

Susan Landau

Department of Computer Science Harvard University
33 Oxford Street
Cambridge MA 02138
413-259-2018
susan.landau@privacyink.org
<http://privacyink.org/>

EDUCATION

- 1983** Ph.D., MIT.
- 1979** M.S., Cornell University.
- 1976** B.A., Princeton University.
- 1972** Bronx High School of Science.

EMPLOYMENT

- 2011-2012** Visiting Scholar, Department of Computer Science, Harvard University.
- 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 (1995-1996, Visiting Associate Professor, Cornell University).
- 1989-1991** Visiting Assistant Professor, Computer Science Department, University of Massachusetts (on leave from Wesleyan University).
- 1983 - 1991** Assistant Professor of Computer Science, Math Dept., Wesleyan University (Fall 1988, postdoctoral 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, Advisory Board, National Cyber Security Hall of Fame, 2012-present.

member, Computer Science and Telecommunications Board, National Research Council, 2010-present.

member, Advisory Committee, National Science Foundation Directorate for Computer and Information Science and Engineering, 2009-present.

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

member, ACM-W Council Executive Council, 2009-present.

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:

section board member, Privacy and Security Viewpoints column, *Communications of the ACM*, 2007-present.

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

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

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

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

Program Committees and Related Work:

program committee member, New Security Paradigms Workshop, 2012.

committee member, Usability, Security, and Privacy of Computer Systems: a Workshop, National Research Council, 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.

Security and Privacy session, Massachusetts Telecommunications Conference (co-chair), 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):

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

chair (2006-2011), co-chair (2005-2006), Athena Lecturer Selection Committee.

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

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

moderator (and organizer), ResearchHers, a mailing list for women computer science researchers (organized under the auspices of CRA-W and the Anita Borg Institute for Women and Technology), 2004 - present.

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

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

AWARDS

ACM Fellow, 2011.

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

ACM Distinguished Engineer, 2006.

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

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

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

NSF Mathematical Sciences Postdoctoral Fellowship, 1988.

GOVERNMENT BRIEFINGS (recent)

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 Sopha 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:

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

Early 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.

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

Privacy on the Line attracted international attention. I was on NPR three times to discuss the book, and Diffie and I were on 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 short reply), in Stewart Baker, Harvey Rishikof, and Bernie Horowitz, eds., *Patriot Debates II: Contemporary Issues in National Security*, American Bar Association, to appear.
- 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:

- 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, “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.

Journal Publications:

- C. Landwehr, D. Boneh, J. Mitchell, S. Bellovin, S. Landau, and M. Lesk, "Privacy and Cybersecurity: The Next 100 Years," to appear, *Proceedings of the IEEE*.
- 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. 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, "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. 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, *CACM* 50, p. 128, Dec, 2007.
- S. Landau, "Security, Wiretapping, and the Internet," *IEEE Security and Privacy*, Vol. 3, No. 6 November/December 2005, pp. 26-33.
- 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, "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.
- 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.

- W. Diffie and S. Landau, "September 11th Did Not Change Cryptography Policy," *Notices of the American Mathematical Society*, April 2002, pp. 450-454.
- S. Landau, "Designing Cryptography for the New Century," *Communications of the Association for Computing Machinery*, 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 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, "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, "Security, Liberty, and Electronic Communications," (invited talk), in Matt Franklin (ed.), *Advances in Cryptology: CRYPTO 2004*, Springer Verlag, pp. 355-372.
- 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.

Conference Proceedings (which did not also appear in journals):

- S. Landau and T. Moore, "Economic Tussles in Federated Identity Management," Workshop on Economics of Information Security, 2011.
- 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, "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:

- 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/ED2881.6; Who are You?," introductory editor's 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:

- S. Landau, "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*, 9 September 1979, Section X, p.7.

Other Publications:

- S. Landau, “Clipper and Capstone,” “Cryptography,” and “Digital signatures,” entries in W. Staples, ed., *Encyclopedia 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 Anyway?,” 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:

- 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.ita.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

Radio Interviews:

- 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 (nationally-syndicated), February 2, 1998.

Television Appearances:

Great Decisions, PBS, to appear, multiple stations, January 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.

Selected Invited Talks (recent):

“Privacy: It’s All in the Use Case,” Invited Essayist, Advanced Computer Security Applications Confernece, December 2011.
“Envisioning Cybersecurity Research — and Education — in New England,” New England Summit on Cyber Security, Boston University, June 2011.
“Cybersecurity: Asking the Right Questions,” Distinguished Lecture, AT&T, May 2011.
“A Computer Scientist Goes to Washington: How to Be Effective When Facts are 10% of the Equation,” SIGCSE Keynote, March 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,” Invited Talk, Large Installation System Administration Conference (LISA), December 2011; 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,” 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.
“Bits and Bytes: Explaining Communications Security (and Insecurity) in Washington and Brussels,” Invited Talk, Grace Hopper Celebration of Women in Computer Science, October 2009.

- “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.
- “Internet Surveillance: Building our own Trojan Horse,” Invited Talk, USENIX, June 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.
- “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.
- “COMSEC v. COMINT, and is Terrorism the Right Question?,” Ecole Polytechnique Fédérale Lausanne, July 2007.
- “DRM: A Different Approach,” Harvard CRCS seminar, November 2006.
- “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.

Conference and Workshop Participation:

- 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,” T 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 Institute 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, “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’ Association, April 1998.

Panelist, “Washington Update,” RSA Data Security Conference, January, 1998.

Panelist, “What are the Pros and Cons of Cryptography?,” International Conference on Privacy, 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:

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

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.