

Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs

Committee

Fred H. Cate

Chair

Fred H. Cate is Vice President for Research, Distinguished Professor, C. Ben Dutton Professor of Law, and Adjunct Professor of Informatics and Computing at Indiana University. He served as the founding director of IU's Center for Applied Cybersecurity Research, a National Center of Academic Excellence in Information Assurance Research and Information Assurance Education, from 2003 to 2014, where he is now a senior fellow. Professor Cate is a member of the National Academies' Forum on Cyber Resilience, the Department of Homeland Security's Cybersecurity Subcommittee, the National Security Agency's Privacy and Civil Liberties Panel, the OECD's Panel of Experts on Health Information Infrastructure, Intel's Privacy and Security External Advisory Board, and the board of directors of The Privacy Projects. He serves as a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP. Previously, Professor Cate served as a member of the National Academies' Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention, counsel to the Department of Defense Technology and Privacy Advisory Committee, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security and Microsoft's Trustworthy Computing Academic Advisory Board. He chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. He has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups. The author of more than 150 articles and books, he served as the privacy editor for the Institute of Electrical and Electronic Engineers' Security & Privacy and is one of the founding editors of the Oxford University Press journal, International Data Privacy Law. Professor Cate attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. A former Senator and President of the Phi Beta Kappa Society, he is a fellow of Phi Beta Kappa and the American Bar Foundation, and an elected member of the Council on Foreign Relations and the American Law Institute.

Dan Boneh

Member

Dan Boneh (NAE) is a professor of computer science and heads the applied cryptography group at Stanford University, where he has been on the faculty since 1997. Boneh's research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, web security, security for mobile devices, digital copyright protection, and cryptanalysis. He is the author of over a hundred publications in the field and a recipient of the Packard Award, the Alfred P. Sloan Award, and the RSA award in mathematics. Last year Boneh received the Ishii award for industry education innovation. Professor Boneh received his Ph.D in computer science from Princeton University.

Frederick R. Chang

Member

Frederick Chang (NAE) is the director of the Darwin Deason Institute for Cyber Security, the Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, and professor in the Department of Computer Science and Engineering in the Lyle School of Engineering at Southern Methodist University. He is also a senior fellow in the John Goodwin Tower Center for Political Studies at SMU's Dedman College and a distinguished scholar in the Robert S. Strauss Center for International Security and Law, at the University of Texas at Austin. He is the former director of research at the National Security Agency. Dr. Chang received his B.A. from the University of California, San Diego and his M.A. and Ph.D. from the University of Oregon. He also completed the senior executive program at the Sloan School of Management at the Massachusetts Institute of Technology. He has served as a member of the Commission on Cyber Security for the 44th Presidency and as a member of the Computer Science and Technology Board of the National Academies of Sciences, Engineering, and Medicine. He has also served as a member of the Academies Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection. He has been awarded the NSA Director's Distinguished Service Medal and was the 2014 Information Security Magazine "Security 7" award-winner for education.

Scott Charney

Member

Scott Charney is corporate vice President for Microsoft's Trustworthy Computing Group, where he helps ensure the company's products and services comply with Microsoft's security engineering policies. Charney also works with governments, partners, and customers on security issues such as critical infrastructure protection, cybersecurity norms, encryption policy, and IoT security. Before joining Microsoft in 2002, he led PricewaterhouseCoopers' Cybercrime Prevention and Response Practice and served as chief of the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. He serves on the U.S. President's National Security and Telecommunications Advisory Committee and was a co-chair of the Center for Strategic and International Studies nonpartisan Commission on Cybersecurity. He holds a law degree with honors from Syracuse University in Syracuse, N.Y., and bachelor's degrees in history and English from the State University of New York in Binghamton.

Shafira Goldwasser

Member

Shafira Goldwasser (NAS, NAE) is the RSA Professor of Electrical Engineering and Computer Science at MIT, a co-leader of the cryptography and information security group and a member of the complexity theory group within the Theory of Computation Group and the Computer Science and Artificial Intelligence Laboratory. In 1992 she began a parallel career as a Professor of Computer Science and Applied Mathematics at the Weizmann Institute of Science in Israel. Goldwasser has made fundamental contributions to cryptography, computational complexity, computational number theory and probabilistic algorithms. She was a recipient of the first ACM SIGACT Gödel Prize for outstanding papers in theoretical computer science in 1993 and co-recipient of the Turing Award in 2012. She received a B.S. in mathematics from Carnegie Mellon University (1979) and M.S. (1981) and Ph.D. (1984) in electrical engineering and computer science from the University of California, Berkeley.

David A. Hoffman

Member

David A. Hoffman is director of security policy and global privacy Officer at Intel Corporation, in which capacity he oversees Intel's privacy activities and security policy engagements. Mr. Hoffman joined Intel in 1998 as Intel's eBusiness attorney to manage the team providing legal support for Intel's Chief Information Officer. In 1999, he founded Intel's Privacy Team, and in 2000 was appointed Group Counsel of eBusiness and Director of Privacy. In 2005, Mr. Hoffman moved to Munich, Germany, as group counsel in the Intel European Legal Department, while leading Intel's Worldwide Privacy and Security Policy Team. Mr. Hoffman served on the U.S. Federal Trade Commission's Online Access and Security Advisory Committee. Mr. Hoffman served on the TRUSTe board of directors from 2000-2006, where he was Chair of the Compliance Committee of the Board. Mr. Hoffman was a member of the U.S. Federal Trade Commission's Online Access and Security Committee and the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Mr. Hoffman has lectured on privacy and security law at schools in the U.S., Europe, Japan and China. He received a J.D. from Duke University School of Law and an A.B. from Hamilton College.

Seny Kamara

Member

Seny Kamara is an associate professor of computer science at Brown University. He was previously a researcher in the Cryptography Group at Microsoft Research. Kamara's research interests are in cryptography and security with a focus on privacy issues in surveillance, cloud computing and databases. In 2016, he was named as a Dukakis Fellow by Boston Global Forum. In 2006, he was a research fellow at the UCLA Institute for Pure and Applied Mathematics. In 2012, Kamara chaired the ACM Cloud Computing Security Workshop. In 2015, he founded the Workshop on Surveillance and Technology. He received his Ph.D. in computer science from Johns Hopkins University.

David Kris

Member

David Kris is a founder of Culper Partners LLC, a business consulting firm specializing in national security issues. Prior to forming Culper in 2017, Kris was for six years the General Counsel of Intellectual Ventures, a privately held invention investment company. He was also the Deputy General Counsel and Chief Compliance officer of Time Warner, Inc., the network and media company, where he worked from 2003 to 2009. In government, Kris was the Presidentially-appointed and Senate-confirmed head of the Department of Justice's National Security Division (2009-2011); a senior advisor to Republican and Democratic Attorneys General and Deputy Attorneys General (2000-2003); and a federal prosecutor (1992-2000). He currently advises two elements of the U.S. Intelligence Community and serves as an amicus curiae to the two Foreign Intelligence Surveillance Courts. Kris is co-author of the treatise, *National Security Investigations and Prosecutions*, as well as the author of several other articles and blog posts. He is a Director and Contributing Editor of the Lawfare website, adjunct professor at the University of Washington Law School, and a University Affiliate at Georgetown University. He is a recipient of the National Intelligence Superior Service Medal, the Office of the Secretary of Defense Medal for Exceptional Public Service, the CIA Agency Seal Medal, the Department of Justice Edmund J. Randolph Award, and on two occasions the Attorney General's Award for Exceptional Service. He is a 1988 graduate of Haverford College and a 1991 graduate of Harvard Law School, and a former law clerk to Judge Stephen S. Trott of the U.S. Court of Appeals for the Ninth Circuit.

Susan Landau

Member

Susan Landau is Bridge Professor in the Fletcher School of Law and Diplomacy and the School of Engineering, Department of Computer Science, Tufts University and Visiting Professor of Computer Science, University College London. Landau works at the intersection of cybersecurity, national security, law, and policy. Her new book, *"Listening In: Cybersecurity in an Insecure Age,"* was published by Yale University Press. Landau has testified before Congress and frequently briefed US and European policymakers on encryption, surveillance, and cybersecurity issues. Landau has been a Senior Staff Privacy Analyst at Google, a Distinguished Engineer at Sun Microsystems, and a faculty member at Worcester Polytechnic Institute, the University of Massachusetts Amherst and Wesleyan University. She is a member of the Cybersecurity Hall of Fame, a fellow of the American Association for the Advancement of Science and of the Association for Computing Machinery.

Steven B. Lipner

Member

Steven B. Lipner is an independent consultant who recently retired as Partner Director of Software Security in Trustworthy Computing Security at Microsoft, where was responsible for programs that provide improved product security for Microsoft customers. Lipner led Microsoft's Security Development Lifecycle (SDL) team and was responsible for the definition, tools development and company-wide execution of Microsoft's internal SDL process and for tools and programs that make the SDL available to organizations beyond Microsoft. Lipner was also responsible for Microsoft's corporate strategies and policies for supply chain security and for strategies related to government security evaluation of Microsoft products. He also served as the Microsoft member of the board of SAFECode, a nonprofit organization focused on software assurance. He has served on several Computer Science and Telecommunications Board study committees and is currently a member of the Academies Forum on Cyber Resilience. He has been working in the field of computer and network security since late 1970s. He received an S.B. and S.M. in civil engineering from MIT.

Richard Littlehale

Member

Richard Littlehale is special agent in charge of the Tennessee Bureau of Investigation's Criminal Investigation Division, which includes TBI's electronic surveillance, digital forensics, online child exploitation, and cyber investigation functions. Littlehale has testified as an expert witness in the law enforcement use of communications records in numerous homicide and violent crime trials. Littlehale is an attorney, and serves as one of TBI's primary constitutional law and criminal procedure trainers. Littlehale has provided instruction to law enforcement officers at all levels of government in techniques for obtaining and using communications evidence in support of criminal investigations, and is active in national groups of law enforcement technical and electronic surveillance specialists, including the National Technical Investigators Association and the FBI Law Enforcement Technical Forum. Littlehale serves as a subject matter expert on electronic surveillance for the Association of State Criminal Investigative Agencies and the International Association of Chiefs of Police. In that capacity, he represents the law enforcement community's interest in lawful access to communications evidence at the national level before Congress and other groups. Littlehale received his bachelor's degree in 1992 from Bowdoin College in Brunswick, Maine, and his law degree in 1995 from Vanderbilt Law School in Nashville, Tennessee.

Kate Martin

Member

Kate Martin is currently a senior fellow at the Center for American Progress where she works on issues at the intersection of national security, civil liberties, and human rights. The New York Times' Taking Note blog described her as "an expert on surveillance and detention, and a leading advocate for the rule of law in the so-called 'war on terror.'" Before coming to American Progress, Martin served as director of the Center for National Security Studies for more than 20 years. She frequently testifies before Congress on national security and civil liberties issues. She is also a frequent commentator in the national media and has written extensively on these issues for the past 25 years. At the Center for National Security Studies, Martin brought lawsuits that challenged government deprivations of civil liberties. She has taught national security law and served as general counsel to the National Security Archive. Martin is a graduate of the University of Virginia School of Law and Pomona College. Before joining the public interest world, she served as a partner at the law firm of Nussbaum, Owen & Webster.

Harvey Rishikof

Member

Harvey Rishikof is a senior counsel in Crowell & Moring's Privacy & Cybersecurity and Government Contracts groups in Washington, D.C. His practice focuses on national security, cybersecurity, government contracts, civil and military courts, terrorism, international law, civil liberties, and the U.S. Constitution. At the leading edge of many of the interactions between the legal community and the federal government and corporations, Harvey is routinely called upon to represent the legal community at meetings and forums on national security, cybersecurity, and terrorism. Prior to joining the firm, Harvey was most recently the dean of faculty, National War College at the National Defense University, Washington, D.C. He currently serves as an outside director to CBI, Baton Rouge, LA, chairing the company's Government Security Committee - CFIUS. Harvey is also the chair of the American Bar Association Advisory Standing Committee on Law and National Security, co-chair with Judy Miller of the ABA National Taskforce on Cyber and the law, and a lifetime member of the American Law Institute and the Council on Foreign Relations. Over his career, Harvey has been a member of Hale and Dorr and has held multiple positions in government focused on national and cyber security investigations. He most recently served as senior policy advisor to the National Counterintelligence Executive (NCIX), the agency responsible for counterintelligence and insider threat management across the federal government. He has also served at the FBI as a legal counsel to the deputy director of the FBI focusing on national security and terrorism and served as liaison to the Office of the Attorney General at the Department of Justice. Prior to serving as dean, he was a professor of National Security Law at the National War College and dean of Roger Williams University School of Law. Until recently, Harvey also had a joint appointment as professor of law at Drexel University teaching courses in national security and cyber law.

Peter J. Weinberger

Member

Peter Weinberger works as a software engineer for Google in New York, where he works on software design and implementation, and as technical consultant on some privacy-related projects. After teaching mathematics at the University of Michigan in Ann Arbor he moved to Bell Laboratories. At Bell Labs he worked on Unix, and did research on topics including operating systems, compilers, and security. He then moved into research management, ending up as Information Sciences Research Vice President, responsible for computer science research, math and statistics, and speech. He's also a co-author of The Awk Programming Language.) After Lucent and AT&T split apart, he moved to Renaissance Technologies, a technical trading hedge fund, as Head of Technology, was responsible for computing and security. Weinberger has a Ph.D. in mathematics (number theory) from the University of California at Berkeley.