KEYNOTE SPEAKER

Richard Salgado
Director of Law Enforcement and Information Security, Google

Richard Salgado serves as Google's Director for information security and law enforcement matters. Prior to joining Google, Richard was with Yahoo!, focusing on international security and compliance work. He also served as senior counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. As a federal prosecutor, Richard specialized in investigating and prosecuting computer network cases, such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other technology-driven privacy crimes. In 2005, Richard joined Stanford Law School as a legal lecturer on computer crime and on Internet business legal and policy issues; he previously served as an adjunct law professor at Georgetown University Law Center and George Mason Law School and as a faculty member of the National Judicial College. Richard is a senior instructor with the SANS Institute, teaching on the legal issues in computer forensics and network investigations. He regularly speaks on the legal and policy implications of searching and seizing computers and electronic evidence, emerging surveillance technologies, digital evidence, and related criminal conduct. Richard graduated magna cum laude from the University of New Mexico and in 1989 received his JD from Yale Law School.

DATA MANAGEMENT PRACTICES PANEL

Harriet Pearson
Cybersecurity Partner, Hogan Lovells

Clients value Harriet Pearson’s extensive experience in every aspect of cybersecurity & privacy law, policy, and compliance. Drawing on her in house experience as IBM’s first and longstanding global chief privacy officer and security counsel, since joining Hogan Lovells in 2012 Harriet has been advising companies and boards on cyber and data risk governance, global regulatory compliance, and breach investigations and enforcement.

Harriet was named North America’s 2016 “Legal Innovator of the Year” by the Financial Times; a Cybersecurity and Privacy Trailblazer by the National Law Journal; and one of the 500 “Leading Lawyers in America” by LawDragon. Harriet leads Hogan Lovells’ global multi-disciplinary cybersecurity practice and she co-chairs and co-founded the Georgetown Cybersecurity Law Institute, now in its sixth year.

She has led high-profile reviews and investigations for, among others, Bloomberg LP, The Home Depot (after the company's large payment card breach in 2014), Uber, a leading global insurance and financial services company, a top-5 defense and government contractor, a major U.S. credit bureau, and a leading global technology company. In addition to her cybersecurity work, she is currently working with a wide range of companies on designing and implementing global and EU GDPR-focused privacy compliance programs.

Daniel Crowley
Trust and Safety Manager, Quizlet

Daniel Crowley manages Quizlet's Trust & Safety efforts, including oversight of privacy, security, content policy, safety, compliance, and more. He is dedicated to ensuring a safe environment for all of Quizlet's users, including K-12, college students, post-grads and lifelong learners. Prior to joining Quizlet, Dan spent several years in both Facebook and Google's privacy programs, where he helped develop internal policy development programs and led privacy-by-design efforts across a broad range of consumer and business products. At Facebook, his portfolio included live video and media products, civic engagement efforts, and News Feed. At Google, he focused on personalization and machine learning, search, and location. Earlier in his career, Dan worked at Google as a legal assistant at Google handling law enforcement compliance, including child protection cases and has previously presented at the Crimes Against Children Conference, SXSWedu, and various privacy bootcamps and summits across the United States. Dan received his BA in Government from Claremont McKenna College and has earned CIPP/US, CIPP/Europe, and CIPM certifications from the International Association of Privacy Professionals.

Eric Talley
Professor, Columbia Law School

Eric Talley is the Isidor and Seville Sulzbacher Professor of Law and Co-Director, Millstein Center for Global Markets and Corporate Ownership. He is an expert in the intersection of corporate law, governance, and finance, and he teaches/researches in areas that include corporate law and finance, mergers and acquisitions, quantitative methods, machine learning, contract and commercial law, game theory, and economic analysis of law.

(cont. on next page)
Talley has held permanent or visiting appointments at the University of California at Berkeley, University of Southern California, Caltech, University of Chicago; Harvard University; Georgetown University, RAND Graduate School, and Stanford University. He has also taught short courses at the University of New South Wales; the University of Sydney; University of San Diego; Tel Aviv University, the Interdisciplinary Center; University of Zurich; University of Amsterdam; and University of Miami. In 2017, Talley was chosen by Columbia Law School's graduating class to receive the Willis L.M. Reese Prize for Excellence in Teaching.

He is current Chair of the board of directors of the Society for Empirical Legal Studies (SELS) and was the SELS co-president in 2013–2014. He also serves on the board of directors of the American Law and Economics Association (ALEA). Talley is a frequent commentator in the national media, and he speaks regularly to corporate boards and regulators on issues pertaining to fiduciary duties, governance, and finance.

Talley holds a J.D. from Stanford University, where he was articles editor for the Stanford Law Review; a Ph.D. in economics from Stanford University; and B.A. degrees in economics and political science from the University of California, San Diego. He is a native of Los Alamos, N.M.

Tyler Newby is a partner in the Litigation Group at Fenwick & West LLP, and co-chairs the firm’s Privacy and Data Security practice. His practice focuses on privacy and data security litigation, federal and state regulatory investigations and counseling for high technology clients ranging from early-stage startups to mature public companies. From 2007 through 2010, Tyler was a federal prosecutor with the U.S. Department of Justice in Washington, D.C. where he was a Trial Attorney in the Criminal Division’s Computer Crime and Intellectual Property Section, and a Special Assistant United States Attorney in the Cyber Division of the U.S. Attorney’s Office for the Eastern District of Virginia.

Mr. Newby graduated from Stanford Law School in 1999, where he was a Notes Editor of the Stanford Law Review.

Todd Hinnen is a partner with Perkins Coie’s Privacy & Security practice. He counsels clients and represents them in litigation regarding privacy, data security, compliance with law enforcement and national security issues. He works closely with the Department of Justice and the Intelligence Community.

Prior to joining Perkins Coie, Todd was the Acting Assistant Attorney General for National Security at the U.S. Department of Justice (DOJ). While in office, he led an office of 320 attorneys responsible for overseeing the DOJ’s nationwide counterterrorism, counterespionage and export control programs. In that capacity, he represented the United States before the Foreign Intelligence Surveillance (FISA) Court and on the Committee on Foreign Investment in the United States (CFIUS); supervised oversight and compliance programs at law enforcement, intelligence and national security agencies; and testified before Congress on numerous occasions in both open and classified hearings.

Eran Kahana is a cybersecurity and intellectual property lawyer as well as a Fellow at Stanford Law School. He counsels clients on a wide variety of matters related to cybersecurity, technology law, trademarks, patents, and copyright issues. Eran also serves in a variety of cybersecurity thought-leadership roles and works closely with the FBI, Department of Justice, Secret Service, and colleagues from the private and academic sectors to set, promote, and sustain cybersecurity best practices. Eran serves as both general counsel and as a director on the Executive Board of InfraGard (MN Chapter).

At Stanford Law School, Eran writes and lectures on the intersect between law and artificial intelligence and is a frequent speaker at Stanford’s annual E-Commerce Best Practices Conference. He has been interviewed on cybersecurity, privacy, and technology law at Bloomberg Law, BBC, KABC radio, Minnesota Public Radio, Twin Cities Business magazine, Star Tribune, TheStreet.com, and Stanford University Radio, KZSU FM.
Nathaniel Gleicher is an engineer and a lawyer, and works at the intersection of technology, policy, and law. He has taught computer programming, built and secured computer networks, prosecuted cybercrime at the U.S. Department of Justice, and served as Director for Cybersecurity Policy at the National Security Council (NSC) in the White House. At the NSC, he developed U.S. government policy on key technology and cybersecurity challenges, including encryption, cyber deterrence, internet governance, and network security. Since leaving government, Nathaniel served as head of cybersecurity strategy at Illumio, and is currently the Head of Cybersecurity Policy at Facebook.

Chris Cook is an attorney at the U.S. Department of Justice, National Security Division and a reserve officer with the U.S. Navy Judge Advocate General’s (JAG) Corps. Prior to joining the Justice Department, Cook practiced intelligence, cybersecurity and information assurance law with the Office of General Counsel at the National Security Agency.

Beth George is Of Counsel in the San Francisco office of Wilson Sonsini Goodrich & Rosati, where her practice focuses on the representation of companies in complex cybersecurity and data security matters, including providing advice on legal challenges faced by companies when preparing for and responding to cybersecurity breaches.

Beth advises clients on internal and government investigations, privacy and compliance, and responding to law enforcement requests for data. In addition, she represents clients in other national security-related areas, including applications before the Committee on Foreign Investment in the United States (CFIUS) and for foreign acquisition of licenses issued by the Federal Communications Commission (FCC). Beth currently is a lecturer on surveillance law and technology at the UC Berkeley School of Law, and she serves as a senior adjunct fellow for the New York University School of Law's Center for Law and Security and as an affiliate at Stanford University’s Center for International Security and Cooperation (CISAC).

Jeff Rabkin has tried 18 cases to verdict in federal and state courts, and has the rare combination of working on civil and criminal disputes and corporate executive experience as the Vice President of a cybercrime investigations consultant. Now a leading practitioner in the fields of cybersecurity and privacy, as well as on legal issues and regulatory risk arising from disruptive technology, Jeff represents businesses in all types of government investigations, regulatory proceedings, and private disputes, and also advises in-house counsel, corporate executives, and boards of directors on these issues.

Jesse Sowell is currently a Postdoctoral Cybersecurity Fellow at Stanford’s Center for International Security and Cooperation (CISAC). Broadly, Jesse’s research focuses on the non-state institutions that ensures the Internet stays glued together in a secure and stable manner. This work started with studies of how operational communities share information necessary to solve operational and security incidents that often span firm and jurisdictional boundaries. Historically, these actors have served as the stewards of the Internet’s infrastructure. Increasingly, the social, political, and economic magnitude of cybersecurity incidents require the capabilities of both operational communities and state actors. Jesse’s ongoing work explores the operational-policy interface between closed security communities (trust groups) and state actors, in particular law enforcement and national security.

(continues on next page)
Jesse’s research interests include bridging the gaps between private transnational security regimes and conventional government authorities, the commodification of malware value networks, credible knowledge assessment of science and technology policy, the economics of IoT security, and the growing tension between Internet privacy and security efforts. At M3AAWG, Jesse serves as a Senior Advisor and Vice-Chair of the Growth and Development Committee directing M3AAWG’s outreach efforts. He is also serves as the co-chair of the IoT SIG. Jesse has a background in computer science, criminal justice, and technology and policy; he holds a PhD in Technology, Management, and Policy from MIT’s Engineering Systems Division.

Cryptography and Ethics Panel

Riana Pfefferkorn
Cryptography Fellow, Stanford Center for Internet and Society

Riana Pfefferkorn is the Cryptography Fellow at the Stanford Center for Internet and Society. Her work, made possible through funding from the Stanford Cyber Initiative, focuses on investigating and analyzing the U.S. government's policy and practices for forcing decryption and/or influencing crypto-related design of online platforms and services, devices, and products, both via technical means and through the courts and legislatures. Riana also researches the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests.

Prior to joining Stanford, Riana was an associate in the Internet Strategy & Litigation group at the law firm of Wilson Sonsini Goodrich & Rosati, where she worked on litigation and counseling matters involving online privacy, Internet intermediary liability, consumer protection, copyright, trademark, and trade secrets and was actively involved in the firm's pro bono program. Before that, Riana clerked for the Honorable Bruce J. McGiverin of the U.S. District Court for the District of Puerto Rico. She also interned during law school for the Honorable Stephen Reinhardt of the U.S. Court of Appeals for the Ninth Circuit. Riana earned her law degree from the University of Washington School of Law and her undergraduate degree from Whitman College.

Paul Kocher
Entrepreneur and Cryptography Researcher

Paul Kocher is interested the algorithms, hardware, and software that underpin the security of modern systems. He founded Cryptography Research in 1995 and led the company through its acquisition by Rambus in 2011, where he served as SVP/Chief Scientist until 2017. His technical work includes co-discovering the recently disclosed Spectre vulnerability, co-authoring the SSL/TLS 3.0 standards, architecting numerous hardware security cores, and discovering Differential Power Analysis. He is currently an independent researcher and advisor/investor for security start-ups. Paul is a member of the National Academy of Engineering and serves on the National Academies’ Forum on Cyber Resilience.

Attribution and Deterrence of Nation States in Cyberspace

Christopher Painter
Former Coordinator for Cyber Issues, U.S. State Department

Chris Painter is a globally recognized leader and expert on cybersecurity, cyber policy, Cyber Diplomacy and combating cybercrime. He has been on the vanguard of US and international cyber issues for over twenty-five years—first as a leading federal prosecutor of some of the most high-profile cybercrime cases in the country, then as a senior official at the Department of Justice, the FBI, the National Security Council and finally as the world’s first top cyber diplomat at the State Department. He has helped drive, initiated or been involved in virtually every major US cyber policy for over a decade and has created innovative new organizations and approaches to deal with threats and take advantage of opportunities in cyberspace. Among other things, he currently serves as a Commissioner on the Global Commission for the Stability of Cyberspace, a member of the Board of Directors for the Center for Internet Security and has been named the Bartels World Affairs Fellow for 2017-18 by Cornell University.

In his most recent government role as the nation’s top cyber diplomat, Mr. Painter coordinated and led the United States’ diplomatic efforts to advance an open, interoperable, secure and reliable Internet and information infrastructure and advised the Secretary and Deputy Secretary of State on these emerging issues.

From 2009-2011, Mr. Painter served in the White House as the first Senior Director for Cyber Policy and Acting Cyber Coordinator in the National Security Council. Mr. Painter began his federal career as an Assistant US Attorney in Los Angeles. He subsequently helped lead the case and policy efforts of the Computer Crime and Intellectual Property Section in the US Department of Justice. He also served, for a short time, as Deputy Assistant Director of the FBI's Cyber Division focusing on a range of national security, cybercrime, international and industry issues. Prior to joining the US government, Mr. Painter was an attorney at the law firm of Arnold and Porter where he specialized in securities litigation, communications law, international trade and pro bono matters. He is a graduate of Stanford Law School and Cornell University and clerked for US Circuit Judge Betty Fletcher.

CRYPTOGRAPHY AND ETHICS PANEL

Riana Pfefferkorn
Cryptography Fellow, Stanford Center for Internet and Society

Riana Pfefferkorn is the Cryptography Fellow at the Stanford Center for Internet and Society. Her work, made possible through funding from the Stanford Cyber Initiative, focuses on investigating and analyzing the U.S. government's policy and practices for forcing decryption and/or influencing crypto-related design of online platforms and services, devices, and products, both via technical means and through the courts and legislatures. Riana also researches the benefits and detriments of strong encryption on free expression, political engagement, economic development, and other public interests.

Prior to joining Stanford, Riana was an associate in the Internet Strategy & Litigation group at the law firm of Wilson Sonsini Goodrich & Rosati, where she worked on litigation and counseling matters involving online privacy, Internet intermediary liability, consumer protection, copyright, trademark, and trade secrets and was actively involved in the firm's pro bono program. Before that, Riana clerked for the Honorable Bruce J. McGiverin of the U.S. District Court for the District of Puerto Rico. She also interned during law school for the Honorable Stephen Reinhardt of the U.S. Court of Appeals for the Ninth Circuit. Riana earned her law degree from the University of Washington School of Law and her undergraduate degree from Whitman College.

Paul Kocher
Entrepreneur and Cryptography Researcher

Paul Kocher is interested the algorithms, hardware, and software that underpin the security of modern systems. He founded Cryptography Research in 1995 and led the company through its acquisition by Rambus in 2011, where he served as SVP/Chief Scientist until 2017. His technical work includes co-discovering the recently disclosed Spectre vulnerability, co-authoring the SSL/TLS 3.0 standards, architecting numerous hardware security cores, and discovering Differential Power Analysis. He is currently an independent researcher and advisor/investor for security start-ups. Paul is a member of the National Academy of Engineering and serves on the National Academies’ Forum on Cyber Resilience.
Nate Cardozo is a senior staff attorney on the Electronic Frontier Foundation’s digital civil liberties team. He works on EFF’s “Who Has Your Back?” report and Coders’ Rights Project. In addition, Cardozo has projects involving cryptography and the law, automotive privacy, government transparency, and Freedom of Information Act litigation. Cardozo received his J.D. from the University of California, Hastings where he has taught first-year legal writing and moot court.

Robyn Greene is the policy counsel and government affairs lead for the Open Technology Institute at New America specializing in issues concerning surveillance and cybersecurity. She helps to research and develop policies to protect individuals’ privacy, secure the internet, and fuel the development of and access to emerging technologies. Prior to joining the Open Technology Institute, Greene worked at the American Civil Liberties Union's Washington Legislative Office, where she focused on legislation and administration policies concerning surveillance, cybersecurity, government secrecy, and federal law enforcement oversight.

Dr. Dan Boneh is a Professor of Computer Science at Stanford University where he heads the applied cryptography group and co-directs the computer security lab. Dr. Boneh’s research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, security for mobile devices, web security, and cryptanalysis.

He is the author of over a 150 publications in the field and is a recipient of the 2014 ACM prize, the 2013 Godel prize, the RSA award in mathematics, and six best paper awards. In 2016 Dr. Boneh was elected to the National Academy of Engineering.

THE FUTURE OF CYBERSECURITY PANEL

Matt Long is General Counsel of Palantir and leads the company’s “Legal Ninja” team responsible for worldwide legal, contracting, compliance and privacy engineering. Matt joined Palantir’s Business Development team in 2009 as the company’s first lawyer and oversaw growth of the legal team to over 60 professionals, including 35 lawyers. Prior to Palantir, Matt was an associate at Quinn Emanuel.

Jeff Kosseff is an Assistant Professor of Cybersecurity Law at the United States Naval Academy. He is the author of Cybersecurity Law, a textbook published by Wiley in 2017. He is the author of the forthcoming book, *The Twenty-Six Words That Created the Internet*, a history of Section 230 of the Communications Decency Act that will be published next year by Cornell University Press. He clerked for Judge Milan D. Smith, Jr. of the U.S. Court of Appeals for the Ninth Circuit and for Judge Leonie M. Brinkema of the U.S. District Court for the Eastern District of Virginia. Kosseff is a graduate of Georgetown University Law Center and the University of Michigan. Before becoming a lawyer, he was a journalist for The Oregonian and was a finalist for the Pulitzer Prize for national reporting.

Olga Mack is a technology strategist who enjoys advising her clients to success and growth. Currently Vice President of Strategy at Quantstamp and former General Counsel at ClearSlide. She previously worked at Zoosk, Visa Inc., Pacific Art League of Palo Alto, and Wilson Sonsini Goodrich & Rosati. She is a passionate advocate for women and founded the WomenServeOnBoards.com movement.

@OlgaVMack
Samir Jain has more than 20 years of experience at high levels of government and in private practice working on legal and policy issues involving cybersecurity, privacy, national security, communications, and internet law. He is a Partner at Jones Day in the Cybersecurity, Privacy & Data Protection group. Previously, he was Senior Director for Cybersecurity Policy for the National Security Council at The White House in the Obama Administration. He led the teams responsible for cyber incident responses and review of cyber operations, directed evaluation of legislative proposals concerning reform of the Electronic Communications Privacy Act and foreign law enforcement access to communications content, helped lead an interagency group on encryption policy, and worked with international counterparts, including heading a delegation to India and gaining acceptance of international cyber norms.

He also served as Associate Deputy Attorney General at the Department of Justice, where his responsibilities included overseeing the development of proposals to modernize cybercrime laws, leading the development of the policy for law enforcement use of cell site simulators, and representing the DOJ in White House cybersecurity meetings and international negotiations, such as China's agreement not to engage in cyber-enabled IP theft for commercial gain.

Previously, Samir was a partner at a leading international law firm, where his practice involved litigation and counseling on privacy, data security, and law enforcement issues; representing clients in proceedings and investigations before the FTC and FCC; and litigating internet law issues of first impression.

Amelia Vance is the Director of the Education Privacy Project and a Policy Counsel at the Future of Privacy Forum. She leads FPF’s work to ensure the responsible use of student data and education technology in schools, convening school districts, state and federal policymakers, companies, and privacy advocates to develop and share best practices and resources. Prior to FPF, Amelia was the Director of the Education Data & Technology Project at NASBE. Amelia is a member of the International Association of Privacy Professionals and the Virginia State Bar.

Phil Malone is Professor of Law at Stanford Law School and the director of the school’s Juelsgaard Intellectual Property and Innovation Clinic. His current work and scholarship focuses on understanding and promoting sound innovation policy, including the relationship between innovation and intellectual property, security, privacy, and other laws and regulations. Professor Malone was previously a Clinical Professor of Law at Harvard Law School and the director of the Cyberlaw Clinic at the Berkman Center for Internet & Society. In addition to his clinic work, he has taught classes on cyber/computer crime and technology policy and litigation.

Prior to joining the academy, Professor Malone was a senior attorney for over 20 years with the Antitrust Division of the U.S. Department of Justice, where he directed numerous civil and criminal antitrust investigations and litigated a number of major antitrust trials. Much of his Antitrust Division experience focused on high-technology industries, the Internet and computer software and hardware, including the antitrust trial and appeal against Microsoft (U.S. v. Microsoft Corp.) and the antitrust trial challenging Oracle’s acquisition of PeopleSoft.

Aaron Ghiradelli is a Visiting Professor at Loyola Law School, Los Angeles. His scholarship focuses on the intersection between law and technology, in particular with reference to the evolution of blockchain technologies and the impact that these technologies have on current legal principles.