Susan Landau

Bridge Professor
Fletcher School of Law & Diplomacy and School of Engineering, Department of Computer Science
160 Packard Avenue
Tufts University
Medford, MA 02155
617-627-4792
susan.landau@tufts.edu
https://privacyink.org

EDUCATION

1983 Ph.D., MIT.

1979 M.S., Cornell University.

1976 B.A., Princeton University.

1972 Bronx High School of Science.

EMPLOYMENT

2017-present Bridge Professor in the Fletcher School of Law & Diplomacy and the School of Engineering, Department of Computer Science, Tufts University.

2015-present Visiting Professor, Department of Computer Science, University College London.

2014-2017 Professor of Cybersecurity Policy, Department of Social Science and Policy Studies; 2016-2017, Professor of Computer Science, Worcester Polytechnic Institute.

2013-2014 Senior Staff Privacy Analyst, Google.

2011-2012 Visiting Scholar, Department of Computer Science, Harvard University.
(Visiting Lecturer: taught freshman seminar on privacy, spring 2012.)

2010-2011 Fellow, Radcliffe Institute for Advanced Study, Harvard University.

2005-2010 Distinguished Engineer, Sun Microsystems Laboratories, Burlington, Massachusetts.

1999-2005 Senior Staff Engineer, Sun Microsystems Laboratories, Burlington, Massachusetts.

1991-1999 Research Associate Professor, Computer Science Department, University of Massachusetts, Amherst (1995-1996, Visiting Associate Professor, Cornell University).

1989-1991 Visiting Assistant Professor, Computer Science Department, University of Massachusetts, Amherst (on leave from Wesleyan University).

1983 - 1991 Assistant Professor of Computer Science, Math Dept., Wesleyan University (Fall 1988, post-doctoral fellow, Mathematics Dept., Yale University; Fall 1987, visiting assistant professor, Computer Science Dept., Yale University; Fall 1985, visitor, Mathematical Sciences Research Institute, Berkeley).

Summers, 1993, 1983, 1979 Senior staff at Hampshire College Summer Studies in Mathematics, for high ability high school students.

Summers 1974-1977 Junior Staff, Hampshire College Summer Studies in Mathematics (NSF-SSTP).

PROFESSIONAL EXPERIENCE

Advisory Committees

member, Forum on Cyber Resilience, a National Academies of Sciences, Engineering, and Medicine Roundtable, 2016-present.

member, Computer Science and Telecommunications Board, National Academies of Sciences, Engineering, and Medicine, 2010-2016.

member, Advisory Board, National Cyber Security Hall of Fame, 2012-2015.

advisory board member, Committee on Women in Science and Technology, Stevens Institute of Technology, 2011-2013.

member, Advisory Committee, National Science Foundation Directorate for Computer and Information Science and Engineering, 2009-2012 (co-chair, Breakthrough Proposals subcommittee, spring 2012).

member, Commission on Cyber Security for the 44th Presidency, Center for Strategic and International Studies, 2009-2011.

member, ACM-W Council Executive Committee, 2009-2012.

member, ACM Committee on Women Advisory Board, 2003 - 2008.

board member, Computing Research Association Committee on the Status of Women in Computing Research, 2003-2010.

member, Information Security and Privacy Advisory Board, National Institute of Standards and Technology, 2002-2008.

Editorial

area editor, political and policy perspectives, *Journal of Cybersecurity,* 2015-present.

contributing editor, Lawfareblog, 2015-present.

associate editor in chief, *IEEE Security and Privacy,* 2013-2016.

editor, special issue on social networks, *IEEE Security and Privacy,* May/June 2013.

associate editor, *IEEE Security and Privacy,* 2005-2012 (editor, Emerging Standards column, 2005-2008).

co-editor, special issue on identity management, *IEEE Security and Privacy,* March/April 2008.

section board member, Privacy and Security Viewpoints column, *Communications of the ACM,* 2008-2014.

member, DIMACS Module Series Editorial Board, 1997 – 1999.

associate editor, *Notices of the American Mathematical Society,* 1994-2001.

Program Committees and Related Work

program committee member, Privacy Enhancing Technologies Symposium (PETS) and member of editorial board, *Proceedings of PETS (PoPETS), 2018*.

committee member, Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Trade Offs, National Academies of Sciences, Engineering, and Medicine.

program committee member, Privacy Enhancing Technologies Symposium (PETS) and member of editorial board, *Proceedings of PETS (PoPETS), 2017*.

participant, Berkman Center Berklett Cybersecurity Project, *Don't Panic: Making Progress on the Going Dark Debate,* 2016.

member, ACM Policy Award Committee, 2015-present.

member, Committee on the Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions, National Academies of Sciences, Engineering, and Medicine, 2015-2016.

member, Intelligence Science and Technology Experts Group, National Academies of Sciences, Engineering, and Medicine, 2015-present.

committee member, Committee on the Workshop on Privacy for the Intelligence Community: Emerging Technologies, Academic and Industry Research, and Best Practices, National Academies of Sciences, Engineering, and Medicine, 2015.

organizing committee member, Principles and Practice of Privacy Science Workshop, 2015.

organizing committee member, CCC Privacy by Design Workshops, 2014-2015.

program committee member, First International Workshop on Privacy Engineering, 2015.

steering committee member, Sackler Forum on Cybersecurity, National Academy of Science, 2014.

member, Committee on Responding to Section 5(d) of Presidential Decision Directive 28: The Feasability of Software to Provide Alternatives to Bulk Signals Intelligence Collection, National Research Council, 2014.

program committee member, ACM Workshop on Information Sharing and Collaboration, 2014.

member, Electorate Nominating Committee, Section on Information, Computing, and Communication, American Association for the Advancement of Science, 2014-present.

steering committee member, "Cybersecurity Ideas Lab," NSF, February 2014.

consultant, SRI, "Cybersecurity Policy Research at SRI: Scope, Value, and Challenges," 2013.

steering committee member, NSF Secure and Trustworthy Computing meeting, 2012.

program committee member, New Security Paradigms Workshop, 2012.

participant, Meeting of Experts, Department of Homeland Security's National Protection and Programs Directorate, Computer Science and Telecommunications Board, 2012.

committee member, Usability, Security, and Privacy of Computer Systems: a Workshop, National Academies of Sciences, Engineering, and Medicine, 2009-2010.

program committee member, Cloud Computing Security Workshop, CCS, 2009.

review committee member, NSF Future of the Internet program, April 2009.

member, Panels, Workshops, and Presentations Committee and Industry Advisory Committee, Grace Hopper Celebration of Women in Computer Science, 2007.

program committee member, Computers, Freedom, and Privacy, 2007.

program committee member, IEEE Symposium on Security and Privacy, 2006.

program committee member, Industry and Government Track, 12th ACM Conference on Computer and Communications Security, 2005.

program committee member, Workshop on Privacy in the Electronic Society, 2004.

advisory board member, Computers, Freedom, and Privacy, 2004.

program committee member, CRA "Grand Challenges in Information Security and Assurance" conference, 2003.

program committee member, Computers, Freedom, and Privacy, 2000.

distinguished lecturer, Sigma Xi, 1999-2001.

member, ACM Advisory Committee on Security and Privacy, 2001-2003.

member, ACM Committee on Law and Computing Technology, 1999-2003.

member-at-large, Mathematics Section, AAAS, 1994-1998.

member, Symbolic Computation Panel, NSF, 1997.

member (1995, 1996), chair (1997), Fulbright Scholars Discipline Advisory Committee: Computer Science.

consultant, National Research Council, 1996.

co-chair, Security and Privacy session, Massachusetts Telecommunications Conference, 1994.

program committee member, 1993 ISSAC Conference.

member, NSF PYI Panel, 1990.

member, NSF Panel on Scientific Computing Equipment in the Mathematical Sciences, 1987.

NSF Graduate Fellowship in Computer Science Evaluation Panel chair, 1989, member, 1987, 1988.

organizer, Cornell Day at Wesleyan Conference, 1987.

Service in Support of Women in Science (see also advisory committees)

co-chair, GREPSEC III Workshop, May 2017.

co-chair, GREPSEC II Workshop, May 2015.

co-chair, GREPSEC Workshop, May 2013.

member, PhD Forum Committee, Grace Hopper Celebration of Women in Computer Science, 2011.

chair, Athena Lecturer Selection Committee, 2006-2011.

founding co-chair, Athena Lecturer Selection Committee, 2005-2006.

co-chair, Women Engineers@Sun meeting, October 2008.

co-chair, Celebration of Women in Math at MIT, April 2008.

moderator, ResearcHers, a mailing list for women computer science researchers (organized under the auspicies of CRA-W and the Anita Borg Institute for Women and Technology), 2004 - 2016 (founder, 2004).

member, Speaker's Bureau, Association for Women in Mathematics, 1980-1985.

member, Membership Committee, Association for Women in Mathematics, 1981-1983.

AWARDS

EFF Pioneer Award, 2016, for *Keys under Doormats,* shared with Harold Abelson, Ross Anderson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter Neumann, Ronald Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, and Daniel Weitzner.

Inductee, Cybersecurity Hall of Fame, 2015.

M3AAWG J.D. Falk Award, 2015 for *Keys under Doormats,* shared with Harold Abelson, Ross Anderson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter Neumann, Ronald Rivest, Jeffrey Schiller, Bruce Schneier, Michael Specter, and Daniel Weitzner.

Surveillance Studies Book Prize, 2012, for *Surveillance or Security?*

The Guardian's Open 20: Fighters for Internet Freedom, 2012.

Fellow, John S. Guggenheim Foundation, 2012.

Fellow, Association for Computing Machinery, 2011.

Women of Vision Social Impact Award, Anita Borg Institute of Women and Technology, 2008.

ACM Distinguished Engineer, 2006.

Fellow, American Association for the Advancement of Science, 2000.

IEEE-USA Award for Distinguished Literary Contributions Furthering Public Understanding of the Profession, 1999 for *Privacy on the Line*, shared with Whitfield Diffie.

McGannon Book Award for Social and Ethical Relevance in Communication Policy Research, Donald McGannon Communication Research Center (Fordham University), 1998 for *Privacy on the Line*, shared with Whitfield Diffie.

NSF Mathematical Sciences Postdoctoral Fellowship, 1988.

GOVERNMENT BRIEFINGS (recent)

Panelist, Cybersecurity Session, Second Session of the Massachusetts-Quebec Collaborative Research Council, Massachusetts Senate, August, 2017.

Panelist, Setting the Problem: The National Encryption Debate, and Modernizing Law Enforcement panels, Workshop on the Future of Encrypted Communications, Hoover Institution, December 2016.

Panelist, "The 'Going Dark' Debate: Encryption and Evolving Technology," Congressional Research Service Congressional Seminar, July 2016.

Briefings, House and Senate Judiciary Committee staffs, Breakdown of content/non-content distinction and third-party doctrine in face of IP communications, April 2016.

Briefing, Senate Select Committee on Intelligence Staff, on Berkman Center Berklett Cybersecurity Project, *Don't Panic: Making Progress on the Going Dark Debate* and related issues, March 2016.

Testimony, House of Representatives Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy,* March 2016.

Briefing, Federal Communications Commission (Public Safety and Homeland Security), August 2014.

Commentary, Privacy and Civil Liberties Oversight Board, February 2014.

Briefing, Senate and House Judiciary Staff, Senate Commerce Committee Staff, Wiretapping without Weakening Communications Infrastructure, December 2012.

Briefing, Federal Communications Commission (Public Safety and Homeland Security) and Department of Justice (Office of Legal Counsel), Security Risks of Extending *Communications Assistance for Law Enforcement Act,* December 2011.

Briefing, Senate Judiciary staff, Security Risks with Extending *Communications Assistance for Law Enforcement Act,* April 2011.

Testimony, House of Representatives Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies,* February 2011.

Testimony, House of Representatives Committee on Science and Technology, Subcommittee on Technology and Innovation, *Cybersecurity Activities at NIST's Information Technology Laboratory,* October 2009.

Meeting with Sophia In't Veld and Alexander Alvaro, Members of European Parliament, security risks of the *Protect America Act,* May 2008.

Meeting with Achim Klabunde and Anna Buchta, European Commissions Directorate General Information, Society and Media, Electronic communications policy, security risks of *Protect America Act,* December 2007.

Meeting with Peter Hustinx, European Data Protection Supervisor, security risks of *Protect America Act,* December 2007.

Briefing, House Intelligence Committee, security risks of *Protect America Act,* October 2007.

Briefing, NSA Legal Staff, security risks of *Protect America Act,* October 2007.

Briefing European Commission, Information Society and Media, DRM, November 2007.

Meeting with Representative Zoe Lofgren re *Protect America Act,* August 2007 (with Whitfield Diffie).

Meeting with staff for Senator Mike DeWine, security risks in expansion of the *Communications Assistance for Law Enforcement Act,* September 2006.

PUBLICATIONS

Books

Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collections, National Research Council, *Bulk Collection of Signals Intelligence: Technical Options,* National Academies Press, 2015.

Susan Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies,* MIT Press, February 2011.

Winner of the 2012 Surveillance Studies Book Prize, given by the Surveillance Studies Network. Cited in *Liberty and Security in a Changing World,* 2013 (President's NSA Review Committee report). Comments on the book include: "This is an absolutely mandatory source book for everyone interested in the would-be conflicts," Peter Neumann (RISKS); "Landau's well-researched writing is a superb resource," Hilarie Orman *Cipher* (IEEE Committee on Security and Privacy); "the definitive text on the topic . . . a title that needs to be read," Ben Rothke, *Slashdot*; "the material is presented in way that is accessible for the general public yet specific enough to guide policymakers in Congress and the Executive branch—for whom it should be required reading," Suzanne Spaulding, former Executive Director, National Commission on Terrorism; "Susan Landau has taken an exceptionally complex but vital subject and presented it in a clear and compelling way," Jonathan Zittrain, Harvard Law School. "There are few books that comprehensively cover the subtle and complex interactions between technology, law, and public policy, and this is one of them. . . This book . . . will definitely be the standard reference for years to come." Earl Boebert.

Whitfield Diffie and Susan Landau, *Privacy on the Line: the Politics of Wiretapping and Encryption,* MIT Press, 1998 (rev. ed., 2007).

Winner, IEEE-USA Award for Distinguished Literary Contributions Furthering Public Understanding of the Profession, 1999, and McGannon Book Award for Social and Ethical Relevance in Communication Policy Research, Donald McGannon Communication Research Center (Fordham University), 1998.*Privacy on the Line* attracted international attention, including presentations on NPR and CSPAN's "About Books" program. The book was reviewed in *Business Week*,*Daily Telegraph* (British national newspaper), *The Guardian* (British national newspaper), *The Sciences,* and *Notices of the American Mathematical Society*," and received short reviews in *Science News, New Scientist, European Business Report, On Wall Street* among others. Review comments include "This book should be considered urgent reading," Robert Bruen in *Cipher* (IEEE Committee on Security and Privacy); "[a]

gem," *The Guardian*; "it's hard to imagine a better introduction to an issue that will be with us for years to come," Stewart Baker (former NSA counsel), in *Notices of the American Math Society*, and a listing as "recommended reading" in *Scientific American*. The Electronic Privacy Information Center distributed eighty copies to members of Congress.

Book Chapters

S. Landau, "CALEA: What's Next?" (opening argument, rejoinder, and last words), in Stewart Baker, Harvey Rishikof, and Bernie Horowitz, eds., *Patriot Debates II: Contemporary Issues in National Security,* American Bar Association, 2012, pp. 143-148, 151-154, 155-157.

W. Diffie and S. Landau, "The Export of Cryptography in the 20th Century and the 21st," *The History of Information Security: A Comprehensive Handbook,* Karl De Leeuw and Jan Bergstra (eds.), Elsevier, 2007, pp. 725-736. A modified version of this paper, "September 11th Did Not Change Cryptography Policy," *Notices of the Mathematical Society,* April 2002, pp. 450-454.

S. Landau, "Universities and the Two-Body Problem," in Bettye Anne Case and Anne Leggett (eds.), *Complexities: Women in Mathematics,* Princeton University Press, 2005, pp. 253-256. Originally appeared in *Computing Research Association Newsletter,* March, 1994, p.4, and was reprinted in the *Association for Women in Mathematics Newsletter,* March 1994, pp. 12-14, and in *SIGACT News,* December 1994, pp. 41-43.

S. Landau, "Tenure Track, Mommy Track," in Bettye Anne Case and Anne Leggett (eds.), *Complexities: Women in Mathematics,* Princeton University Press, 2005, pp. 260-263. Originally appeared in *Association for Women in Mathematics Newsletter,* May-June 1991, and was reprinted in shortened form in *Notices of the American Mathematical Society,* September 1991, pp. 703-4.

S. Landau, "Computations with Algebraic Numbers," in J. Grabmeier, E. Kaltofen, V. Weispfennig (eds.), *Computer Algebra Handbook,* Springer Verlag, 2003, pp. 18-19.

S. Landau, "The Transformation of Global Surveillance," in R. Latham (ed.), *Bytes, Bombs, and Bandwidth: Information Technology and Global Security,* Social Science Research Council, pp. 117-131, 2003.

S. Landau, "The Responsible Use of 'Expert' Systems," in *Directions and Implications of Advanced Computing,* Volume I, Ablex Publishing Corp. (1989), pp. 191-202, and *Proceedings of the Symposium on Directions and Implications of Advanced Computing,* (1987), pp. 167-181.

Law Review Articles and Related Work

S. Bellovin, M. Blaze, S. Landau, and S. Pell, "It's Too Complicated: How the Internet Upends *Katz, Smith,* and Electronic Surveillance Law," *Harvard Journal of Law and Technology,* Vol. 30, No. 1 (2017).

S. Bellovin, M. Blaze, and S. Landau, "Comments on Proposed Search Rules," *Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure,* October 31, 2014.

S. Landau, "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," *Journal of National Security Law and Policy,* Vol. 7, No. 3 (2014); one section, "The 1980s and 1990s — Who Controls Communication Security — The Department of Commerce or the NSA? and Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure," was reprinted in *Intelligence,* translation by Junichi Hiramatsu, Vol. 15, March 2015.

S. Bellovin, M. Blaze, S. Clark, and S. Landau, "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," *Northwestern Journal of Technology and Intellectual Property,* Vol. 12, Issue 1 (2014).

S. Landau, "The Large Immortal Machine and the Ticking Time Bomb," *Journal of Telecommunications and High Technology Law,* Volume 11, Issue 1 (2013), pp. 1-43.

S. Bellovin, S. Bradner, W. Diffie, S. Landau, and J. Rexford, "Can It Really Work? Problems with Extending EINSTEIN to Critical Infrastructure," *Harvard National Security Journal,* Vol. 3, Issue 1 (2012). A short version of the paper appeared as "As Simple as Possible — But No Simpler," *Communications of the ACM,* Vol. 54, No. 8 (August 2011), pp. 30-33.

D. D. Clark and S. Landau, "Untangling Attribution," *Harvard National Security Journal,* Vol. 2, Issue 2 (2011); earlier version appeared in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy,* National Academies Press, 2010, pp. 25-40.

S. Landau, "National Security on the Line," *Journal of Telecommunications and High Technology Law,* Vol. 4, Issue 2, Spring 2006, pp. 409-447.

Refereed Technical Publications

S. Bellovin, S. Landau, and H. Lin, "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications," *Journal of Cybersecurity,* Vol. 3, Issue 1 (2017), pp. 59-68.

S. Bellovin, M. Blaze, and S. Landau, "Searching Securely: Technical Risks with Remote Computer Searches," *COMPUTER,* Vol. 49, No. 3 (March 2016) pp. 14-24; reprinted in *Computing Now,* June 2016.

H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter, D. Weitzner, "Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity,* Vol. 1; a short version of "Keys under Doormats," appeared in *Communications of the ACM,* Vol. 58, No. 10 (October 2015), pp. 24-26.

S. Landau, "NSA and Dual EC_DRBG: Deja Vu All Over Again?," *Mathematical Intelligencer,* Vol. 37, Issue 4 (December 2015), pp. 72-83.

S. Bellovin, M. Blaze, S. Clark, and S. Landau, "Going Bright: Wiretapping without Weakening Communications Infrastructure," *IEEE Security and Privacy,* Vol. 11, No. 1, January/February 2013, pp. 62-72. [Cited in *Washington Post* op-ed, "How to Break the Deadlock over Data Encryption," March 13, 2016, and *New York Times* editorial, "Eavesdropping on Internet Communications," May 20, 2013.]

C. Landwehr, D. Boneh, J. Mitchell, S. Bellovin, S. Landau, and M. Lesk, "Privacy and Cybersecurity: The Next 100 Years," *Proceedings of the IEEE,* Vol. 100, Issue: Special Centennial Issue (2012), 1659-1673.

S. Landau and T. Moore, "Economic Tussles in Federated Identity Management," *First Monday,* Vol. 17, No. 10 (October 2012). Originally appeared at *Workshop on Economics of Information Security,* 2011.

W. Diffie and S. Landau, "Communications Surveillance: Privacy and Security at Risk," *Communications of the ACM,* Vol. 52 No. 11 (November 2009), Pages 42-47, and Queue (October 2009).

S. Bellovin, M. Blaze, W. Diffie, S. Landau, P. Neumann, and J. Rexford, "Risking Communications Security: Potential Hazards of the 'Protect America Act'," *IEEE Security and Privacy,* Vol. 6, No. 1 (January/February 2008), pp. 24-33. A short version of this paper appeared as "Internal Risks, External Surveillance," Inside Risks 209, *Communications of the ACM* 50, p. 128, Dec, 2007.

S. Landau, "Find Me a Hash," *Notices of the American Mathematical Society,* March 2006, pp. 330-332; reprinted in *Mathematical Advance in Translation,* Chinese Academy of Sciences, 3 (2010) pp. 226-228.

S. Landau, "Security, Wiretapping, and the Internet," *IEEE Security and Privacy*, Vol. 3, No. 6 November/December 2005, pp. 26-33.

S. Landau, "Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard," *American Mathematical Monthly,* February 2004, pp. 89-117.

S. Landau and N. Immerman, "Embedding Linkages in Integer Lattices," *Algorithmica*, Vol. 32, No. 3 (2002), pp. 423-436, originally appeared in *MSI Workshop on Computational Geometry,* October 1994.

S. Landau, "Designing Cryptography for the New Century," *Communications of the ACM,* Vol. 43, No. 5, May 2000, pp. 115–120.

S. Landau "Communications Security for the Twenty-First Century: the Advanced Encryption Standard," *Notices of the American Mathematical Society,* April 2000, pp. 450–459. Reprinted, in translation, in "Surveys in Applied and Industrial Mathematics," TVP Publishers (Moscow), Vol. 7, No. 2 (2000), pp. 259-281.

S. Landau, "Standing the Test of Time: the Data Encryption Standard," *Notices of the American Mathematical Society,* March 2000, pp. 341-349. Reprinted, in translation, in "Surveys in Applied and Industrial Mathematics," TVP Publishers (Moscow), Vol. 7, No. 2 (2000), pp. 240-258.

S. Landau, "$\sqrt{2}+\sqrt{3}$: Four Different Views," *Mathematical Intelligencer*, Vol. 20, No. 4 (Fall 1998), pp. 55-60.

D. Kozen, S. Landau, and R. Zippel, "Decomposition of Algebraic Functions," *Journal of Symbolic Computation*, Vol. 22 (1996), pp. 235-246, originally appeared in *Algorithmic Number Theory Symposium (1994)*.

S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann and D. Sobel, "Crypto Policy Perspectives," in *Communications of the ACM,* Vol. 37 (August, 1994), pp. 115-121 (a longer version appears in "Reports").

S. Landau, "How to Tangle with a Nested Radical," *Mathematical Intelligencer*, Vol. 16, No. 2 (Spring 1994), pp. 49-55.

N. Immerman and S. Landau, "The Complexity of Iterated Multiplication," *Information and Computation*, Vol. 116, No. 1 (1995), pp. 103-116, originally appeared in *Fourth Annual Structure in Complexity Conference (1989)*, pp. 104-111.

S. Landau, "Simplification of Nested Radicals," *SIAM J. of Comput.*, Vol. 21 (1992), pp. 85-110, originally appeared in *Thirtieth Annual IEEE Symposium on Foundations of Computer Science (1989)*.

S. Landau, "A Note on 'Zippel Denesting,' " *J. Symb. Comput.*, Vol. 13 (1992), pp. 41-47.

J. Cremona and S. Landau, "Shrinking Lattice Polyhedra," *SIAM J. of Discrete Math*, Vol 3, No. 3 (1990), pp. 338-348, originally appeared in *Proceedings of the First ACM-SIAM Symposium on Discrete Algorithms (1990)*, pp. 188-193.

D. Kozen and S. Landau, "Polynomial Decomposition Algorithms," *J. Symb. Comput*., Vol. 7 (1989), pp.445-456; a different version appeared as J. von zur Gathen, D. Kozen and S. Landau under the title "Functional Decomposition of Polynomials" at the *Twenty Eighth Annual IEEE Symposium of the Foundations of Computer Science (1987),* pp. 127-134.

S. Landau, "Some Remarks on Computing the Square Parts of Integers," *Information and Computation,* Vol. 78, No. 3 (1988), pp. 246-253.

S. Landau, "Zero Knowledge and the Department of Defense," *Notices of the American Mathematical Society* [Special Article Series], Vol. 35, No. 1 (1988), pp. 5-12.

S. Landau, "Factoring Polynomials Quickly," *Notices of the American Mathematical Society*, [Special Article Series], Vol. 34, No. 1 (1987), pp. 3-8.

S. Landau and G. Miller, "Solvability by Radicals is in Polynomial Time," *J. of Comput. and Sys. Sci.*, Vol. 30, No. 2 (1985), pp. 179-208, originally appeared in *Fifteenth ACM Symposium on Theory of Computing* (1983).

S. Landau, "Factoring Polynomials over Algebraic Number Fields," *SIAM J. of Comput.*, Vol 14, No. 1 (1985), pp. 184-195.

S. Landau, "Primes, Codes and the National Security Agency,"*Notices of the American Mathematical Society*, [Special Article Series], Vol. 30, No. 1 (1983), pp. 7-10.

Other Journal Publications

S. Landau, "Transactional information is remarkably revelatory" *Proceedings of the National Academy of Sciences,* Vol. 113, No. 20 (May 17, 2016), pp. 5467-5469.

S. Landau, "Choices: Privacy & Surveillance in a Once & Future Internet," *Daedulus,* Vol. 145, No. 1 (Winter 2016), pp. 54-64.

S. Landau, "Educating Engineers: Teaching Privacy in a World of Open Doors," *IEEE Security and Privacy,* Vol. 12, No. 3 (May/June 2014), pp.66-70.

S. Landau, "Making Sense of Snowden Part II: What's Significant in the NSA Surveillance Revelations," online in *IEEE Security and Privacy,* Vol. 12, No. 1, January/February; a short version, "Highlights from Making Sense of Snowden Part II: What's Significant in the NSA Surveillance Revelations," appeared in *IEEE Security and Privacy,* Vol. 12, No. 1 (January/February 2014), pp. 62-64.

S. Landau, "Making Sense of Snowden: What's Significant in the NSA Surveillance Revelations," *IEEE Security and Privacy,* Vol. 11, No. 4 (July/August 2013), pp. 54-63.

A. Cavoukian, A. Davidson, M. Hansen, S. Landau, and A. Slomovic, "Privacy: Front and Center," *IEEE Security and Privacy,* Vol. 10, No. 5 (September/October 2012), pp. 5-10.

S. Landau, "The NRC Takes on Data Mining, Behavioral Surveillance, and Privacy," *IEEE Security and Privacy,* Vol. 7, No. 1 (January/February 2009), pp. 58-62.

S. Landau, "Security and Privacy Landscape in Emerging Technologies," *IEEE Security and Privacy,* Vol. 6, No. 4 (August/September 2008), pp. 74-77.

S. Landau and M. Stytz, "Overview of Cyber Security: A Crisis of Prioritization," *IEEE Security and Privacy,* Vol. 3, No. 3, May/June 2005, pp. 9-11 and sidebar, S. Landau, C. Landwehr, and F. Schneider, "The PITAC Report: A Brief Analysis," p. 10.

S. Landau, "Security, Liberty, and Electronic Communications," (invited talk), in Matt Franklin (ed.), *Advances in Cryptology: CRYPTO 2004,* Springer Verlag, pp. 355-372.

S. Landau, "RSA and Public-Key Cryptography; Introduction to Cryptography; Cryptography: Theory and Practice; Algebraic Aspects of Cryptography; Elliptic Curves; Number Theory and Cryptography; Elliptic Curves in Cryptography; Modern Cryptography, Probabilistic Proofs, and Pseudorandomness; Foundations of Cryptography: Basic Tools; The Design of Rijndael: AES — the Advanced Encryption Standard; Handbook of Applied Cryptography," *Bulletin of the American Mathematical Society,* Vol. 41, No. 3 (2004), pp. 357-367.

Conference and Workshop Proceedings (that did not also appear in journals)

D. D. Clark and S. Landau, "The Problem isn't Attribution; It's Multi-Stage Attacks," *Third International Workshop on Re-Architecting the Internet, 2010.*

S. Landau, H. Le Van Gong, and R. Wilton, "Achieving Privacy in a Federated Identity Management System," *Financial Cryptography and Data Security '09*, pp. 51-70.

S. Landau, R. Stratulate, and D. Twilleager, "Consumers, Fans, and Control: What the Games Industry Has to Teach Hollywood about DRM," *ACM CCS Workshops: DRM '06,* pp. 1-7.

S. Landau, "Eavesdropping and Encryption: U.S. Policy in an International Perspective," *Conference on the Impact of the Internet on Communications Policy (1997),* John F. Kennedy School of Government, Harvard University.

S. Landau and N. Immerman, "The Similarities (and Differences) between Polynomials and Integers," *International Conference on Number Theoretic and Algebraic Methods in Computer Science,* 1993 Moscow, pp. 57-59.

S. Landau, "Polynomial Time Algorithms for Galois Groups," *Proceedings of the International Symposium on Symbolic and Algebraic Computation (1984),* Springer Verlag Lecture Notes in Computer Science No. 174, pp. 225-236.

Editorials and Opinion Columns

S. Landau, "Is it Legal? Is it Right? The Can and Should of Use," *IEEE Security and Privacy,* Vol. 14, No. 5 (September/October 2016), pp. 3-5.

R. Wyden, M. Blaze, and S. Landau, "The Government Will Soon Be Able to Legally Hack Anyone," *Wired,* September 14, 2016.

S. Landau, "The Real Security Risks of the iPhone Case," *Science,* Vol. 352, Issue 6292 (June 17, 2016), pp. 1398-1399.

S. Landau, "Transactional information is remarkably revelatory," *Proceedings of the National Academy of Sciences,* Vol. 113, No. 19 (May 17, 2016), 5467-5469.

S. Landau, "Perspective: Cybersurveillance and the New Frontier of Deterrence," *Current History,* Vol. 115, Issue 117 (January 2016), pp. 29-31.

S. Landau, "What was Samsung Thinking?," *IEEE Security and Privacy,* Vol. 13, No. 3 (May/June 2015), pp. 3-4.

S. Landau, "Control Use to Protect Privacy," *Science,* Vol. 347, Issue 6221, January 30, 2015, pp. 504-506.

S. Landau, "Privacy and Security: Summing Up," *Communications of the ACM,* Vol. 57, Issue 11 (November 2014), pp. 37-39.

S. Landau, "Security and Privacy: Facing Ethical Choices," *IEEE Security and Privacy,* Vol. 12, No. 4 (July/August 2014), pp. 3-6.

S. Landau, "Politics, Love, and Death in a World of No Privacy," guest editor column for *IEEE Security and Privacy* special issue on privacy and online social networks Vol. 11, No. 3 (May/June 2013), pp. 11-13.

S. Landau, "Privacy and Security: A Multidimensional Problem," introductory editor's column for Privacy and Security Viewpoints, *Communications of the ACM,* Vol. 51, Issue 11 (November 2008), pp. 25-26.

S. Landau and D. Mulligan, "I'm Pc01002/SpringPeeper/ED288l.6; Who are You?," guest editors' column for *IEEE Security and Privacy* special issue on identity management, Vol. 6, No. 2 (March/April 2008), pp. 13-15.

S. Bellovin, M. Blaze, and S. Landau, "The Real National-Security Needs for VoIP," *Communications of the ACM,* Vol. 48, No. 11, November 2005, p. 120.

S. Landau, "What Lessons are we Teaching?," Insider Risks 180, *Communications of the ACM* Vol. 48, No. 6, June 2005, p. 144.

S. Landau, "Time to Move Mountains," *Notices of the American Mathematical Society,* September 2000, p. 853.

S. Landau, "Internet Time," *Notices of the American Mathematical Society,* March 2000, p. 325.

S. Landau, "Compute and Conjecture," *Notices of the American Mathematical Society,* February 1999, pg. 189.

S. Landau, "Cryptography in Crisis," *Notices of the American Mathematical Society,*" April 1998, p. 461.

S. Landau, "The Myth of the Young Mathematician," *Notices of the American Mathematical Society,* November 1997, p. 1284.

S. Landau, "Mathematicians and Social Responsibility," *Notices of the American Mathematical Society,* February, 1997, p. 188.

S. Landau, "Rising to the Challenge," *Notices of the American Mathematical Society,* June, 1996, p. 652.

S. Landau, "Something There is That Doesn't Love a Wall," *Notices of the American Mathematical Society,* November 1995, p. 1268.

S. Landau, *Notices of the American Mathematical Society,* May 1995, p. 524.

Magazine and Newspaper Publications; Blog Postings

S. Landau, "Russia's Hybrid Warriors Got the White House, Now They're Coming for America's Town Halls," *Foreign Policy,* September 26, 2017.

S. Landau, "The Encryption Wars: Everything has Changed, and Nothing has Changed," *Scientific American* (blog post), November 18, 2015.

S. Landau and C. O'Neil, "Why Ghosts in the Machine Should Remain Ghosts," Lawfareblog.com, December 7, 2016.

S. Landau, "Phones Move—and So Should the Law," August 16, 2017; "An Important Russian Hacking Story," June 2, 2017; "A Step Forward for Security," May 17, 2017;"The FBI and I Agree," March 14, 2017; "The FBI Should be Enhancing US Cybersecurity, Not Undermining It," December 1, 2016; "Protecting the Republic: Securing Communications is More Important than Ever," November 21, 2016; "Securing Phones and Securing US (revisited)," September 15, 2016; "Setting Up a Straw Man: ODNI's Letter in Response to 'Don't Panic,' " May 12, 2016; "Million Dollar Vulnerabilities and an FBI for the Twenty-first Century," April 26, 2016; "A Response to Susan's Post," March 25, 2016; "The National-Security Needs for Ubiquitous Encryption," February 2, 2016 (also appeared in *Don't Panic: Making Progress on the Going Dark Debate*, Berkman Center Berklett Cybersecurity Project); "Be Careful What You Wish For: A Response," January 8, 2016; "Why the Support for Crypto," September 21, 2015; "A Public Split: Listening to the Conversation at Aspen," July 28, 2015; "Thoughts on Encryption and Going Dark: Counterpart," July 15, 2015; "Keys Under Doormats: Mandating Insecurity," July 7, 2015; "Director Comey and the Real Threat," July 3, 2015; "Why the Privacy Community Focuses Where it Does," June 16, 2015; "Time to Resolve the Metadata Fight," May 29, 2015; "What We Must Do about Cyber," March 10, 2015; "Finally . . . Some Clear

Talk on the Encryption Issue," February 16, 2015; "What David Cameron Doesn't Get," January 20, 2015; "Securing Phones — and Securing US," September 29, 2014; "On NSA's Subversion of NIST's Algorithm," July 25, 2014; "What the Court Didn't Say in *Riley* may be the Most Important Thing of All," June 30, 2014; "Obama Administration's New Wiretapping Proposal," May 13, 2013;"US Government Surveillance via New Technologies," April 30, 2013; Lawfareblog.com.

M. Blaze and S. Landau, "The FBI Needs Hackers, Not Backdoors," *Wired,* January 14, 2013.

S. Landau, "Surveillance and Security: Securing whom? And at what cost?," *Privacy International,* November 30, 2011.

S. Landau, "What the President Said — and Didn't Say — About Surveillance," August 11, 2013; "Canaries in the Coal Mine," June 6, 2013; S. Landau, "Boston and the Right to Privacy," April 22, 2013; 'Cybersecurity — Getting it Right This Time," February 13, 2013; "Searching in a Haystack . . . Finds Straw," October 15, 2012; "Nothing to Fear but Fear Itself," April 29, 2012; "One Small Step for Privacy . . .," January 26, 2011; "It's All in How You View It," January 17, 2012; "Hollywood and the Internet: Time for the Sequel," November 28, 2011; "Who Knows Where I Am? What Do They Do with the Information?," October 3, 2011; "Data Retention? *News of the World* Shows the Risks," July 21, 2011; "Mr. Murdoch and Mr. Brown: A Real-Life Example of Why Privacy Matters," July 18, 2011; "Where Have All the Wiretaps Gone?," July 14, 2011; "Privacy, Online Identity Solutions, and Making Money: Pick Three?," July 7, 2011; "Getting Communications Security Right," April 19, 2011; "Getting Wiretapping Right," July 5, 2011; "NIST Leads the Charge on Online Authentication," January 12, 2011; "Who's Been Looking Over my Shoulder? — The FTC Seeks to Update Online Privacy," December 6, 2010; "The FBI Wiretap Plan: Upsetting the Security Equation," October 25, 2010; "Moving Rapidly Backwards on Security," October 13, 2010; "The Pentagon's Message on Cybersecurity," August 31, 2010; "Wrong Direction on Privacy," August 2, 2010; "Separating Wheat from Chaff," July 23, 2010, *Huffington Post.*

W. Diffie and S. Landau, "Brave New World of Wiretapping," *Scientific American,* September 2008, pp. 33-39.

S. Landau, "A Gateway for Hackers: The Security Threat in the New Wiretapping Law," *Washington Post,* August 9, 2007, p. A17.

W. Diffie and S. Landau, "Cybersecurity Should be Kept in Civilian Hands," *Boston Globe,* 19 August 2002, pp. E-4. Appeared in slightly different form as "Ensuring Cybersecurity" in *NGO Reporter,* Vol. 10, No. 2, Sept. 2002.

W. Diffie and S. Landau, "The Threat of .NET," *New Technology Week,* November 5, 2001.

S. Landau, "Dangerous Increase of FBI Surveillance," Op-Ed, *Chicago Tribune,* March 6, 1998, p. 23.

S. Landau and W. Diffie, "Cryptography Control: FBI Wants It, but Why?," Op-Ed, *Christian Science Monitor,* October 6, 1997, p. 19.

S. Landau, "Joseph Rotblat: From Fission Research to a Prize for Peace," *Scientific American*, January 1996, pp. 38-39.

S. Landau, "Joseph Rotblat: The Road Less Traveled," *Bulletin of the Atomic Scientists*, January-February 1996, pp. 46-54.

S. Landau, "What's Doing in Ithaca, New York," *New York Times*, September 9, 1979, Section X, p.7.

Other Publications

T. Benzel, S. Landau, and H. Orman, "Expanding the Pipeline: G/rep{sec}= underrepresented groups in security research," *Computing Research News,* March 2015, pp. 8-10.

S. Landau, "Timesharing Dexter" (Laudito), in R.L. Constable and A. Silva, eds., *Kozen Festschrift,* LNCS 7230, pp. 329-332, Springer, 2012.

S. Landau, "Clipper and Capstone," "Cryptography," and "Digital signatures," entries in W. Staples, ed., *Encylopedia of Privacy,* Greenwood Press, 2007, pp. 101-104, pp. 151-153, pp. 166-168, resp.

S. Landau, "Anywhere, Anytime — Or Just Where is Your Office Anyhow?," Pipeline series, *Computing Research News,* September 2005, p. 2.

S. Landau, "A Far Cry from Galois Fields," *Association for Women in Mathematics Newsletter,* November-December 2003, pp. 11-13.

S. Landau, ed., *Liberty ID-WSF Security and Privacy Review,* 2003.

S. Landau and J. Hodges, *A Brief Introduction to Liberty,* 13 February 2003.

G. Ellison, J. Hodges, and S. Landau, *Risks Presented by Single Sign-On Architectures,* 18 October 2002.

G. Ellison, J. Hodges, and S. Landau, *Security and Privacy of Internet Single Sign-On: Risks and Issues as They Pertain to Liberty Alliance Version 1.0,* 6 September 2002.

S. Landau, "Cryptography," *Computer Sciences,* Ed., Roger R. Flynn. Vol. 4: Electronic Universe. New York: Macmillan Reference USA, 2002. pp. 49-53.

S. Landau, "Advanced Encryption Standard Choice is Rijndael," *Notices of the American Mathematical Society,* January 2001, p. 38.

S. Landau, "Finding Maximal Subfields," *SIGSAM Bulletin,* Vol. 27, No. 3 (1993), pp. 4-8.

S. Landau, "The Secret of Life is a Nontrivial Computation," *SIAM News*, May 1991, pp. 12-13.

Reports

B. Adida, C. Anderson, A. Anton, R. Dingledine, E. Felten, M. Green, A. Halderman, D. Jefferson, C. Jennings, S. Landau, N. Mitter, P. Neumann, E. Rescorla, F. Schneider, B. Schneier, H. Shacham, M. Sherr, D. Wagner, and P. Zimmermann, "CALEA II: Risks of Wiretap Modifications to Endoints," Center for Democracy and Technology, May 2013.

S. Bellovin, M. Blaze, E. Brickell, C. Brooks, V. Cerf, W. Diffie, S. Landau, J. Peterson, J. Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP," http://www.itaa.org/news/docs/CALEAVOIPreport.pdf, 2006.

S. Landau, S. Kent, C. Brooks, S. Charney, D. Denning, W. Diffie, A. Lauck, D. Miller, P. Neumann and D. Sobel, "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy," ACM Press, 1994.

Software

Both the Maple and AXIOM (formerly Scratchpad) symbolic computation systems use the Kozen-Landau algorithm as a basis for their polynomial decomposition routines.

OTHER PRESENTATIONS

Television Appearances

CNBC Nightly Business Report (PBS), February 17, 2016.

PBS News Hour, July 8, 2015.

Democracy Now, "More Intrusive Than Eavesdropping? NSA Collection of Metadata Hands Gov't Sweeping Personal Info," June 12, 2013.

Great Decisions: Cybersecurity, PBS, multiple stations, spring 2012.

Brian Lehrer Show, WNYC, June 29, 2011.

Capital Insider, WJLA (Washington), April 21, 2011.

Everybody's Internet, Boston Neighborhood Network, March 10, 1999.

BOOKS!, Channel 3, Boston (local cable network), November 7, 14, 21, 28, 1998; DC showing April 1999.

About Books, CSPAN-2, August 1, 1998.

Radio Interviews

Today, BBC, March 27, 2017.

Codebreaker (produced by Marketplace), NPR, December 21, 2016.

The John Batchelor Show, July 5, 2016.

To The Point, Public Radio International, March 24, 2016.

All Things Considered, NPR, March 7, 2016.

The Inquiry, BBC, March 1, 2016.

Security Mom, WGBH, October 9, 2015.

The Takeaway, Public Radio International, July 10, 2015.

The Takeaway, Public Radio International, July 7, 2015.

The Takeaway, Public Radio International, October 17, 2014.

The Digital Show, Business Radio on Sirius XM, October 6, 2014.

Big Picture Science, PRSS, PRX, and Radio Pacifica Network, August 5, 2014.

To the Best of Our Knowledge, Public Radio International, June 21, 2013.

Fairness Radio, June 17, 2013.

Cyberjungle, June 11, 2013.

BBC 5 Live, June 7, 2013.

WTOP Radio, June 7, 2013.

Free Speech Radio News, Pacifica Radio (NPR affiliate), June 7, 2013.

Marc Steiner Show, WEAA (NPR affiliate), September 8, 2011.

Marc Steiner Show, WEAA (NPR affiliate), February 22, 2011.

All Things Considered, NPR, February 22, 2011.

Marc Steiner Show, WEAA (NPR affiliate), September 28, 2010.

Patt Morrison, KPCC (NPR affiliate), September 27, 2010.

On the Media, WNYC (NPR affiliate), September 20, 2008.

Science Friday, NPR (nationally-syndicated), August 17, 2007.

Marketplace, NPR (nationally-syndicated), August 10, 2000.

Marketplace, NPR (nationally-syndicated), July 11, 2000.

Fieger Show, WXYT, Detroit, Michigan, April 15, 1999.

FOCUS 580, WILL, Indianapolis, Indiana (NPR affiliate), June 12, 1998.

WBUR, Boston (NPR affiliate), May 7, 1998.

The Green Room, WFMU, New Jersey, February 9, 1998.

Talk of the Nation, NPR, February 2, 1998.

Major Talks (including Keynotes)

"Crypto Wars: The Apple iPhone and the FBI," Keynote, DigiDark—The Dark Side of Digitization: Fraud, Surveillance, Sourveillance, Disinformation, Privacy Loss, and Cyber Extremism, Darmstadt, July 2016.

"Mining the Metadata — and Its Consequences," Keynote, International Conference on Software Engineering, May 2015.

"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," Keynote, Conference on Detection of Intrusions and Malware and Vulnerability Assessment, July 2014.

"The Large Immortal Machine and the Ticking Time Bomb," Fifth Annual Privacy Lecture, Berkeley Center for Law and Technology, March 2012 (CLE credit).

"Surveillance or Security? The Risks Posed by New Wiretapping Technologies," Plenary, AusCERT, May 2012; Invited Talk, Large Installation System Administration Conference (LISA), December 2011.

"Privacy: It's All in the Use Case," Invited Essayist, Advanced Computer Security Applications Conference, December 2011.

"A Computer Scientist Goes to Washington: How to Be Effective When Facts are 10% of the Equation," SIGCSE Keynote, March 2011.

"Bits and Bytes: Explaining Communications Security (and Insecurity) in Washington and Brussels," Invited Talk, Grace Hopper Celebration of Women in Computer Science, October 2009.

"Internet Surveillance: Building our own Trojan Horse," Invited Talk, USENIX, June 2008.

"Unsecuring the Internet: A New Government Policy?," Keynote, Northeastern Conference of the Consortium for Computing Sciences in Colleges, Plattsburgh, NY, April 2008.

"Wiretapping the Internet: Communications Insecurity," Keynote, British Columbia Privacy and Security Conference, February 2008.

"Keep Calm and Carry On," Invited Talk, HP Day, Royal Holloway College, December 2007.

"The Missing Link," Keynote, Privacy Enhancing Technologies Workshop, June 2006.

"Security, Trusted Computing, and DRM," Invited Talk, Javapolis 2004, Antwerp, December 2004.

"Security, Liberty, and Privacy," Invited Talk, CRYPTO, August, 2004.

"Old Math, New Math: Using Polynomials to Gain Insight into the Design of Cryptosystems," Invited Hour MAA Speaker, Joint Math Meetings, January 2002.

Other Invited Talks

"Cybersecurity," "Surveillance," Asia Pacific School on Internet Governance, Bangkok, July 2017.

"Protecting and Exposing Private Data," 9/11 Memorial Museum, May 2016.

"Architectures and the Differences They Create: Why Security, Authentication, and Attribution are Easy on the Phone Network and Hard in IP Networks," "A Brief history of Internet-Based attacks, and Why Security is So Hard," "Privacy risks and Protections in an Internet Context," KAIST GLobal Lecture Series, May 2016.

Introductory Remarks before *The Conversation,* Science on Screen Series, Coolidge Corner Theatre, November 2015.

"The Second Crypto Wars in Context," Microsoft Briefing, October 2015.

"It's Too Complicated: The Conflict between the Technological Implications of IP-Based Communications and US Surveillance Law," Information Security Project, Yale Law School, April 2017; The Academic Perspective on Cybersecurity Challenges, Blavatnik ICRC, Tel Aviv University, June 2016; KAIST CSRC/GSIS International Workshop on Legal Regulations for 21st Century, May, 2016; UCL Distinguished Lecture, October 2015.

"Crypto Wars: Plus ça Change, Plus c'est la Même Chose," Merck, July 2016; KAIST, May 2016; NSF WATCH series, April 2016, Twenty Years of Cryptography and Security at WPI Symposium, October 2015.

"Keys under Doormats: Mandating insecurity by requiring government access to all data and communications," Kennedy School Nye Cyber Seminar Series, October 2015.

"Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet," Duo Tech Talk, September 2016; University of Massachusetts at Amherst, March 2015.

"Bulk Collection of Signals Intelligence: Technical Alternatives — or — There's no Technological Magic," CISAC, Stanford University, April 2015; Kennedy School Nye Cyber Seminar Series, March 2015; Columbia University Security Seminar, February 2015.

"Cryptography and Privacy — and the Role for Mathematicians: Parts I and II," G. Milton Wing Lecture Series, University of Rochester, October 2014.

"Cybersecurity Ideas Lab Report: Interdisciplinary Pathways towards a More Secure Internet," Kennedy School Nye Cyber Seminar Series, October 2014.

"NSA Crypto Trapdoors and the Damage to US Interests," Bureau of Intelligence and Research, State Department, August 2014.

"Does Wiretapping Make Us More Secure? What a Computer Scientist Has to Add to the National Conversation," University of Michigan Distinguished Lecture, Februry 2014.

"What's Significant in the NSA Revelations," G. Milton Wing Lectures, University of Rochester, October 2014; IDA 30th Year Celebration Seminar, Linkoping University, Sweden, October 2013.

"Primes, Surveillance, and the National Security Agency," Hampshire Summer Studies in Math, July 2013.

"The Future of Wiretapping," IEEE Webinar, June 2013.

"A US Wiretap Snapshot: May 2013," British Telecom Executive Visitor's Group, MIT, May 2013.

"Under the Radar: NSA's Efforts to Secure Private-Sector Communications Infrastructure," Kennedy School Minerva Working Group, April 2013.

"Can It Really Work? Problems with Extending EINSTEIN to Critical Infrastructure," Kennedy School Minerva Working Group, March 2012.

"Envisioning Cybersecurity Research — and Education — in New England," New England Summit on Cyber Security, Boston University, June 2011.

"Cybersecurity: Asking the Right Questions," Watson Institute, Brown University, February 2013; Distinguished Lecture, AT&T, May 2011.

"Cybersecurity and Cyber Freedom: The Future of Digital Surveillance Technology," Brookings Institution, February 2011.

"Surveillance or Security? The Risks Posed by New Wiretapping Technologies," ISPIA Distinguished Lecture, University of Calgary, April 2013; Bolt, Beranek, and Newman, January 2013; Sammet Lecture, Mt. Holyoke, November, 2012; Mitre, November 2012; Politecnico di Milano, September

2012; Triangle Distinguished Lecture (Duke, NCSU, UNC), November 2011; ETHZ/University of Zurich Workshop and Lecture Series on Technology: Policy, Law, and Economics, November, 2011; IEEE/ACM-CS Central New Jersey Chapter, April 2011; Berkman Institute for Internet and Society, Harvard University, March 2011; University of California at Berkeley, February 2011; Google, New York, November 2010; Distinguished Lecture, University of Waterloo, November 2010.

"Untangling Attribution: Designing for Requirements," Computational Cybersecurity in Compromised Environments (C3E), Arlington VA, June 2015; University of Calgary, April 2013; Invited Talk, Third Workshop on Mathematical Cryptology (WMC2012), Castro Urdiales, Spain, July 2012; Distinguished Lecture, Stevens Institute of Technology, April 2012; ETHZ/University of Zurich Workshop and Lecture Series on Technology: Policy, Law, and Economics, November, 2011; CRCS seminar, Harvard, November 2010; Kennedy School Minerva Working Group, November 2010; Information Science Department, Cornell University, November 2010.

"Building our own Trojan Horse: Communications Surveillance and Creating Communications (In)Security," Institute for Information Infrastructure, October 2009; Berkeley EECS, March 2009; MIT CSAIL, February 2009; LERIAS, University of Pittsburgh, November 2008; Interdisciplinary Studies in Information Security, Ascona, Switzerland, July 2008.

"Transactional Information is Remarkably Revelatory," Women's Institute in Summer Enrichment, Cornell, June 2008.

"The Logic of the Law: Warrants for Content, Subpoenas for Transactional Information," Women's Institute in Summer Enrichment, Cornell, June 2008.

"COMSEC v. COMINT, and is Terrorism the Right Question?," Ecole Polytechnique Fédérale Lausanne, July 2007.

"DRM: A Different Approach," Harvard CRCS seminar, November 2006.

"Polynomials in the Nation's Service: Designing the Advanced Encryption Standard," Tufts University, October 2002.

"Putting Precision into the 'Crypto' Wars," Social Science Research Council. Workshop on Information Technology and Social Research: Setting the Agenda, June 2002.

"The Internet, Security, and Privacy," ETH, Zurich, November 2001.

"The Profound Effect of Computer Science on Teaching and Research in Mathematics," Fundamentals of Computing Workshop, CSTB, National Research Council, July 2001.

"Cryptology: Technology and Policy," University of Puerto Rico, Ponce, February 2001; CERIAS seminar, Purdue, December 2000; Physics Colloquium, Argonne National Laboratory, December 2000; Williams College, November 2000; Stanford University, February 2000; Connecticut College, May 2000; C.K. Whitco (Uniroyal), September 1999; Hoffman LaRoche, May 1999; NASA Greenbelt, Maryland, March 1999; Rockefeller Distinguished Lecturer, Dartmouth College, March 1999; Institute for Defense Analyses, Alexandria, Virginia, February 1999; Corning Research Labs, February 1999; University Lecture Series, University of Wisconsin, December 1998; Institute for Science and Interdisciplinary Studies, Hampshire College, October 1998; Policy Program, University of Massachusetts, October 1998; Worcester Polytechnic Institute, April 1998; MSRI; January 1998, DIMACS Research and Education Institute, July 1997.

"Codes, Keys, and Conflicts: Issues in US Crypto Policy," Amherst College, November 1996, Distinguished Lecture, UC Irvine, January 1996; Cornell University, November 1995, DIMACS, February 1995.

"$\sqrt{2} + \sqrt{3}$: Four Different Views," MIT Math Department, February 2009; East Coast Algebra Day, Northeastern University, April 1997.

"Embedding Linkages in Integer Lattices," Combinatorics Day at Smith, February 1993.

"How to Tangle with a Nested Radical," Williams College, October 1992.

"Elegant Algorithms and Slow Solutions," University of Denver, May 1996, IBM, San Jose, July 1992, Haverford College, May 1992; CUNY, New York, March 1992; University of Cantabria, Santander, Spain, January 1992; Supercomputing Research Center, April 1991; Valley Geometry Seminar, Univ. of Mass., April, 1991.

"Simplification of Nested Radicals," Cornell, February, 1993; Algofest, New England Theory Network, Bristol, RI, April 1992; IBM, Yorktown Heights, June 1991; Purdue University, July 1990, SIAM Annual Meeting (Special Session on Symbolic Computation), July 1990; University of Texas, Austin, January, 1990; Northeastern University, November, 1989, Rensselaer Polytechnic Institute, September, 1989, University of Massachusetts Math Colloquim, September, 1989; AMS Annual Meeting (Special Session On Computational Number Theory), August, 1989; Greater Philadelphia Combinatorics Colloquim, February, 1989.

"Shrinking Lattice Polyhedra," AMS Meeting (Special Session on Computational Algebra), Hoboken, October, 1989.

"Some Remarks on Computing the Square Parts of Integers," MIT Theory of Computation seminar, October, 1988.

"Factoring Polynomials Quickly," IBM Research, Yorktown Heights, August, 1987; University of Washington, July, 1987; University of Warsaw, July, 1987; Sandia Labs, May, 1987.

"Polynomial Decomposition Algorithms," Bonn Workshop on Foundations of Computing, July, 1987; MIT, December, 1986; Cornell University, June, 1986.

"Solvability by Radicals is in Polynomial Time," Math Sciences Institute, Cornell, March 1993; University of Washington, May 1986; MSRI Workshop on Computation in Algebra and Number Theory, October, 1985; Dartmouth College, October, 1984; Williams College, September, 1984; Cornell University, August, 1984; Beijing Computer Institute, June, 1984; University of California, Berkeley, May, 1984; Stanford University, January, 1984; Women in Mathematics Mini-Conference, CUNY, December, 1983; University of Toronto, October, 1983; IBM, Yorktown Heights, April, 1983; Carnegie-Mellon, April, 1983; Bell Labs, January, 1983.

"The Complexity of Polynomial Factorization," Beijing Computer Institute, June, 1984; IBM San Jose, January, 1984; Assoc. for Women in Math, Boston Chapter, October 1982.

"The Parallel Complexity of Certain Algebraic Problems," Beijing Computer Institute, June, 1984.

"Factoring Polynomials over Algebraic Number Fields," Cornell University, August, 1982.

"Primes, Codes and the National Security Agency," Wellesley College, April 1993; Stanford University, October, 1985; Williams College, September, 1984; Academia Sinica, Beijing, June, 1984; Tufts University, February, 1981; Dartmouth College, October, 1980.

"Mapping the Universe," Connecticut Junior Science and Humanities Symposium, March, 1984; Hampshire College Summer Studies in Math, August, 1982.

Conference and Workshop Participation

Organizer and Moderator, "Cybersecurity: Why So Difficult?," breakout session, National Academies of Sciences Annual Meeting, April 2017.

Panelist, "New Platforms of Control (or Someone to Watch Over Me)," Princeton-Fung Global Forum: Can Liberty Survive the Digital Age, Berlin, March 2017.

Panelist, "Cybersecurity: Mathematics and Privacy," AAAS Annual Meeting, February 2017.

Panelist, Cryptographers' Panel, RSA Conference, February 2017.

Panelist, "Promoting Trust in the Evolving Security Landscape," BSA General Counsel Forum, November 2016.

Panelist, "The New Threats: Cyber Security," *The Atlantic's* Fifteen Years Later: Are We Any Safer?, September 2016.

Panelist, "Government Access to Encrypted Data," Microsoft Research Faculty Summit, July 2016.

Moderator, "The Security Economics of Surveillance," Workshop in Economics of Information Security, June 2016.

Panelist, "Why does privacy research need to be Interdisciplinary? How can we incentivize interdisciplinary research? What are the barriers?," Principles and Practices of Privacy Science Workshop, December 2015.

Participant, "Protecting Online Privacy by Enhancing IT Security and EU IT Autonomy," Civil Liberties Justice and Home Affairs Committee and Science and Technology Options Assessment Panel, European Parliament, December 2015.

Panelist, "Going Dark: The Balance between Encryption, Privacy, and Public Safety," Advanced Cyber Security Center, Boston, November, 2015.

Participant, "Global Encryption: Will it Make Us Safer?," East-West Institute, Global Cyberspace Cooperation Summit IV, September 2015.

Session Chair, "Tension between Civil Liberties and Security," Multi Disciplinary Workshop in Cyber Security, School of International Affairs, Columbia University, June 2015.

Panelist, "Security, Surveillance, and Encryption," Threats, Profits, and Security: Today's Cyber Challenges, Fordham University, April 2015 (CLE credit).

Panelist, "Impact of Technological Change on Norms, Policy, and Practice," Secrecy, Surveillance, Privacy, and International Relations, MIT, April 2015.

Panelist, "Privacy Perspective: Society," NITRD National Privacy Research Strategy Workshop, February 2015.

Panelist, "Post Snowden: Implications of the NSA and GCHQ Surveillance Programs Revelations for the PETs community," Privacy Enhancing Technologies Symposium, July 2014.

Panelist, "NSA in Historical and Diplomatic Perspective," The National Security Agency at the Crossroads, University of Texas at Austin, April 2014.

Panelist, "After Snowden: Privacy, Surveillance, & the NSA," SXSW, March 2014.

Discussion Leader, "Identity management: why don't we have it and do we actually need it?" NSF Secure and Trustworthy Computing meeting, November 2012.

Participant, "Cybersecurity and the Future of the Internet," Joint CASBS/CISAC meeting, Stanford University, November 2012.

Participant, "Transparency and Lawful Access," Google Brussels, September 2012.

Guest Scholar, Faculty Workshop: Civilian Cybersecurity Policy for an Age of Globalization,Center on Law and Information Policy, Fordham Law School, April 2012.

Panelist, "On the Rise of Smart Technologies, Surveillance, Privacy, and Ethics,"Fifth International Conference on Computers, Privacy, and Data Protection, Brussels, January 2012.

Panelist, "The Search for Meaningful Trustworthiness," ACSAC, December 2011.

Panelist, "Surveillance and Citizenship," MIT Communications Forum, October 2011.

Panelist, White House launch of National Strategy for Trusted Identities in Cyberspace, April 2011.

Moderator, "Privacy Concerns in Cybersecurity," Cybersecurity: Law, Privacy, and Warfare in a Digital World, Harvard Law School, March 2011.

Participant, "Internet Privacy Workshop: How can Technology Help to Improve Privacy on the Internet?," IAB, W3C, ISOC, and CSAIL, December 2010.

Participant, "No More Secrets: National Security Strategies for a Transparent World," ABA Standing Committee on Law and National Security, Office of the National Counterintelligence Executive, and National Security Forum, June, 2010.

Panelist, "The CIO Roadmap for Data Protection and Privacy," CIO Forum, Department of Homeland Security, March 2010.

Panelist, "Privacy in the Digital World of the Internet, E-Commerce, and Post-9/11 America," ABA Program on Data Privacy, Boston, February 2009 (CLE credit).

Panelist, "Managing Opportunities," CRA-W CAPP-L Workshop, Santa Fe, November 2008.

Moderator and Organizer, "Letting The Cup Overflow: Expanding Your Experiences Outside the Research Lab," Grace Hopper Celebration of Women in Computer Science, October 2008.

Panelist, "Security Risks of the Protect America Act," Modernization of FISA, Georgetown Law School, September 2007.

Panelist, "Government Security, Surveillance and Civil Liberties." ABA National Institue on Computing and the Law, June 2007 (CLE credit).

Panelist, "Engaging Privacy and Information Technology in a Digital Age: Discussion on the findings of the report of the National Research Council (US)," Computers, Freedom, and Privacy, May 2007.

Panelist, "Private Sector Initiatives to Design Technology to Enable (Some) Privileged Uses," Copyright, DRM Technologies, and Consumer Protection meeting, Boalt Hall School of Law, Berkeley, March 2007 (CLE credit).

Session Speaker, "Prime Numbers: New Developments in Ancient Problems," AAAS Annual Meeting, February 2007 (repeated, by invitation, at MAA Mathfest, August 2007).

Panelist, "Security and Privacy," Global Forum 2006, Paris November 2006.

Panelist, "Non-traditional Ways to Advance Your Career," Grace Hopper Celebration of Women in Computer Science, October 2006.

Panelist, "Lawful Intercept: Reconciling Privacy with National Security in an IP-enabled World," VON Fall meeting, September 2006.

Panelist, "Digital Rights Management," Computers, Freedom, and Privacy, 2006

Panelist, "Career Paths Contrasted," CRA-W Career Mentoring Workshop, 2005.

Moderator and Organizer, "National Leadership Opportunities," Grace Hopper Celebration of Women in Computer Science, October 2004.

Panelist, "Managing Career Change," Grace Hopper Celebration of Women in Computer Science, October 2004.

Participant, DTO/DNI Privacy Protection Workshop (series of three one-day meetings), Fall 2004.

Speaker, "Privacy and Civil Liberties Issues in Computing Applications Research and Development" workshop, Computers, Freedom, and Privacy, April 2004.

Speaker, "Who Are You? The Basics of Authentication, Privacy, and Identity Today" tutorial, Computers, Freedom, and Privacy, April 2004.

Participant, "Workshop on Proactive DRM Agenda," American Library Association and School of Information Management, UC Berkeley, January 2003.

Panelist, "Security, Freedom, and Privacy in a Post-September 11 World," Grace Hopper Celebration of Women in Computer Science, Vancouver, October 2002.

Participant, Public Design Workshop, NYU Law School, September 2002.

Participant, DARPA Workshop on e-Authentication, August 2002.

Panelist, "Visual Surveillance" and "Content Analysis" panels, Symposium on Security and Privacy, Zurich November 2001.

Participant, Cybercrime Workshop, Institute for Prospective Technical Studies, Joint Research Center, European Commission, Seville, January 2001.

Organizer, "Achieving Balance," Grace Hopper Celebration of Women in Computer Science, September 2000.

Panelist, "The Brave New World of the Net: Will Policy and Technology Liberate or Enslave Us?," Grace Hopper Celebration of Women in Computer Science, September 2000.

Organizer, "Battling the Crypto Wars," symposium at American Association for the Advancement of Science annual meeting, February 2000.

Panelist, "Cyberspace and Privacy," Stanford Law Review, Stanford, February 2000.

Panelist, "Anonymity on the Internet," ACM Conference on Computer and Communication Security, November 1998.

Panelist, "Conceptual Approaches to Security and Export Control on the Internet," The International Cyberlaw and Business Conference 1998: Conceptual Issues Across Borders, New York County Lawyers' Assocation, April 1998.

Panelist, "Washington Update," RSA Data Security Conference, January, 1998.

Panelist, "What are the Pros and Cons of Cryptography?," International Conference on Privacy, Montreal, September 1997.

Panelist, "Washington Update," RSA Data Security Conference, January, 1996.

Participant, "National Information Infrastructure Forum," Privacy and Security Track, National Institutes of Standards and Technology, February 28 – March 1, 1994.

Participant, "Women in Mathematics Workshop," National Security Agency, November, 1993.

Senior participant in "Individual Rights in the Information Age" workshop, Fourth International Student Pugwash Conference, Princeton University, June 23-29, 1985.

Student participant in "Computers and Society" workshop, Second International Student Pugwash Conference, Yale University, June 15-21, 1981.

GRANTS

PI, Google Research Award, 2017.

co-P.I., NSF Grant: Scholarship Track: Scholarships for Service at WPI, 2015-2019.

P.I., CRA-W/CDC Grant: Discipline-Specific Workship Grant, GREPSEC II, 2015.

P.I., CRA-W/CDC Grant: Discipline-Specific Workship Grant, GREPSEC I, 2013.

P.I., NSF Grant: Certification of Security Protocols, 10/97-4/99.

P.I., Sun Microsystems, Cryptography and Public Policy research, 1997.

P.I., NSF Grant: ISSAC Travel Grant, 8/93-12/94.

P.I., NSF Grant: Algebraic Algorithms, 7/92-12/95.

P.I., NSF Grant: Algebraic Algorithms and Computational Complexity, 7/88-12/89.

MSRI Postdoctoral Fellowship, 9/85-12/85.

P.I., NSF Grant: Algebraic Algorithms and Computational Complexity, 5/84-11/86.

STUDENTS

Oshani Seneviratne, MIT, member, PhD committee, 2014.

Lewis McCarthy, UMass Amherst, MS, 1999.