of Justice, where she prosecutes criminal cases, including cases involving online dark markets, cryptocurrency, computer hacking, identity theft, and online fraud. Louisa was one of the prosecutors who investigated and charged the founder and administrator of AlphaBay Market, and participated in the operation that dismantled the site in July 2017. Louisa also advises on legal questions relating to electronic evidence, cybercrime investigations and prosecutions, and virtual currency-related matters, and conducts training on these topics for U.S. and foreign law enforcement. She has a bachelor's degree from Stanford University and a law degree from the University of Michigan Law School.

PAUL OHM, *Professor of Law, Georgetown Law, Faculty Director of Center on Privacy and Technology.*

Paul Ohm specializes in information privacy, computer crime law, intellectual property, and criminal procedure. He teaches courses in all of these topics and more and he serves as a faculty director for the Center on Privacy and Technology at Georgetown.

In his work, Professor Ohm tries to build new interdisciplinary bridges between law and computer science. Much of his scholarship focuses on how evolving technology disrupts individual privacy. His article *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, has sparked an international debate about the need to reshape dramatically the way we regulate privacy. He is commonly cited and quoted by news organizations including the NEW YORK TIMES, WALL STREET JOURNAL, and NPR.

Professor Ohm began his academic career on the faculty of the University of Colorado Law School, and from 2012 to 2013, served as Senior Policy Advisor to the Federal Trade Commission. Before becoming a professor, he served as an Honors Program trial attorney in DOJ's Computer Crime and Intellectual Property Section. Before that, he clerked for Judge Betty Fletcher of the United States Court of Appeals for the Ninth Circuit and Judge Mariana Pfaelzer of the United States District Court for the Central District of California. He is a graduate of the UCLA School of Law.

Before attending law school, Professor Ohm worked for several years as a computer programmer and network systems administrator after earning undergraduate degrees in computer science and electrical engineering from Yale University. Today he continues to write thousands of lines of python and perl code each year. Professor Ohm blogs at Freedom to Tinker.

DAVI OTTENHEIMER, *President, flyingpenguin LLC*

Davi Ottenheimer, founder of flyingpenguin LLC, has more than 20 years' experience managing global security operations and assessments, including a decade of leading incident response and digital forensics.

He is co-author of the book *Securing the Virtual Environment: How to Defend the Enterprise Against Attack* and author of the book *The Realities of Securing Big Data*. He formerly was head of global security at BGI, the world's largest investment fund manager.

Prior to that, he was the dedicated paranoid at Yahoo! responsible for Connected Life, managing security for hundreds of millions of mobile, broadband and digital home products.

Ottenheimer received his postgraduate academic Master of Science degree in international history from the London School of Economics.

STEPHANIE PELL, *Assistant Professor and Cyber Ethics Fellow, West Point's Army Cyber Institute*

Stephanie Pell writes about privacy, surveillance and security law and policy, and is particularly interested in the tensions inherent in enabling traditional law enforcement efforts and making our communications networks more secure. Prior to joining the ACI faculty, Stephanie served as Counsel to the House Judiciary Committee, where she was lead counsel on Electronic Communications Privacy Act (ECPA) reform and PATRIOT Act reauthorization during the 111th Congress. Stephanie was also a federal prosecutor for over fourteen years, working as a Senior Counsel to the Deputy Attorney General, as a Counsel to the Assistant Attorney General of the National Security Division, and as an Assistant U.S. Attorney in the U.S. Attorney's Office for the Southern District of Florida. She was a lead prosecutor in *U.S. v. Jose Padilla* (American Citizen detained as an enemy combatant prior to criminal indictment and trial), for which she received the Attorney General's Exceptional Service Award, and in *U.S. v. Conor Claxton* (IRA operatives who purchased weapons in South Florida and smuggled them into Belfast, Northern Ireland during peace process negotiations). Stephanie received her undergraduate, master's and law degrees from the University of North Carolina at Chapel Hill.

MICHELLE RICHARDSON, *Director, Privacy & Data Project, Center for Democracy and Technology*

Michelle Richardson leads CDT's efforts to create a user-centered internet. Her team engages companies and government officials to create policies and technical solutions that protect individual privacy, empower users, and advance social justice.

Michelle has testified before Congress, advised government agencies, and frequently appears in national press such as THE WASHINGTON POST, THE NEW YORK TIMES, NPR, and POLITICO. Recognized by The Hill as one of the most influential nonprofits lobbyists in Washington, she has led left-right coalitions to defend privacy in the face of ever-expanding government authorities.

Before joining CDT in 2017, Michelle led the American Civil Liberties Union's preeminent legislative campaigns against overreaching surveillance programs for 10 years. She also served as a democratic counsel for the House Judiciary Committee where she worked on a range of anti-terrorism laws and policies. She received her B.A. from the University of Colorado and her J.D. from American University, Washington College of Law. She currently serves as a Senior Fellow at George Washington University's Center for Cyber and Homeland Security.

MICHAEL STAWASZ, *Deputy Chief for Computer Crime, U.S. Department of Justice*

Michael Stawasz is the Deputy Chief for Computer Crime for the US Department of Justice. Mick consults on every Computer Fraud and Abuse Act prosecution in the country as well as supervising the Cybersecurity Unit.

He has received back-to-back Attorney General's Awards, including the John Marshall Award, the Department's highest award for attorneys. He is a graduate of Dartmouth College and earned his Juris Doctorate from Georgetown University Law Center.

TRENT TEYEMA, *Senior VP and Chief Technology Officer, Parsons Corporation*

Trent Teyema drives Parsons' intellectual property protection and technology solutions through new research and development initiatives and technical engagements with customers. Mr. Teyema has spent more than two decades in the cybersecurity field, most recently serving as Chief Operating Officer and Chief of Cyber Readiness for the Federal Bureau of Investigation (FBI), and was twice appointed to roles in the White House. Mr. Teyema holds a master's degree in Forensic Science from George Washington University, as well as several technical certifications.

HEATHER WEST, *Senior Policy Manager, Americas Principal, Mozilla*

Heather West works on policy for the digital age at Mozilla, maker of the Firefox browser. At the intersection of public policy and technology, she is a policy-to-tech translator, product consultant and long-term Internet strategist.

She helped found the public policy team at CloudFlare (a website performance and security company), served as privacy and security issue expert for Google's policy team, and started her career working on privacy and identity management at the Center for Democracy and Technology.

She holds a dual B.A. in computer science and cognitive science from Wellesley College and is a Certified Information Privacy Professional (CIPP/US). She is recognized as a Christian Science Monitor Passcode Influencer and a member of the 2014 Forbes 30 Under 30 in Law and Policy.

Thank you for joining us today!

We value your feedback; please email
nationalsecurity@law.georgetown.edu
with your thoughts and comments on today’s program.