Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the *Economist*. He is the *New York Times* best-selling author of 14 books—including *Click Here to Kill Everybody*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Professional Experience

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back, WW Norton & Co., 2022.

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Co., 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Co,, 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

J. Penney and B. Schneier, “Platforms, Encryption, and the CFAA: The Case of *WhatsApp v. NSO Group*,” *Berkeley Technology Law Journal*, v. 36, n. 1, 2021.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, “Bugs in our Pockets: The Risks of Client-Side Scanning,” arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, “Machine Learning Featurizations for AI Hacking of Political Systems,” arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, “Rechanneling Beliefs: How Information Flows Hinder or Help Democracy,” Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, “The Coming AI Hackers,” Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, “Chinese Technology Platforms Operating in the United States: Assessing the Threat,” *Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law*, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, "Legal Risks of Adversarial Machine Learning Research," arXiv:2006.16179.

N. Kim, T. Herr, and B. Schneier, "The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain," *Atlantic Council*, June 2020.

K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships," *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, "Weaponizing Digital Health Intelligence," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, "Politics of Adversarial Machine Learning," *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, "Superheroes on Screen: Real Life Lessons for Security Debates," *Security Journal*, 2019.

H. Farrell, B. Schneier, "Common-Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7, October 2018.

T. Herr, B. Schneier, and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," July 2017 (revised October 2017).

O. S. Kerr, B. Schneier, "Encryption Workarounds," March 2017.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, "Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure'?," *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity,* November 2015.

B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, "Surreptitiously Weakening Cryptographic Systems," *Cryptology ePrint Archive* Report 2015/097, 2015.

A. Czeskis, D. Mah, O. Sandoval, I. Smith, K. Koscher, J. Appelbaum, T. Kohno, B. Schneier, “DeadDrop/Strongbox Security Assessment,” *UW Computer Science and Engineering Technical Report #13-08-02*, August 8, 2013.

B. Schneier, “Schneier on Security: Privacy and Control,” *Journal of Privacy and Confidentiality*, v.2, n.1, pp. 3–4, 2010.

N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, J. Walker, “The Skein Hash Function Family,” version 1.2, September 15, 2009.

M. Bellare, T. Kohno, S. Lucks, N. Ferguson, B. Schneier, D. Whiting, J. Callas, J. Walker, “Provable Security Support for the Skein Hash Family,” April 29, 2009.

A. Czeskis, D. J. St. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, “Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications,” 3rd Usenix Workshop on Hot Topics in Security, 2008.

B. Schneier, “The Psychology of Security,” *AFRICACRYPT 2008, LNCS 5023*, Springer-Verlag, 2008, pp. 50–79.

R. Anderson and B. Schneier, “Economics of Information Security,” *IEEE Security and Privacy* 3 (1), 2005, pp. 12–13.

J. Kelsey and B. Schneier, “Second Preimages on n-bit Hash Functions for Much Less than 2n Work,” *Advances in Cryptology: EUROCRYPT 2005 Proceedings*, Springer-Verlag, 2005, pp. 474–490.

D. Whiting, B. Schneier, S. Lucks, and F. Muller, “Phelix: Fast Encryption and Authentication in a Single Cryptographic Primitive,” *ECRYPT Stream Cipher Project Report* 2005/027.

N. Ferguson and B. Schneier, “A Cryptographic Evaluation of IPsec,” December 2003.

N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, “Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive,” *Proceedings of Fast Software Encryption 2003*, pp. 345–362.

K. Jallad, J. Katz, and B. Schneier, “Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG,” *Information Security Conference 2002 Proceedings*, Springer-Verlag, 2002.

B. Schneier, “Inside Risks 129: Cyber Underwriters Lab?,” *Communications of the ACM*, vol 44, n 4, Apr 2001.

N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting, “Improved Cryptanalysis of Rijndael,” *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 213–230.

J. Kelsey, T. Kohno, and B. Schneier, “Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent,” *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 7–93.

J. Kelsey and B. Schneier, "The Street Performer Protocol and Digital Copyrights," *First Monday*, v. 45, n. 6 (June 2001).

J. Katz and B. Schneier, "A Chosen Ciphertext Attack against Several E-Mail Encryption Protocols," 9th USENIX Security Symposium, 2000.

B. Schneier, "The Fallacy of Trusted Client Software" (Cryptorhythms column), *Information Security Magazine*, August 2000.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, "The Twofish Team's Final Comments on AES Selection," May 15, 2000.

D. Whiting, B. Schneier, S. Bellovin, "AES Key Agility Issues in High-Speed IPsec Implementations," May 15, 2000.

B. Schneier, "The Process of Security," *Information Security Magazine*, April 2000.

N. Ferguson, B. Schneier, and D. Wagner, "Security Weaknesses in Maurer-Like Randomized Stream Ciphers," *Fifth Australasian Conference on Information Security and Privacy* (ACISP 2000), Springer-Verlag, 2000, pp. 234–241.

J. Kelsey and B. Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 169–185.

T. Kohno, J. Kelsey, and B. Schneier, "Preliminary Cryptanalysis of Reduced-Round Serpent," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 195–211.

B. Schneier and D. Whiting, "A Performance Comparison of the Five AES Finalists," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 123–135.

N. Ferguson, J. Kelsey, B. Schneier, D. Whiting, "A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish," Twofish Technical Report #6, February 14, 2000.

C. Ellison and B. Schneier, "Inside Risks 116: Risks of PKI: Electronic Commerce," *Communications of the ACM*, vol 43, n 2, Feb 2000.

C. Ellison and B. Schneier, "Inside Risks 115: Risks of PKI: Secure E-Mail," *Communications of the ACM*, vol 43, n 1, Jan 2000.

C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure," *Computer Security Journal*, v 16, n 1, 2000, pp. 1–7.

C. Ellison, C. Hall, R. Milbert, and B. Schneier, "Protecting Secret Keys with Personal Entropy," *Future Generation Computer Systems*, v. 16, 2000, pp. 311–318.

B. Schneier, "Self-Study Course in Block Cipher Cryptanalysis," *Cryptologia*, v.24, n.1, Jan 2000, pp. 18–34.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *Journal of Computer Security*, v. 8, n. 2–3, 2000, pp. 141–158.

J. Kelsey and B. Schneier, "Key-Schedule Cryptanalysis of DEAL," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 118–134.

J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 13–33.

B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, v. 24, n. 12, Dec 1999, pp. 21–29.

B. Schneier, "The 1999 Crypto Year-in-Review," *Information Security Magazine*, January 1999.

B. Schneier, "Security in the Real World: How to Evaluate Security Technology," *Computer Security Journal*, v 15, n 4, 1999, pp. 1–14.

B. Schneier, "A Plea for Simplicity," *Information Security Magazine*, November 1999.

B. Schneier and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)," *CQRE '99*, Springer-Verlag, 1999, pp. 192–203.

B. Schneier, "Inside Risks 112: Risks of Relying on Cryptography," *Communications of the ACM*, vol 42, n 10, Oct 1999.

B. Schneier, "Inside Risks 111: The Trojan Horse Race," *Communications of the ACM*, vol 42, n 9, September 1999.

B. Schneier, "International Cryptography," *Information Security Magazine*, September 1999.

J. Kelsey and B. Schneier, "Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs," *Second International Workshop on the Recent Advances in Intrusion Detection* (RAID '99), September 1999.

B. Schneier, "Inside Risks 110: Biometrics: Uses and Abuses," *Communications of the ACM*, vol 42, n 8, August 1999.

C. Hall, I. Goldberg, and B. Schneier, "Reaction Attacks Against Several Public-Key Cryptosystems," *Proceedings of Information and Communication Security*, ICICS'99, Springer-Verlag, 1999, pp. 2–12.

B. Schneier and A Shostack, "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 175–185.

J. Kelsey and B. Schneier, "Authenticating Secure Tokens Using Slow Memory Access," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 101–106.

D. Whiting, J. Kelsey, B. Schneier, D. Wagner, N. Ferguson, and C. Hall, "Further Observations on the Key Schedule of Twofish," Twofish Technical Report #4, March 16, 1999.

E. Biham, A. Biryukov, N. Ferguson, L. Knudsen, B. Schneier, and A. Shamir, "Cryptanalysis of Magenta," Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "New Results on the Twofish Encryption Algorithm," Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions," Second AES Candidate Conference, April 1999.

D. Whiting, N. Ferguson, and B. Schneier, "Cryptanalysis of FROG," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Key Schedule Weakness in SAFER+," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications Against RC5P and M6, Fast Software Encryption," *Sixth International Workshop Proceedings* (March 1999), Springer-Verlag, 1999, pp. 139–155.

B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics," *ACM Transactions on Information and System Security*, v. 2, n. 2, May 1999, pp. 159–176.

B. Schneier, "The 1998 Crypto Year-in-Review," *Information Security Magazine*, January 1999.

J. Riordan and B. Schneier, "A Certified E-Mail Protocol with No Trusted Third Party," *13th Annual Computer Security Applications Conference*, ACM Press, December 1998, pp. 347–351.

B. Schneier, "Cryptographic Design Vulnerabilities," *IEEE Computer*, v. 31, n. 9, Sep 1998, pp. 29–33.

B. Schneier and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," *Proceedings of the 5th ACM Conference on Communications and Computer Security*, ACM Press, November 1998, pp. 132–141.

J. Kelsey and B. Schneier, "The Street Performer Protocol," *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.

B. Schneier, "Scrambled Message," *Information Security Magazine*, October 1998.

C. Salter, O.S. Saydjari, B. Schneier, and J. Wallner, "Towards a Secure System Engineering Methodology," *New Security Paradigms Workshop*, September 1998, pp. 2–10.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *ESORICS '98 Proceedings*, Springer-Verlag, September 1998, pp. 97–110.

C. Hall, J. Kelsey, V. Rijmen, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 319–338.

D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 296–305.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, "On the Twofish Key Schedule," Fifth *Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 27–42.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Building Pseudo-Random Functions from Pseudo-Random Permutations," *Advances in Cryptology—CRYPTO '98 Proceedings*, Springer-Verlag, August 98, pp. 370–389.

J. Riordan and B. Schneier, "Environmental Key Generation towards Clueless Agents," *Mobile Agents and Security*, G. Vigna, ed., Springer-Verlag, 1998, pp. 15–24.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED (Extended Abstract)," *Financial Cryptography '98*, Springer-Verlag, 1998, 309–310.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher," 15 June 1998.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1998), Springer-Verlag, 1998, pp. 168–188.

D. Coppersmith, D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of TwoPrime," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1988), Springer-Verlag, 1998, 32–48.

B. Schneier and J. Kelsey, "Cryptographic Support for Secure Logs on Untrusted Machines," *The Seventh USENIX Security Symposium Proceedings*, USENIX Press, January 1998, pp. 53–62.

J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure Applications of Low-Entropy Keys," *1997 Information Security Workshop* (ISW'97), Proceedings (September 1997), Springer-Verlag, 1998, pp. 121–134.

B. Schneier and C. Hall, "An Improved E-mail Security Protocol," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 232–238.

C. Hall and B. Schneier, "Remote Electronic Gambling," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 227–230.

J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," *ICICS '97 Proceedings*, Springer-Verlag, November 1997, pp. 233–246.

D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm," *Advances in Cryptology—CRYPTO '97 Proceedings*, Springer-Verlag, August 1997, pp. 526–537.

N. Ferguson and B. Schneier, "Cryptanalysis of Akelarre," Fourth Annual Workshop on Selected Areas in Cryptography, August 1997, pp. 201–212.

H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," *World Wide Web Journal*, v.2, n.3, 1997, pp. 241–257.

J. Kelsey and B. Schneier, "Conditional Purchase Orders," *4th ACM Conference on Computer and Communications Security*, ACM Press, April 1997, pp. 117–124.

J. Kelsey, B. Schneier, and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," *Security Protocols, International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

B. Schneier and J. Kelsey, "Remote Auditing of Software Outputs Using a Trusted Coprocessor," *Journal of Future Generation Computer Systems*, v.13, n.1, 1997, pp. 9–18.

B. Schneier, "Why Cryptography is Harder than it Looks," *Information Security Bulletin*, v. 2, n. 2, March 1997, pp. 31–36.

B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor," *Fast Software Encryption, Fourth International Workshop Proceedings* (January 1997), Springer-Verlag, 1997, pp. 242–259.

B. Schneier, "Cryptography, Security, and the Future," *Communications of the ACM*, v. 40, n. 1, January 1997, p. 138.

J. Kelsey, B. Schneier, and C. Hall, "An Authenticated Camera," *12th Annual Computer Security Applications Conference*, ACM Press, December 1996, pp. 24–30.

B. Schneier and J. Kelsey, "A Peer-to-Peer Software Metering System," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 279–286.

D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 29–40.

B. Schneier, J. Kelsey, and J. Walker, "Distributed Proctoring," *ESORICS 96 Proceedings*, Springer-Verlag, September 1996, pp. 172–182.

J. Kelsey and B. Schneier, "Authenticating Outputs of Computer Software Using a Cryptographic Coprocessor," *Proceedings 1996 CARDIS*, September 1996, pp. 11–24.

J. Kelsey, B. Schneier, and D. Wagner, “Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES,” *Advances in Cryptology—CRYPTO ’96 Proceedings*, Springer-Verlag, August 1996, pp. 237–251.

B. Schneier and J. Kelsey, “Automatic Event Stream Notarization Using Digital Signatures,” *Security Protocols, International Workshop April 1996 Proceedings*, Springer-Verlag, 1997, pp. 155–169.

B. Schneier and J. Kelsey, “Unbalanced Feistel Networks and Block Cipher Design,” *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121–144.

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, “Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security,” January 1996.

M. Jones and B. Schneier, “Securing the World Wide Web: Smart Tokens and their Implementation,” *Proceedings of the Fourth International World Wide Web Conference*, December 1995, pp. 397–409.

B. Schneier, “Blowfish—One Year Later,” *Dr. Dobb’s Journal*, September 1995.

M. Blaze and B. Schneier, “The MacGuffin Block Cipher Algorithm,” *Fast Software Encryption, Second International Workshop Proceedings* (December 1994), Springer-Verlag, 1995, pp. 97–110.

B. Schneier, “The GOST Encryption Algorithm,” *Dr. Dobb’s Journal*, v. 20, n. 1, January 1995, pp. 123–124.

B. Schneier, “A Primer on Authentication and Digital Signatures,” *Computer Security Journal*, v. 10, n. 2, 1994, pp. 38–40.

B. Schneier, “Designing Encryption Algorithms for Real People,” *Proceedings of the 1994 ACM SIGSAC New Security Paradigms Workshop*, IEEE Computer Society Press, August 1994, pp. 63–71.

B. Schneier, “The Blowfish Encryption Algorithm,” *Dr. Dobb’s Journal*, v. 19, n. 4, April 1994, pp. 38–40.

B. Schneier, “Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish),” *Fast Software Encryption, Cambridge Security Workshop Proceedings* (December 1993), Springer-Verlag, 1994, pp. 191–204.

B. Schneier, “One-Way Hash Functions,” *Dr. Dobb’s Journal*, v. 16, n. 9, September 1991, pp. 148–151.

Selected Awards

Schneier on Security listed as one of the Cyber Security Blogs You Need to See, Focus Training, February 2017.

Business Leader in Cybersecurity Award from Boston Global Forum, December 2015.

Named as one of the 20 top security influencers by *eSecurity Planet*, June 2015.

EPIC Lifetime Achievement Award, June 2015.

Named as one of the top ten information security bloggers of 2014 by the ISO 27001 and ISO 22301 blog, December 2014.

Named as an industry pioneer in information security by *SC Magazine*, December 2014.

Berkman Fellow at the Berkman Center for Internet and Society at Harvard University, 2013–2015 academic years.

Named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013.

Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011.

CSO Compass Award, May 2010.

Named as one of the top 25 most influential people in the security industry by *Security* magazine, December 2008

Inducted into the Infosecurity Europe Hall of Fame, April 2008.

Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award, January 2008.

Electronic Frontier Foundation (EFF) Pioneer Award, March 2007.

Dr. Dobb's Journal Excellence in Programming Award, April 2006.

Named as one of the top five influential IT security thinkers by *SC* magazine, December 2005.

Infoworld CTO 25 Award, April 2005.

Secrets and Lies won a Productivity Award in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.

Legislative Testimony

Letter to the US Senate Judiciary Committee in support of S.2992 and S.2710, January 31, 2022.

Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection, hearing on “Securing Consumers’ Credit Data in the Age of Digital Commerce,” November 1, 2017.

Testimony at the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology, and the Subcommittee on Commerce, Manufacturing, and Trade, hearing on “Understanding the Role of Connected Devices in Recent Cyber Attacks,” November 16, 2016.

Testimony before the U.S. Senate Judiciary Committee, hearing on “Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns,” May 8, 2007.

Testimony at the U.K. House of Lords Science and Technology Committee inquiry into “Personal Internet Security,” February 21, 2007.

Testimony before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development, hearing on “Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk,” June 25, 2003.

Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, Subcommittee on Science, Technology, and Space, hearing on Internet Security, July 16, 2001.

Published Articles

“Big Tech Isn’t Prepared for A.I.’s Next Chapter,” *Slate*, May 30, 2023.

“Rethinking Democracy for the Age of AI,” *Cyberscoop*, May 10, 2023.

“Can We Build Trustworthy AI?,” *Gizmodo*, May 4, 2023.

“Just Wait Until Trump Is a Chatbot,” *The Atlantic*, April 28, 2023.

“How Artificial Intelligence Can Aid Democracy,” *Slate*, April 21, 2023.

“Brace Yourself for a Tidal Wave of ChatGPT Email Scams,” *Wired*, April 4, 2023.

“How AI Could Write Our Laws,” *MIT Technology Review*, March 14, 2023.

“Why the U.S. Should Not Ban TikTok,” *Foreign Policy*, February 23, 2023.

“Everything Is Hackable,” *Slate*, February 10, 2023.

"We Don't Need to Reinvent Our Democracy to Save It from AI," *Harvard Kennedy School Belfer Center*, February 9, 2023.

"The Big Idea: Bruce Schneier," *Whatever*, February 7, 2023.

"Opinion: What Peter Thiel and the 'Pudding Guy' revealed," *CNN*, February 7, 2023.

"How ChatGPT Hijacks Democracy," *New York Times*, January 15, 2023.

"How to Decarbonize Crypto," *Atlantic*, December 6, 2022.

"Centralized vs. Decentralized Data Systems—Which Choice Is Best?" *VentureBeat*, September 12, 2022.

"NIST's Post-Quantum Cryptography Standards Competition," *IEEE Security & Privacy*, August 7, 2022.

"When Corporate Interests and International Cyber Agreements Collide," *Cipher Brief*, May 5, 2022.

"Why Vaccine Cards Are So Easily Forged," *The Atlantic*, March 8, 2022.

"Letter to the US Senate Judiciary Committee on App Stores," January 31, 2022.

"Robot Hacking Games," *IEEE Security & Privacy*, January 1, 2022.

"How to Cut Down on Ransomware Attacks Without Banning Bitcoin," *Slate*, June 17, 2021.

"Hacked Drones and Busted Logistics Are the Cyber Future of Warfare," *Brookings TechStream*, June 5, 2021.

"Russia's Hacking Success Shows How Vulnerable the Cloud Is," *Foreign Policy*, May 24, 2021.

"'Grassroots' Bot Campaigns Are Coming. Governments Don't Have a Plan to Stop Them.," *The Washington Post*, May 20, 2021.

"Hackers Used to Be Humans. Soon, AIs Will Hack Humanity," *Wired*, April 19, 2021.

"Bitcoin's Greatest Feature Is Also Its Existential Threat," *Wired*, March 9, 2021.

"Illuminating SolarStorm: Implications for National Strategy and Policy," *Aspen Institute*, March 04, 2021.

"Why Was SolarWinds So Vulnerable to a Hack?" *New York Times*, February 23, 2021.

"The Government Will Guard Biden's Peloton from Hackers. What About the Rest of Us?," *The Washington Post*, February 2, 2021.

"The Solarwinds Hack Is Stunning. Here's What Should Be Done," *CNN*, January 5, 2021.

"Audio: Firewalls Don't Stop Dragons Podcast," *Firewalls Don't Stop Dragons*, December 28, 2020.

"Audio: The Hack by Russia Is Huge. Here's Why It Matters.," *MPR News*, December 28, 2020.

"Review of Data and Goliath (German)," *Nerdhalla*, December 27, 2020.

"Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?," *LA Times*, December 24, 2020.

"Video: AshbrookLIVE #14 – Bruce Schneier," *AshbrookLIVE*, December 24, 2020.

"Audio: Full Disclosure with Bruce Schneier," *BarCode*, December 20, 2020.

"Audio: How Your Digital Footprint Makes You the Product," *TechSequences*, December 16, 2020.

"Video: Hack in the Box Security Conference Keynote Interview," *Hack In The Box Security Conference*, December 3, 2020.

"Video: Election Security: Securing the Vote While Securing the System," *The Legal Edition*, November 19, 2020.

"#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier," *Infosecurity*, November 18, 2020.

"Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair," *Pioneer Institute*, October 13, 2020.

"Audio: We Live in a Security and Privacy World that Science Fiction Didn't Predict," *OWASP PDX Podcast*, October 4, 2020.

"How Amazon and Walmart Could Fix IoT Security," *Data Breach Today*, June 26, 2020.

"The Cyberflâneur #29: Bruce Schneier," *The Syllabus*, June 16, 2020.

"Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series," *Blockchain Rules Podcast*, June 16, 2020.

"Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy," *Policy Punchline*, June 2, 2020.

"Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»," *Open*, June 2, 2020.

"Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World," *Policy Punchline*, May 29, 2020.

"Audio: Bruce Schneier on Truth, Reality, and Contact Tracing," *Reality 2.0*, May 27, 2020.

"Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas," *Cyber Cyber Cyber Cyber*, May 19, 2020.

"The Public Good Requires Private Data," *Foreign Policy*, May 16, 2020.

"How Hackers and Spies Could Sabotage the Coronavirus Fight," *Foreign Policy*, February 28, 2020.

"Technologists vs. Policy Makers," *IEEE Security & Privacy*, January/February 2020.

"We're Banning Facial Recognition. We're Missing the Point.," *The New York Times*, January 20, 2020.

"China Isn't the Only Problem With 5G," *Foreign Policy*, January 10, 2020.

"Bots Are Destroying Political Discourse As We Know It," *The Atlantic*, January 7, 2020.

"We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It," *World Economic Forum*, November 12, 2019.

"Every Part of the Supply Chain Can Be Attacked," *The New York Times*, September 25, 2019.

"The Real Threat from China Isn't 'Spy Trains,'" *CNN*, September 21, 2019.

"What Digital Nerds and Bio Geeks Have to Worry About," *CNN*, September 13, 2019.

"The Myth of Consumer Security," *Lawfare*, August 26, 2019.

"8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, August 12, 2019.

"Attorney General William Barr on Encryption Policy," *Lawfare*, July 23, 2019.

"We Must Prepare for the Next Pandemic," *The New York Times*, June 17, 2019.

"AI Has Made Video Surveillance Automated and Terrifying," *Motherboard*, June 13, 2019.

"AI Can Thrive in Open Societies," *Foreign Policy*, June 13, 2019.

"When Fake News Comes to Academia," *Lawfare*, May 24, 2019.

"Democracy's Dilemma," *Boston Review*, May 15, 2019.

"Russia's Attacks on Our Democratic Systems Call for Diverse Countermeasures," *The Hill*, May 7, 2019.

"Toward an Information Operations Kill Chain," *Lawfare*, April 24, 2019.

"A New Privacy Constitution for Facebook," *OneZero*, March 8, 2019.

"Cybersecurity for the Public Interest," *IEEE Security & Privacy*, January/February 2019.

"There's No Good Reason to Trust Blockchain Technology," *Wired*, February 6, 2019.

"The Public-Interest Technologist Track at the RSA Conference," *RSA Conference Blogs*, January 29, 2019.

"Defending Democratic Mechanisms and Institutions against Information Attacks," *Defusing Disinfo*, January 28, 2019.

"Evaluating the GCHQ Exceptional Access Proposal," *Lawfare*, January 17, 2019.

"Machine Learning Will Transform How We Detect Software Vulnerabilities," *SecurityIntelligence*, December 18, 2018.

"The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia," *Motherboard*, November 19, 2018.

"Surveillance Kills Freedom By Killing Experimentation," *Wired*, November 16, 2018.

"Information Attacks on Democracies," *Lawfare*, November 15, 2018.

"We Need Stronger Cybersecurity Laws for the Internet of Things," *CNN*, November 9, 2018.

"Nobody's Cellphone Is Really That Secure," *The Atlantic*, October 26, 2018.

"Internet Hacking Is About to Get Much Worse," *New York Times*, October 11, 2018.

"Cryptography after the Aliens Land," *IEEE Security & Privacy*, September/October 2018.

"Don't Fear the TSA Cutting Airport Security. Be Glad That They're Talking about It," *Washington Post*, August 17, 2018.

"Censorship in the Age of Large Cloud Providers," *Lawfare*, June 7, 2018.

"Why the FBI Wants You to Reboot Your Router — and Why That Won't Be Enough Next Time," *The Washington Post*, June 6, 2018.

"Data Protection Laws Are Shining a Needed Light on a Secretive Industry," *The Guardian*, June 1, 2018.

"What 'Efail' Tells Us About Email Vulnerabilities and Disclosure," *Lawfare*, May 24, 2018.

"Banning Chinese Phones Won't Fix Security Problems with Our Electronic Supply Chain," *The Washington Post*, May 8, 2018.

"American Elections Are Too Easy to Hack. We Must Take Action Now," *The Guardian*, April 18, 2018.

"It's Not Just Facebook. Thousands of Companies are Spying on You," *CNN*, March 26, 2018.

“Artificial Intelligence and the Attack/Defense Balance,” *IEEE Security & Privacy*, March/April 2018.

“Can Consumers’ Online Data Be Protected?,” *CQ Researcher*, February 9, 2018.

“How to Fight Mass Surveillance Even Though Congress Just Reauthorized It,” *The Washington Post*, January 25, 2018.

“The New Way Your Computer Can Be Attacked,” *The Atlantic*, January 22, 2018.

“The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse,” *CNN*, January 5, 2018.

“How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You,” *The Washington Post*, November 27, 2017.

“Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection,” , November 1, 2017.

“Don’t Waste Your Breath Complaining to Equifax about Data Breach ,” *CNN*, September 11, 2017.

“IoT Security: What’s Plan B?,” *IEEE Security & Privacy*, September/October 2017.

“‘Twitter and Tear Gas’ Looks at How Protest Is Fueled and Crushed by the Internet,” *Motherboard*, July 11, 2017.

“Why the NSA Makes Us More Vulnerable to Cyberattacks,” *Foreign Affairs*, May 30, 2017.

“Who Are the Shadow Brokers?,” *The Atlantic*, May 23, 2017.

“What Happens When Your Car Gets Hacked?,” *The New York Times*, May 19, 2017.

“Why Extending Laptop Ban Makes No Sense,” *CNN*, May 16, 2017.

“The Next Ransomware Attack Will Be Worse than WannaCry,” *The Washington Post*, May 16, 2017.

“Three Lines of Defense against Ransomware Attacks,” *New York Daily News*, May 15, 2017.

“Online Voting Won’t Save Democracy,” *The Atlantic*, May 10, 2017.

“Who Is Publishing NSA and CIA Secrets, and Why?,” *Lawfare*, April 27, 2017.

“The Quick vs the Strong: Commentary on Cory Doctorow’s *Walkaway*,” *Crooked Timber*, April 26, 2017.

“Infrastructure Vulnerabilities Make Surveillance Easy,” *Al Jazeera*, April 11, 2017.

“Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress,” *The Guardian*, March 30, 2017.

“Puzzling out TSA’s Laptop Travel Ban,” *CNN*, March 22, 2017.

“Security Orchestration for an Uncertain World,” *SecurityIntelligence*, March 21, 2017.

“How to Keep Your Private Conversations Private for Real,” *The Washington Post*, March 8, 2017.

“Botnets of Things,” *MIT Technology Review*, March/April 2017.

“Click Here to Kill Everyone,” *New York Magazine*, January 27, 2017.

“Why Proving the Source of a Cyberattack is So Damn Difficult,” *CNN*, January 5, 2017.

“Class Breaks,” *Edge*, December 30, 2016.

“U.S. Elections Are a Mess, Even Though There’s No Evidence This One Was Hacked,” *The Washington Post*, November 23, 2016.

“Testimony at the U.S. House of Representatives Joint Hearing ‘Understanding the Role of Connected Devices in Recent Cyber Attacks,’” November 16, 2016.

“American Elections Will Be Hacked,” *The New York Times*, November 9, 2016.

“Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations.,” *The Washington Post*, November 3, 2016.

“Lessons From the Dyn DDoS Attack,” *SecurityIntelligence*, November 1, 2016.

“Cybersecurity Issues for the Next Administration,” *Time*, October 13, 2016.

“We Need to Save the Internet from the Internet of Things,” *Motherboard*, October 6, 2016.

“How Long Until Hackers Start Faking Leaked Documents?,” *The Atlantic*, September 13, 2016.

“Someone Is Learning How to Take Down the Internet,” *Lawfare*, September 13, 2016.

“Stop Trying to Fix the User,” *IEEE Security & Privacy*, September/October 2016.

“New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked,” *Vox*, August 24, 2016.

“Hackers Are Putting U.S. Election at Risk,” *CNN*, July 28, 2016.

“By November, Russian Hackers Could Target Voting Machines,” *The Washington Post*, July 27, 2016.

“The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters,” *Motherboard*, July 25, 2016.

"Credential Stealing as Attack Vector," *Xconomy*, April 20, 2016.

"The Value of Encryption," *The Ripon Forum*, April 2016.

"Can You Trust IRS to Keep Your Tax Data Secure?," *CNN*, April 13, 2016.

"Your iPhone Just Got Less Secure. Blame the FBI.," *The Washington Post*, March 29, 2016.

"Cryptography Is Harder Than It Looks," *IEEE Security & Privacy*, January/February 2016.

"Data Is a Toxic Asset, So Why Not Throw It Out?," *CNN*, March 1, 2016.

"A 'Key' for Encryption, Even for Good Reasons, Weakens Security," *The New York Times Room for Debate*, February 23, 2016.

"Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case," *The Washington Post*, February 18, 2016.

"Candidates Won't Hesitate to Use Manipulative Advertising to Score Votes," *The Guardian*, February 4, 2016.

"The Internet Of Things Will Be The World's Biggest Robot," *Forbes*, February 2, 2016.

"Security vs. Surveillance," *Don't Panic: Making Progress on the 'Going Dark' Debate*, February 1, 2016.

"When Hacking Could Enable Murder," *CNN*, January 26, 2016.

"How an Overreaction to Terrorism Can Hurt Cybersecurity," *MIT Technology Review*, January 25, 2016.

"The Internet of Things That Talk About You Behind Your Back," *Motherboard*, January 8, 2016.

"The Risks—and Benefits—of Letting Algorithms Judge Us," *CNN*, January 6, 2016.

"How the Internet of Things Limits Consumer Choice," *The Atlantic*, December 24, 2015.

"Can Laws Keep Up with Tech World?," *CNN*, December 21, 2015.

"The Automation of Reputation," *Edge.org*, November 5, 2015.

"The Rise of Political Doxing," *Motherboard*, October 28, 2015.

"Face Facts about Internet Security," *CNN*, October 23, 2015.

"The Era Of Automatic Facial Recognition And Surveillance Is Here, *Forbes*, September 29, 2015.

"Stealing Fingerprints," *Motherboard*, September 29, 2015.

"VW Scandal Could Just Be the Beginning," *CNN*, September 28, 2015.

"Living in Code Yellow," *Fusion*, September 22, 2015.

"Hacking Team, Computer Vulnerabilities, and the NSA," *Georgetown Journal of International Affairs*, September 13, 2015.

"Is It OK to Shoot Down a Drone over Your Backyard?" *CNN*, September 9, 2015.

"The Meanest Email You Ever Wrote, Searchable on the Internet," *Atlantic*, September 8, 2015.

"Should Some Secrets Be Exposed?" *CNN*, July 7, 2015.

"Why We Encrypt," Foreword to Privacy International's *Securing Safe Spaces Online*, June 2015.

"China and Russia Almost Definitely Have the Snowden Docs," *Wired,* June 16, 2015

"Why are We Spending $7 Billion on TSA?" *CNN,* June 5, 2015

"Debate: Should Companies Do Most of Their Computing in the Cloud?" *The Economist,* June 5, 2015

"How We Sold Our Souls—and More—to the Internet Giants," *The Guardian,* May 17, 2015

"Could Your Plane Be Hacked?" *CNN,* April 16, 2015

"Baseball's New Metal Detectors Won't Keep You Safe. They'll Just Make You Miss a Few Innings," *The Washington Post,* April 14, 2015

"The Big Idea: *Data and Goliath*," *Whatever*, March 4, 2015.

"Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle," *The Christian Science Monitor*, March 4, 2015.

"The World's Most Sophisticated Hacks: Governments?," *Fortune*, March 3, 2015.

"Cyberweapons Have No Allegiance," *Motherboard*, February 25, 2015.

"Everyone Wants You To Have Security, But Not from Them," *Forbes*, February 23, 2015.

"Your TV May Be Watching You," *CNN*, February 11, 2015.

"When Thinking Machines Break The Law," *Edge*, January 28, 2015.

"The Importance of Deleting Old Stuff—Another Lesson From the Sony Attack," *Ars Technica*, January 12, 2015.

"The Government Must Show Us the Evidence That North Korea Attacked Sony," *Time*, January 5, 2015.

"We Still Don't Know Who Hacked Sony," *The Atlantic*, January 5, 2015.

"2015: The Year 'Doxing' Will Hit Home, *BetaBoston*, December 31, 2014.

"Did North Korea Really Attack Sony?," *The Atlantic*, December 22, 2014.

"Sony Made It Easy, but Any of Us Could Get Hacked," *The Wall Street Journal*, December 19, 2014.

"The Best Thing We Can Do About the Sony Hack Is Calm Down," *Motherboard*, December 19, 2014.

"What Are the Limits of Police Subterfuge?," *The Atlantic*, December 17, 2014.

"Over 700 Million People Taking Steps to Avoid NSA Surveillance," *Lawfare*, December 15, 2014.

"NSA Hacking of Cell Phone Networks," *Lawfare*, December 8, 2014

"Antivirus Companies Should Be More Open About Their Government Malware Discoveries," *MIT Technology Review*, December 5, 2014.

"Why Uber's 'God View' Is Creepy," *CNN*, December 4, 2014.

"Stop the Hysteria over Apple Encryption," *CNN*, October 3, 2014.

"The Future of Incident Response," *IEEE Security & Privacy*, September/October 2014

"The U.S.'s Hypocritical Stance Against Chinese Hackers," *Time,* May 20, 2014.

"A Human Problem," *The Mark News,* May 19, 2014.

"Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?," *The Atlantic,* May 19, 2014.

"Let the Spies Spy, Let the Cops Chase Terrorists," *CNN,* May 15, 2014.

"Internet Subversion," *Boston Review,* May/June 2014.

"How Secure are Snapchat-style Apps?," *CNN,* March 26, 2014.

"Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong," *The Atlantic,* March 25, 2014.

"There's No Real Difference Between Online Espionage and Online Attack," *The Atlantic,* March 6, 2014.

"Metadata = Surveillance," *IEEE Security & Privacy,* March/April 2014.

"NSA Robots are 'Collecting' Your Data, Too, and They're Getting Away With It," *The Guardian,* February 27, 2014.

"Choosing a Secure Password," *Boing Boing,* February 25, 2014.

"It's Time to Break Up the NSA," *CNN,* February 20, 2014.

"Let the NSA Keep Hold of the Data," *Slate,* February 14, 2014.

"Everything We Know About How the NSA Tracks People's Physical Location," *The Atlantic,* Feburary 11, 2014.

"How the NSA Threatens National Security," *The Atlantic,* January 6, 2014.

"The Internet of Things Is Wildly Insecure—And Often Unpatchable," *Wired,* January 6, 2014.

"'Stalker Economy' Here to Stay," *CNN,* November 20, 2013.

"A Fraying of the Public/Private Surveillance Partnership," *The Atlantic,* November 8, 2013.

"Leakers and Governments Should Work Together," *CNN,* November 4, 2013.

"The Battle for Power on the Internet," *The Atlantic,* October 24, 2013.

"Why the NSA's Defense of Mass Data Collection Makes No Sense," *The Atlantic,* October 21, 2013.

"Your Life, Under Constant Surveillance," *CNN,* October 16, 2013.

"How to Design—And Defend Against—The Perfect Security Backdoor," *Wired,* October 16, 2013.

"Want to Evade NSA Spying? Don't Connect to the Internet," *Wired,* October 7, 2013.

"How the NSA Thinks About Secrecy and Risk," *The Atlantic,* October 4, 2013.

"Why the NSA's Attacks on the Internet Must Be Made Public," *The Guardian,* October 4, 2013.

"Attacking Tor: How the NSA Targets Users' Online Anonymity," *The Guardian,* October 4, 2013.

"NSA and GCHQ target Tor Network That Protects Anonymity of Web Users," *The Guardian,* October 4, 2013.

"Book Review: Cyber War Will Not Take Place," *Europe's World,* October 1, 2013.

"Understanding the Threats in Cyberspace," *Europe's World,* September 27, 2013.

"Could U.S. Have Stopped Syria's Chemical Attack?," *CNN,* September 11, 2013.

"The NSA-Reform Paradox: Stop Domestic Spying, Get More Security," *The Atlantic,* September 11, 2013.

"If the New iPhone Has Fingerprint Authentication, Can It Be Hacked?," *Wired,* September 9, 2013.

"NSA Surveillance: a Guide to Staying Secure," *The Guardian,* September 6, 2013.

"The Spooks Need New Ways to Keep Their Secrets Safe," *Financial Times,* September 5, 2013.

"The US Government Has Betrayed the Internet. We Need to Take It Back," *The Guardian,* September 5, 2013.

"The Only Way to Restore Trust in the NSA," *The Atlantic,* September 4, 2013.

"How Advanced Is the NSA's Cryptanalysis—And Can We Resist It?," *Wired,* September 4, 2013.

"Trust in Man/Machine Security Systems," *IEEE Security & Privacy,* September/October 2013.

"Syrian Electronic Army: A Brief Look at What Businesses Need to Know," *The Wall Street Journal,* August 29, 2013.

"NSA Intimidation Expanding Surveillance State," *USA Today,* August 27, 2013.

"Our Decreasing Tolerance To Risk," *Forbes,* August 23, 2013.

"The Real, Terrifying Reason Why British Authorities Detained David Miranda," *The Atlantic,* August 22, 2013.

"How Companies Can Protect Against Leakers," *Bloomberg.com,* August 21, 2013.

"Why It's So Easy to Hack Your Home," *CNN,* August 15, 2013.

"The NSA Is Commandeering the Internet," *The Atlantic,* August 12, 2013.

"The Army in Our Midst," *The Wall Street Journal,* August 5, 2013.

"The Public-Private Surveillance Partnership," *Bloomberg.com,* July 31, 2013.

"NSA Secrets Kill Our Trust," *CNN,* July 31, 2013.

"Cyberconflicts and National Security," *UN Chronicle,* July 18, 2013.

"Mission Creep: When Everything Is Terrorism," *The Atlantic,* July 16, 2013.

"Has U.S. Started an Internet War?," *CNN,* June 18, 2013.

"Before Prosecuting, Investigate the Government," *New York Times Room for Debate Blog,* June 11, 2013.

"You Have No Control Over Security on the Feudal Internet," *Harvard Business Review,* June 6, 2013.

"What We Don't Know About Spying on Citizens: Scarier Than What We Know," *The Atlantic,* June 6, 2013.

"The FBI's New Wiretapping Plan Is Great News for Criminals," *Foreign Policy,* May 29, 2013.

"It's Smart Politics to Exaggerate Terrorist Threats," *CNN,* May 20, 2013.

"Will Giving the Internet Eyes and Ears Mean the End of Privacy?," *The Guardian,* May 16, 2013.

"Transparency and Accountability Don't Hurt Security—They're Crucial to It," *The Atlantic,* May 8, 2013.

"Why FBI and CIA Didn't Connect the Dots," *CNN,* May 2, 2013.

"Do You Want the Government Buying Your Data From Corporations?," *The Atlantic,* April 30, 2013.

"The Boston Marathon Bombing: Keep Calm and Carry On," *The Atlantic,* April 15, 2013.

"IT for Oppression," *IEEE Security & Privacy,* March/April 2013.

"On Security Awareness Training," *Dark Reading,* March 19, 2013.

"The Internet Is a Surveillance State," *CNN,* March 16, 2013.

"Rhetoric of Cyber War Breeds Fear—and More Cyber War," *The Irish Times,* March 14, 2013.

"Our Security Models Will Never Work—No Matter What We Do," *Wired,* March 14, 2013.

"Danger Lurks in Growing New Internet Nationalism," *MIT Technology Review,* March 11, 2013.

"Take Stop-and-Scan with a Grain of Salt," *New York Daily News,* March 3, 2013.

"The Court of Public Opinion Is About Mob Justice and Reputation as Revenge," *Wired*, February 26, 2013.

"How Secure Is the Papal Election?," *CNN*, February 21, 2013.

"Trust and Society," *The Montréal Review*, February 2013.

"Power and the Internet, *Edge*, January 23, 2013.

"Unsafe Security: A Sociologist Aptly Analyzes our Failures in Top-Down Protection," *Reason*, January 2013.

"Our New Regimes of Trust," *The SciTech Lawyer*, Winter/Spring 2013.

"Militarizing Cyberspace Will Do More Harm Than Good," *The Irish Times*, November 29, 2012.

"When It Comes to Security, We're Back to Feudalism," *Wired*, November 26, 2012.

"Lance Armstrong and the Prisoner's Dilemma of Doping in Professional Sports," *Wired*, October 26, 2012.

"Fear Pays the Bills, But Accounts Must Be Settled," *New York Times* Room for Debate blog, October 19, 2012.

"The Importance of Security Engineering," *IEEE Security & Privacy*, September/October 2012.

"Drawing the Wrong Lessons from Horrific Events," *CNN* , July 31, 2012.

"Securing Medical Research: A Cybersecurity Point of View," *Science*, June 22, 2012.

"Debate Club: An International Cyberwar Treaty Is the Only Way to Stem the Threat," *U.S. News*, June 8, 2012.

"The Vulnerabilities Market and the Future of Security," *Forbes*, May 30, 2012.

"To Profile or Not to Profile?," *Sam Harris's Blog*, May 25, 2012.

"The Trouble with Airport Profiling," Forbes, May 9, 2012.

"Economist Debates: Airport Security," *The Economist*, March 20, 2012.

"High-Tech Cheats in a World of Trust," *New Scientist*, February 27, 2012.

"The Big Idea: Bruce Schneier," *Whatever*, February 16, 2012.

"How Changing Technology Affects Security," *IEEE Security & Privacy*, March/April 2012.

"Detecting Cheaters," *IEEE Security & Privacy*, March/April 2011.

"Why Terror Alert Codes Never Made Sense," *CNN*, January 28, 2011.

"Whitelisting and Blacklisting," *Information Security*, January 2011.

"It Will Soon Be Too Late to Stop the Cyberwars," *Financial Times*, December 2, 2010.

"Why the TSA Can't Back Down," *The Atlantic*, December 2, 2010.

"Close the Washington Monument," *The New York Daily News*, December 2, 2010.

"The Dangers of a Software Monoculture," *Information Security Magazine*, November 2010.

"A Waste of Money and Time," *New York Times Room for Debate Blog*, November 23, 2010.

"The Plan to Quarantine Infected Computers," *Forbes*, November 11, 2010.

“When to Change Passwords,” *Dark Reading*, November 10, 2010.

“The Difficulty of Surveillance Crowdsourcing,” *Threatpost*, November 8, 2010.

“The Story Behind The Stuxnet Virus,” *Forbes*, October 7, 2010.

“Web Snooping Is a Dangerous Move,” *CNN*, September 29, 2010.

“Should Enterprises Give In to IT Consumerization at the Expense of Security?,” *Information Security*, September 2010.

“Data Privacy: The Facts of Life,” *The Irish Times*, August 27, 2010.

“A Taxonomy of Social Networking Data,” *IEEE Security & Privacy*, July/August 2010.

“3 Reasons to Kill the Internet Kill Switch Idea,” *AOL News*, July 9, 2010.

“Threat of ‘Cyberwar’ Has Been Hugely Hyped,” *CNN*, July 7, 2010.

“The Failure of Cryptography to Secure Modern Networks,” *Dark Reading*, June 30, 2010.

“Weighing the Risk of Hiring Hackers,” *Information Security*, June 2010.

“The Internet: Anonymous Forever,” *Forbes*, *Information Security*, May 12, 2010.

“Worst-Case Thinking Makes Us Nuts, Not Safe,” *CNN*, May 12, 2010.

“Where Are All the Terrorist Attacks?,” *AOL News*, May 4, 2010.

“Focus on the Threat,” *New York Times Room for Debate Blog*, May 3, 2010.

“The Meaning of Trust,” *The Guardian*, April 16, 2010.

“Scanners, Sensors are Wrong Way to Secure the Subway,” *Daily News*, April 7, 2010.

“Google And Facebook’s Privacy Illusion,” *Forbes*, April 6, 2010.

“Should the Government Stop Outsourcing Code Development?,” *Information Security*, March 2010.

“Spy Cameras Won’t Make Us Safer,” *CNN*, February 25, 2010.

“Security and Function Creep,” *IEEE Security & Privacy*, January/February 2010.

“U.S. Enables Chinese Hacking of Google,” *CNN* and *Ethiopian Review*, January 23, 2010.

“Fixing Intelligence Failures,” *San Francisco Chronicle*, January 15, 2010.

“Stop the Panic on Air Security,” *CNN*, January 7, 2010.

“Our Reaction Is the Real Security Failure,” *AOL News*, January 7, 2010.

"Fixing a Security Problem Isn't Always the Right Answer," *Threatpost*, January 5, 2010.

"Profiling Makes Us Less Safe," *New York Times Room for Debate Blog*, January 4, 2010.

"Is Aviation Security Mostly for Show?," *CNN*, December 29, 2009.

"Cold War Encryption is Unrealistic in Today's Trenches," *The Japan Times* and *Wired News*, December 23, 2009.

"Virus and Protocol Scares Happen Every Day—But Don't Let Them Worry You," *The Guardian*, December 9, 2009.

"Nature's Fears Extend to Online Behavior," *The Japan Times* and *Dark Reading*, November 18, 2009.

"News Media Strategies for Survival for Journalists," *Twin Cities Daily Planet*, November 14, 2009.

"Reputation is Everything in IT Security," *The Guardian*, November 11, 2009.

"Is Antivirus Dead?," *Information Security*, November 2009.

"Beyond Security Theater," *New Internationalist*, November 2009.

"'Zero Tolerance' Really Means Zero Discretion," *MPR NewsQ*, November 4, 2009.

"Why Framing Your Enemies Is Now Virtually Child's Play," *The Guardian*, October 15, 2009.

"The Difficulty of Un-Authentication," *Threatpost*, September 28, 2009.

"The Battle Is On Against Facebook and Co to Regain Control of Our Files," *The Guardian*, September 9, 2009.

"Is Perfect Access Control Possible?," *Information Security*, September 2009.

"Offhand but On Record," *The Japan Times*, August 19, 2009.

"Lockpicking and the Internet," *Dark Reading*, August 10, 2009.

"The Value of Self-Enforcing Protocols," *Threatpost*, August 10, 2009.

"People Understand Risks—But Do Security Staff Understand People?," *The Guardian*, *The Sydney Morning Herald*, and *The Age*, August 5, 2009.

"Technology Shouldn't Give Big Brother a Head Start," *MPR News Q*, July 31, 2009.

"Protect Your Laptop Data From Everyone, Even Yourself," *Wired News*, July 15, 2009.

"Facebook Should Compete on Privacy, Not Hide It Away," *The Guardian*, July 15, 2009.

"So-called Cyberattack Was Overblown," *MPR News Q* and *ITWire*, July 13, 2009.

"Security, Group Size, and the Human Brain," *IEEE Security & Privacy*, July/August 2009.

"Clear Common Sense for Takeoff: How the TSA Can Make Airport Security Work for Passengers Again," *New York Daily News*, June 24, 2009.

"Raising the Cost of Paperwork Errors Will Improve Accuracy," *The Guardian* and *Gulf Times*, June 24, 2009.

"How Science Fiction Writers Can Help, or Hurt, Homeland Security," *Wired News*, June 18, 2009.

"Be Careful When You Come to Put Your Trust in the Clouds," *The Guardian* and *The Japan Times*, June 4, 2009.

"Coordinate, But Distribute Responsibility," *NYTimes.com*, May 29, 2009.

"We Shouldn't Poison Our Minds with Fear of Bioterrorism," *The Guardian*, May 14, 2009.

"Should We Have an Expectation of Online Privacy?," *Information Security*, May 2009.

"Do You Know Where Your Data Are?," *The Wall Street Journal*, April 28, 2009.

"How the Great Conficker Panic Hacked into Human Credulity," *The Guardian* and *Gulf Times*, April 23, 2009.

"An Enterprising Criminal Has Spotted a Gap in the Market," *The Guardian*, April 2, 2009.

"Who Should Be in Charge of Cybersecurity?," *The Wall Street Journal*, March 31, 2009.

"It's Time to Drop the 'Expectation of Privacy' Test," *Wired News*, March 26, 2009.

"Blaming The User Is Easy—But It's Better to Bypass Them Altogether," *The Guardian*, March 12, 2009.

"The Kindness of Strangers," *The Wall Street Journal*, March 12, 2009.

"Privacy in the Age of Persistence," *BBC News*, February 26, 2009.

"How Perverse Incentives Drive Bad Security Decisions," *Wired News*, February 26, 2009.

"The Secret Question Is: Why Do IT Systems Use Insecure Passwords?," *The Guardian*, February 19, 2009.

"Thwarting an Internal Hacker," *The Wall Street Journal*, February 16, 2009.

"Terrorists May Use Google Earth, But Fear Is No Reason to Ban It," *The Guardian*, *The Hindu*, *Brisbane Times*, and *The Sydney Morning Herald*, January 29, 2009.

"How to Ensure Police Database Accuracy," *The Wall Street Journal*, January 27, 2009.

"Architecture of Privacy," *IEEE Security & Privacy*, Jan/Feb 2009.

"State Data Breach Notification Laws: Have They Helped?," *Information Security*, Jan 2009.

"Why Technology Won't Prevent Identity Theft," *The Wall Street Journal*, January 9, 2009.

"Tigers Use Scent, Birds Use Calls—Biometrics Are Just Animal Instinct," *The Guardian*, January 8, 2009.

"How to Prevent Digital Snooping," *The Wall Street Journal*, December 9, 2008.

"When You Lose a Piece of Kit, the Real Loss Is The Data It Contains," *The Guardian* and *The Hindu*, December 4, 2008.

"Why Obama Should Keep His BlackBerry—But Won't," *The Wall Street Journal*, November 21, 2008.

"America's Next Top Hash Function Begins," *Wired News*, November 19, 2008.

"Passwords Are Not Broken, but How We Choose them Sure Is," *The Guardian* and *The Hindu*, November 13, 2008.

"CRB Checking," Schneier on Security, November 3, 2008.

"Time to Show Bottle and Tackle the Real Issues," *The Guardian*, October 23, 2008.

"Quantum Cryptography: As Awesome As It Is Pointless," *Wired News*, October 16, 2008.

"Why Society Should Pay the True Costs of Security," *The Guardian*, October 2, 2008.

"The Seven Habits of Highly Ineffective Terrorists," *Wired News*, October 1, 2008.

"Does Risk Management Make Sense?," *Information Security Magazine*, October 2008.

"Airport Pasta-Sauce Interdiction Considered Harmful," *Wired News*, September 18, 2008.

"A Fetishistic Approach to Security Is a Perverse Way to Keep Us Safe," *The Guardian*, September 4, 2008.

"How to Create the Perfect Fake Identity," *Wired News*, September 4, 2008.

"Security ROI: Fact or Fiction?," *CSO Magazine*, September 2, 2008.

"Here Comes Here Comes Everybody," *IEEE Spectrum*, September 2008.

"The TSA's Useless Photo ID Rules," *Los Angeles Times*, August 28, 2008.

"Boston Court's Meddling With 'Full Disclosure' Is Unwelcome," *Wired News*, August 21, 2008.

"The Problem Is Information Insecurity," *Security Watch*, August 10, 2008.

"Memo to Next President: How to Get Cybersecurity Right," *Wired News*, August 7, 2008.

"Why Being Open about Security Makes Us All Safer in the Long Run," *The Guardian*, August 7, 2008.

"How the Human Brain Buys Security," *IEEE Security and Privacy*, Jul/Aug 2008.

"Lesson From the DNS Bug: Patching Isn't Enough," *Wired News*, July 23, 2008.

"Software Makers Should Take Responsibility," *The Guardian*, July 17, 2008.

"How a Classic Man-in-the-Middle Attack Saved Colombian Hostages," *Wired News*, July 10, 2008.

"Chinese Cyberattacks: Myth or Menace?," *Information Security Magazine*, July 2008.

"I've Seen the Future, and It Has a Kill Switch," *Wired News*, June 30, 2008.

"CCTV Doesn't Keep Us Safe, Yet the Cameras Are Everywhere," *The Guardian*, June 26, 2008.

"The Truth About Chinese Hackers," *Discovery Technology*, June 19, 2008.

"The Pros and Cons of Lifelock," *Wired News*, June 12, 2008.

"Are Photographers Really a Threat?," *The Guardian*, June 4, 2008.

"Why Do We Accept Signatures by Fax?," *Wired News*, May 29, 2008.

"How to Sell Security," *CIO*, May 26, 2008.

"Our Data, Ourselves," *Wired News*, May 15, 2008.

"Crossing Borders with Laptops and PDAs," *The Guardian*, May 15, 2008.

"America's Dilemma: Close Security Holes, or Exploit Them Ourselves," *Wired News*, May 1, 2008.

"The Ethics of Vulnerability Research," *Information Security Magazine*, May 2008.

"Prediction: RSA Conference Will Shrink Like a Punctured Balloon," *Wired News*, April 17, 2008.

"Secret Questions Blow a Hole in Security," *ComputerWeekly*, April 4, 2008.

“The Difference Between Feeling and Reality in Security,” *Wired News*, April 3, 2008.

“Inside the Twisted Mind of the Security Professional,” *Wired News*, March 20, 2008.

“Census of Cyberspace Censoring,” *Nature*, March 13, 2008.

“The Myth of the ‘Transparent Society,’” *Wired News*, March 6, 2008.

“Consolidation: Plague or Progress,” *Information Security Magazine*, March 2008.

“Security at What Cost?,” *Minneapolis Star Tribune*, February 23, 2008.

“When the Internet Is My Hard Drive, Should I Trust Third Parties?,” *Wired News*, February 21, 2008.

“Driver’s Licenses for Immigrants: Denying Licenses Makes Us Less Safe,” *Detroit Free Press*, February 7, 2008.

“With iPhone, ‘Security’ Is Code for ‘Control,’” *Wired News*, February 7, 2008.

“What Our Top Spy Doesn’t Get: Security and Privacy Aren’t Opposites,” *Wired News*, January 24, 2008.

“Steal This Wi-Fi,” *Wired News*, January 10, 2008.

“Why ‘Anonymous’ Data Sometimes Isn’t,” *Wired News*, December 13, 2007.

“Caution: Turbulence Ahead,” *Information Security Magazine*, December 2007.

“The Death of the Security Industry,” *IEEE Security and Privacy*, Nov/Dec 2007.

“How Does Bruce Schneier Protect His Laptop Data? With His Fists — and PGP,” *Wired News*, November 29, 2007.

“Did NSA Put a Secret Backdoor in New Encryption Standard?,” *Wired News*, November 15, 2007.

“Cyberwar: Myth or Reality?,” *Information Security Magazine*, November 2007.

“How We Won the War on Thai Chili Sauce,” *Wired News*, November 1, 2007.

“Economics, Not Apathy, Exposes Chemical Plants To Danger,” *Wired News*, October 18, 2007.

“Paying the Cost of Insecure Software [PDF],” *OutlookBusiness*, October 5, 2007.

“Gathering ‘Storm’ Superworm Poses Grave Threat to PC Nets,” *Wired News*, October 4, 2007.

“Lesson From Tor Hack: Anonymity and Privacy Aren’t the Same,” *Wired News*, September 20, 2007.

“NBA Ref Scandal Warns of Single Points of Failure,” *Wired News*, September 6, 2007.

“Home Users: A Public Health Problem?,” *Information Security Magazine*, September 2007.

“Time to Close Gaps in Emergency Communications,” *Wired News*, August 23, 2007.

“E-Voting Certification Gets Security Completely Backward,” *Wired News*, August 9, 2007.

“Interview with Kip Hawley,” Schneier on Security, August 3, 2007.

“Disaster Planning Is Critical, but Pick a Reasonable Disaster,” *Wired News*, July 26, 2007.

“The Evolutionary Brain Glitch That Makes Terrorism Fail,” *Wired News*, July 12, 2007.

“Strong Laws, Smart Tech Can Stop Abusive ‘Data Reuse,’” *Wired News*, June 28, 2007.

“Portrait of the Modern Terrorist as an Idiot,” *Wired News*, June 14, 2007.

“Don’t Look a Leopard in the Eye, and Other Security Advice,” *Wired News*, May 31, 2007.

“Virginia Tech Lesson: Rare Risks Breed Irrational Responses,” *Wired News*, May 17, 2007.

“Will REAL ID Actually Make Us Safer?,” *Testimony before the Senate Judiciary Committee*, May 8, 2007.

“Nonsecurity Considerations in Security Decisions,” *IEEE Computers and Security*, May 6, 2007.

“Do We Really Need a Security Industry?,” *Wired News*, May 3, 2007.

“Psychology of Security,” *Communications of the ACM*, May 2007.

“Is Big Brother a Big Deal?,” *Information Security Magazine*, May 2007.

“How Security Companies Sucker Us With Lemons,” *Wired News*, April 19, 2007.

“Vigilantism Is a Poor Response to Cyberattack,” *Wired News*, April 5, 2007.

“How to Not Catch Terrorists,” *Forbes*, March 26, 2007.

“Why the Human Brain Is a Poor Judge of Risk,” *Wired News*, March 22, 2007.

“The Problem With Copycat Cops,” *Wired News*, March 8, 2007.

“Real-ID: Costs and Benefits,” *The Bulletin of the Atomic Scientists*, March 4, 2007.

“Is Penetration Testing Worth It?,” *Information Security Magazine*, March 2007.

“Privatizing the Police Puts Us at Greater Risk,” *Minneapolis Star Tribune*, February 27, 2007.

"Why Smart Cops Do Dumb Things," *Wired News*, February 22, 2007.

"Why Vista's DRM Is Bad For You," *Forbes*, February 12, 2007.

"An American Idol for Crypto Geeks," *Wired News*, February 8, 2007.

"The Psychology of Security," February 7, 2007.

"In Praise of Security Theater," *Wired News*, January 25, 2007.

"Solving Identity Theft," *Forbes*, January 22, 2007.

"Life in the Fast Lane," *The New York Times* and *The Mercury News*, January 21, 2007.

"Camera Phones vs. Crime: Now We're Talking," *New York Daily News*, January 19, 2007.

"On Police Security Cameras," *San Francisco Chronicle* and *Arizona Daily Star*, January 16, 2007.

"Secure Passwords Keep You Safer," *Wired News*, January 15, 2007.

"They're Watching," *Forbes*, January 8, 2007.

"Does Secrecy Help Protect Personal Information?," *Information Security*, January 2007.

"Information Security and Externalities," *ENISA Quarterly*, January 2007.

"Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea,'" *CSO Online*, January 2007.

"MySpace Passwords Aren't So Dumb," *Wired News*, December 14, 2006.

"Why Spam Won't Go Away," *Forbes*, December 12, 2006.

"My Data, Your Machine," *Wired News*, November 30, 2006.

"Vote Early, Vote Often," *Wired News*, November 16, 2006.

"Did Your Vote Get Counted?," *Forbes*, November 13, 2006.

"The Boarding Pass Brouhaha," *Wired News*, November 2, 2006.

"Do Federal Security Regulations Help?," *Information Security Magazine*, November 2006.

"The Architecture of Security," *Wired News*, October 19, 2006.

"Casual Conversation, R.I.P.," *Forbes*, October 18, 2006.

"Why Everyone Must Be Screened," *Wired News*, October 5, 2006.

"Lessons From the Facebook Riots," *Wired News*, September 21, 2006.

"The ID Chip You Don't Want in Your Passport," *Washington Post*, September 16, 2006.

"Quickest Patch Ever," *Wired News*, September 7, 2006.

"Is There Strategic Software?," *Information Security Magazine*, September 2006.

"Refuse to be Terrorized," *Wired News*, August 24, 2006.

"Focus on Terrorists, Not Tactics," *Minneapolis Star Tribune*, August 13, 2006.

"Drugs: Sports' Prisoner's Dilemma," *Wired News*, August 10, 2006.

"How Bot Those Nets?," *Wired News*, July 27, 2006.

"Google's Click-Fraud Crackdown," *Wired News*, July 13, 2006.

"Are Security Certifications Valuable?," *Information Security Magazine*, July 2006.

"It's the Economy, Stupid," *Wired News*, June 29, 2006.

"The Scariest Terror Threat of All," *Wired News*, June 15, 2006.

"Make Vendors Liable for Bugs," *Wired News*, June 1, 2006.

"We're Giving Up Privacy and Getting Little in Return," *Minneapolis Star Tribune*, May 31, 2006.

"The Eternal Value of Privacy," *Wired News*, May 18, 2006.

"Everyone Wants to 'Own' Your PC," *Wired News*, May 4, 2006.

"The Anti-ID-Theft Bill That Isn't," *Wired News*, April 20, 2006.

"Why VOIP Needs Crypto," *Wired News*, April 6, 2006.

"Is User Education Working?," *Information Security Magazine*, April 2006.

"Let Computers Screen Air Baggage," *Wired News*, March 23, 2006.

"Why Data Mining Won't Stop Terror," *Wired News*, March 9, 2006.

"Your Vanishing Privacy," *Minneapolis Star Tribune*, March 5, 2006.

"U.S. Ports Raise Proxy Problem," *Wired News*, February 23, 2006.

"Security in the Cloud (Feb 06)," *Network World*, February 15, 2006.

"Fighting Fat-Wallet Syndrome," *Wired News*, February 9, 2006.

"Big Risks Come in Small Packages," *Wired News*, January 26, 2006.

"Anonymity Won't Kill the Internet," *Wired News*, January 12, 2006.

"Unchecked Presidential Power," *Minneapolis Star Tribune*, December 20, 2005.

"Uncle Sam is Listening," *Salon*, December 20, 2005.

"Hold the Photons!," *Wired News*, December 15, 2005.

"The Hackers are Coming!," *Utility Automation & Engineering T&D*, December 13, 2005.

"Airline Security a Waste of Cash," *Wired News*, December 1, 2005.

"The Zotob Storm," *IEEE Security and Privacy*, Nov/Dec 2005.

"The Erosion of Freedom," *Minneapolis Star Tribune*, November 21, 2005.

"Real Story of the Rogue Rootkit," *Wired News*, November 17, 2005.

"Fatal Flaw Weakens RFID Passports," *Wired News*, November 3, 2005.

"Sue Companies, Not Coders," *Wired News*, October 20, 2005.

"A Real Remedy for Phishers," *Wired News*, October 6, 2005.

"University Networks and Data Security," *IEEE Security and Privacy*, Sep/Oct 2005.

"A Sci-Fi Future Awaits the Court," *Wired News*, September 22, 2005.

"Toward a Truly Safer Nation," *Minneapolis Star Tribune*, September 11, 2005.

"Terrorists Don't Do Movie Plots," *Wired News*, September 8, 2005.

"Make Businesses Pay in Credit Card Scam," *New York Daily News*, June 23, 2005.

"Attack Trends: 2004 and 2005," *Queue*, June 2, 2005.

"Risks of Third-Party Data," *Communications of the ACM*, May 2005.

"Two-Factor Authentication: Too Little, Too Late," *Communications of the ACM*, April 2005.

"Digital Information Rights Need Tech-Savvy Courts," *eWeek*, February 14, 2005.

"The Curse of the Secret Question," *Computerworld*, February 9, 2005.

"Authentication and Expiration," *IEEE Security and Privacy*, Jan/Feb 2005.

"Who says safe computing must remain a pipe dream?," *CNET News.com*, December 9, 2004.

"Airport Security and Metal Knives," *The Sydney Morning Herald*, November 30, 2004.

"Desktop Google Finds Holes," *eWeek*, November 29, 2004.

"Profile: 'hinky,'" *Boston Globe*, November 24, 2004.

"Why is it so hard to run an honest election?," *OpenDemocracy*, November 24, 2004.

"Getting Out the Vote," *San Francisco Chronicle*, October 31, 2004.

"Information Security: How Liable Should Vendors Be?," *Computerworld*, October 28, 2004.

"The Security of Checks and Balances," *The Sydney Morning Herald*, October 26, 2004.

"Outside View: Security at the World Series," *UPI*, October 22, 2004.

"Bigger Brother," *The Baltimore Sun*, October 4, 2004.

"Does Big Brother want to watch?," *International Herald Tribune*, October 4, 2004.

"Do Terror Alerts Work?," *The Rake*, October 2004.

"The Non-Security of Secrecy," *Communications of the ACM*, October 2004.

"SIMS: Solution, or Part of the Problem?," *IEEE Security and Privacy*, Sep/Oct 2004.

"Saluting the data encryption legacy," *CNET News.com*, September 27, 2004.

"Academics locked out by tight visa controls," *Mercury News*, September 20, 2004.

"City Cops' Plate Scanner is a License to Snoop," *New Haven Register*, September 19, 2004.

"We Owe Much to DES," *eWeek*, August 30, 2004.

"How Long Can the Country Stay Scared?," *Minneapolis Star Tribune*, August 27, 2004.

"Olympic Security," *The Sydney Morning Herald*, August 26, 2004.

"U.S. 'No-Fly' List Curtails Liberties," *Newsday*, August 25, 2004.

"An Easy Path for Terrorists," *Boston Globe*, August 24, 2004.

"Cryptanalysis of MD5 and SHA: Time for a New Standard," *Computerworld*, August 19, 2004.

"BOB on Board," *The Sydney Morning Herald*, August 2, 2004.

"Customers, Passwords, and Web Sites," *IEEE Security and Privacy*, Jul/Aug 2004.

"Security, Houston-Style," *The Sydney Morning Herald*, July 30, 2004.

"US-VISIT Is No Bargain," *eWeek*, July 6, 2004.

"Insider Risks in Elections," *Communications of the ACM*, July 2004.

"Unchecked Police And Military Power Is A Security Threat," *Minneapolis Star Tribune*, June 24, 2004.

"CLEARly Muddying the Fight Against Terror," *News.com*, June 16, 2004.

"The Witty Worm: A New Chapter in Malware," *Computerworld*, June 2, 2004.

"Security and Compliance," *IEEE Security and Privacy*, May/Jun 2004.

"Microsoft's Actions Speak Louder Than Words," *Network World*, May 31, 2004.

"Curb Electronic Surveillance Abuses," *Newsday*, May 10, 2004.

"We Are All Security Customers," *CNET News.com*, May 4, 2004.

"Terrorist Threats and Political Gains," *Counterpunch*, April 27, 2004.

"Hacking the Business Climate for Network Security," *IEEE Computer*, April 2004.

"A National ID Card Wouldn't Make Us Safer," *Minneapolis Star Tribune*, April 1, 2004.

"Cyber Underwriters Lab?," *Communications of the ACM*, April 2004.

"America's Flimsy Fortress," *Wired Magazine*, March 2004.

"IDs and the illusion of security," *San Francisco Chronicle*, February 3, 2004.

"Risks of PKI: Electronic Commerce," *Communications of the ACM*, February 2004.

"Voting Security," *IEEE Security and Privacy*, Jan/Feb 2004.

"Slouching Towards Big Brother," *CNET News.com*, January 30, 2004.

"Homeland Insecurity," *Salon.com*, January 19, 2004.

"Fingerprinting Visitors Won't Offer Security," *Newsday*, January 14, 2004.

"Risks of PKI: Secure E-Mail," *Communications of the ACM*, January 2004.

"Better Get Used to Routine Loss of Personal Privacy," *Minneapolis Star Tribune*, December 21, 2003.

"Are You Sophisticated Enough to Recognize an Internet Scam?," *Mercury News*, December 19, 2003.

"Blaster and the Great Blackout," *Salon.com*, December 16, 2003.

"Internet Worms and Critical Infrastructure," *CNET News.com*, December 9, 2003.

"Airplane Hackers," *IEEE Security and Privacy*, Nov/Dec 2003.

"Festung Amerika," *Financial Times Deutschland*, November 11, 2003.

"Liability Changes Everything," *Heise Security*, November 2003.

"Terror Profiles by Computers Are Ineffective," *Newsday*, October 21, 2003.

"Fixing intelligence," *UPI*, October 14, 2003.

"CyberInsecurity: The Cost of Monopoly," *Computer & Communications Industry Association Report*, September 24, 2003.

"Voting and Technology: Who Gets to Count Your Vote?," *Communications of the ACM*, August 2003.

"The Speed of Security," *IEEE Security and Privacy*, Jul/Aug 2003.

"Walls Don't Work in Cyberspace," *Wired Magazine*, June 2003.

"Guilty Until Proven Innocent?," *IEEE Security and Privacy*, May/Jun 2003.

"Locks and Full Disclosure," *IEEE Security and Privacy*, Mar/Apr 2003.

"American Cyberspace: Can We Fend Off Attackers?," *Mercury News*, March 7, 2003.

"Secrecy and Security," *SF Chronicle*, March 2, 2003.

"We Are All Security Consumers," *IEEE Security and Privacy*, Jan/Feb 2003.

"Trust, but Verify, Microsoft's Pledge," *CNET News.com*, January 18, 2002.

"The Case for Outsourcing Security *IEEE Computer Magazine*, 2002.

"Foreword," *Security Engineering by Ross Anderson*, May 2001.

"Body of Secrets by James Bamford (Review)," *Salon.com*, April 2001.

"Insurance and the Computer Industry," *Communications of the ACM*, March 2001.

"The Insurance Takeover," *Information Security Magazine*, February 2001.

"The Third Wave of Network Attacks," *ZDNet*, October 3, 2000.

"The Fallacy of Trusted Client Software," *Information Security Magazine*, August 2000.

"The Process of Security," *Information Security Magazine*, April 2000.

"1999 Crypto Year-in-Review," *Information Security Magazine*, December 1999.

"DVD Encryption Broken," *ZDNet*, November 1999.

"Why Computers are Insecure," *Computerworld*, November 1999.

"A Plea for Simplicity," *Information Security Magazine*, November 1999.

"Risks of Relying on Cryptography," *Communications of the ACM*, October 1999.

"The Trojan Horse Race," *Communications of the ACM*, September 1999.

"International Cryptography," *Information Security Magazine*, September 1999.

"Web-Based Encrypted E-Mail," *ZDNet*, August 1999.

"NIST AES News," *ZDNet*, August 1999.

"Biometrics: Uses and Abuses," *Communications of the ACM*, August 1999.

"Cryptography: The Importance of Not Being Different," *IEEE Security and Privacy*, March 1999.

"Why the Worst Cryptography is in the Systems that Pass Initial Analysis," *Information Security Magazine*, March 1999.

"Intel's Processor ID," *ZDNet*, January 26, 1999.

"How to Evaluate Security Technology," *Computer Security Journal*, 1999.

"1998 Crypto Year-in-Review," *Information Security Magazine*, December 1998.

"Key Recovery," *Information Security Magazine*, October 1998.

"Security Pitfalls in Cryptography," *Schneier on Security*, 1998.

"Click here to bring down the Internet," *Schneier on Security*, 1998.

"Cryptography, Security, and the Future," *Communications of the ACM*, January 1997.

"Why Cryptography is Harder than it Looks," *Schneier on Security*, 1997.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,626,667, January 7, 2014.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M Gelman, "System and method for securing electronic games," U.S. Patent 8,608,558, December 17, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 8,549,310, October 1, 2013.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 8,355,991, January 15, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,326,765, December 4, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and device for generating a single-use financial account number," U.S. Patent 8,315,948, November 20, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 8,250,369, August 21, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,135,650, March 13, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,086,653, December 27, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,086,167, December 27, 2011.

J.S. Walker, T.S. Case, J.A. Jorasch, B. Schneier, "Conditional purchase offer management system," U.S. Patent 8,082,221, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,082,180, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent RE42,893, November 1, 2011.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 7,991,698, August 2, 2011.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 7,988,044, August 2, 2011.

B. Schneier, A.H. Gross, J.D. Callas, "Method and system for dynamic network intrusion monitoring, detection and response," U.S. Patent 7,895,641, February 22, 2011.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,887,405, February 15, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent RE42,018, December 28, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,853,529, December 14, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,844,550, November 30, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, “Method and apparatus for verifying secure document timestamping,” U.S. Patent RE41,960, November 23, 2010.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 7,806,320, October 5, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 7,664,672, February 16, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 7,620,619, November 17, 2009.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M. Gelman, “System and method for securing electronic games,” U.S. Patent 7,524,245, April 28, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 7,523,045, April 21, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for educational testing,” U.S. Patent 7,483,670, January 27, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 7,472,074, December 30, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, “Methods and apparatus for awarding prizes based on authentication of computer generated outcomes using coupons,” U.S. Patent 7,362,862, April 22, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,303,468, December 4, 2007.

B. Schneier, J.S. Walker, J.A. Jorasch, “Off-line remote system for lotteries and games of skill,” U.S. Patent 7,285,045, October 23, 2007.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 7,177,835, February 13, 2007.

B. Schneier, A.H. Gross, J.D. Callas, “Method and system for dynamic network intrusion monitoring, detection and response,” U.S. Patent 7,159,237, January 2, 2007.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 7,090,123, August 15, 2006.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,008,318, March 7, 2006.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent 6,959,387, October 25, 2005.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,942,570, September 13, 2005.

J.S. Walker, B. Schneier, "Method and apparatus for remote gaming," U.S. Patent 6,935,952, August 30, 2005.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 6,904,418, June 7, 2005.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, "Method and apparatus for securing a computer-based game of chance," U.S. Patent 6,790,139, September 14, 2004.

J.S. Walker, B. Schneier, M.M. Fincham, "Device and method for promoting the selection and use of a transaction card," U.S. Patent 6,739,505, May 25, 2004.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,607,439, August 19, 2003.

J.S. Walker, B. Schneier, "Secure improved remote gaming system," U.S. Patent 6,527,638, March 4, 2003.

J.S. Walker, S.K. Jindal, B. Schneier, T. Weir-Jones, "System and method for managing third-party input to a conditional purchase offer (CPO)," U.S. Patent 6,484,153, November 19, 2002.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 6,477,513, November 5, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, "Method and apparatus for securing electronic games," U.S. Patent 6,450,885, September 17, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,402,614, June 11, 2002.

S.T. Ansell, A.R. Cherenson, M.E. Paley, S.B. Katz, J.M. Kelsey, Jr., B. Schneier, "Copy security for portable music players," U.S. Patent 6,367,019, April 2, 2002.

J.S. Walker, T.M. Sparico, B. Schneier, "Conditional purchase offer management system for telephone calls," U.S. Patent 6,345,090, February 5, 2002.

J.S. Walker, B. Schneier, M. Mik, “Device and method for promoting the selection and use of a credit card,” U.S. Patent 6,325,284, December 4, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,289,453, September 11, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,282,648, August 28, 2001.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,264,557, July 24, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure document timestamping,” U.S. Patent 6,263,438, July 17, 2001.

J.S. Walker, B. Schneier, “Systems and methods for a user to access digital data provided by an on-line server over a data network,” U.S. Patent 6,249,865, June 19, 2001.

J.S. Walker, R.R. Lech, A.S. Van Luchene, T.M. Sparico, J.A. Jorasch, B. Schneier, “Conditional purchase offer management system for event tickets,” U.S. Patent 6,240,396, May 29, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, “Method and apparatus for securing a computer-based game of chance,” U.S. Patent 6,203,427, March 20, 2001.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 6,163,771, December 19, 2000.

J.S. Walker, T.M. Sparico, T.S. Case, B. Schneier, “Conditional purchase offer management system for cruises,” U.S. Patent 6,134,534, October 17, 2000.

R. Martinez, B. Schneier, G. Guerin, “Virtual property system,” U.S. Patent 6,119,229, September 12, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for authenticating a document,” U.S. Patent 6,111,953, August 29, 2000.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,099,408, August 8, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 6,085,169, July 4, 2000.

J.S. Walker, B. Schneier, “Off-line remote lottery system,” U.S. Patent 6,024,640, February 15, 2000.

B. Schneier, J.M. Kelsey, “Event auditing system,” U.S. Patent 5,978,475, November 2, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, "Remote-auditing of computer generated outcomes, authenticated billing and access control, and software metering system using cryptographic and other protocols," U.S. Patent 5,970,143, October 19, 1999.

B. Schneier, J.M. Kelsey, "Digital signature with auditing bits," U.S. Patent 5,956,404, September 21, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for computer-based educational testing," U.S. Patent 5,947,747, September 7, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure document timestamping," U.S. Patent 5,923,763, July 13, 1999.

J.S. Walker, B. Schneier, T.S. Case, "Method and system for establishing and maintaining user-controlled anonymous communications," U.S. Patent 5,884,272, March 16, 1999.

J.S. Walker, B. Schneier, T.S. Case, "Method and system for facilitating an employment search incorporating user-controlled anonymous communications," U.S. Patent 5,884,270, March 16, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 5,871,398, February 16, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 5,862,223, January 19, 1999.

Schneier; Bruce, "Method and apparatus for analyzing information systems using stored tree database structures," U.S. Patent 5,850,516, December 15, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 5,828,751, October 27, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 5,794,207, August 11, 1998.

B. Schneier, J.S. Walker, J.A. Jorasch, "Remote-auditing of computer generated outcomes and authenticated biling and access control system using cryptographic and other protocols," U.S. Patent 5,768,382, June 16, 1998.

J.S. Walker, B. Schneier, "900 number billing and collection system and method for on-line computer services," U.S. Patent 5,737,414, April 7, 1998.

Published Crypto-Gram Issues

May 15, 2023: Swatting as a Service, Using LLMs to Create Bioweapons, EFF on the UN Cybercrime Treaty, New Zero-Click Exploits against iOS, Using the iPhone Recovery Key to Lock Owners Out of Their iPhones, Hacking Pickleball, UK Threatens End-to-End Encryption, Cyberweapons Manufacturer QuaDream Shuts Down, AI to Aid Democracy, Security Risks of AI, Hacking the Layoff Process, NIST Draft Document on Post-Quantum Cryptography Guidance, SolarWinds Detected Six Months Earlier, Large Language Models and Elections, AI Hacking Village at DEF CON This Year, PIPEDREAM Malware against Industrial Control Systems, FBI Disables Russian Malware, Building Trustworthy AI, Ted Chiang on the Risks of AI, Upcoming Speaking Engagements

April 15, 2023: NetWire Remote Access Trojan Maker Arrested, How AI Could Write Our Laws, Upcoming Speaking Engagements, US Citizen Hacked by Spyware, ChatGPT Privacy Flaw, Mass Ransomware Attack, Exploding USB Sticks, A Hacker’s Mind News, Hacks at Pwn2Own Vancouver 2023, Security Vulnerabilities in Snipping Tools, The Security Vulnerabilities of Message Interoperability, Russian Cyberwarfare Documents Leaked, UK Runs Fake DDoS-for-Hire Sites, North Korea Hacking Cryptocurrency Sites with 3CX Exploit, FBI (and Others) Shut Down Genesis Market, Research on AI in Adversarial Settings, LLMs and Phishing, Car Thieves Hacking the CAN Bus, FBI Advising People to Avoid Public Charging Stations, Bypassing a Theft Threat Model, Gaining an Advantage in Roulette, Hacking Suicide, Upcoming Speaking Engagements

March 15, 2023: Camera the Size of a Grain of Salt, ChatGPT Is Ingesting Corporate Secrets, Defending against AI Lobbyists, Fines as a Security System, The Insecurity of Photo Cropping, A Device to Turn Traffic Lights Green, Cyberwar Lessons from the War in Ukraine, Putting Undetectable Backdoors in Machine Learning Models, Banning TikTok, Side-Channel Attack against CRYSTALS-Kyber, Fooling a Voice Authentication System with an AI-Generated Voice, Dumb Password Rules, Nick Weaver on Regulating Cryptocurrency, New National Cybersecurity Strategy, Prompt Injection Attacks on Large Language Models, BlackLotus Malware Hijacks Windows Secure Boot Process, Another Malware with Persistence, Elephant Hackers, NetWire Remote Access Trojan Maker Arrested, How AI Could Write Our Laws, Upcoming Speaking Engagements

February 15, 2023: Hacked Cellebrite and MSAB Software Released, The FBI Identified a Tor User, AI and Political Lobbying, Security Analysis of Threema, Real-World Steganography, Publisher’s Weekly Review of A Hacker’s Mind, No-Fly List Exposed, Bulk Surveillance of Money Transfers, US Cyber Command Operations During the 2022 Midterm Elections, On Alec Baldwin’s Shooting, A Guide to Phishing Attacks, Kevin Mitnick Hacked California Law in 1983, NIST Is Updating Its Cybersecurity Framework, Ransomware Payments Are Down, Passwords Are Terrible (Surprising No One), AIs as Computer Hackers, Manipulating Weights in Face-Recognition AI Systems, A Hacker’s Mind News, Attacking Machine Learning Systems, Malware Delivered through Google Search, SolarWinds and Market Incentives, Mary Queen of Scots Letters Decrypted, Hacking the Tax Code, A Hacker’s Mind Is Now Published, On Pig Butchering Scams, What Will It Take?, Upcoming Speaking Engagements

January 15, 2023: A Security Vulnerability in the KmsdBot Botnet, Apple Patches iPhone Zero-Day, As Long as We’re on the Subject of CAPTCHAs, How to Surrender to a Drone, Trojaned Windows Installer Targets Ukraine, Ukraine Intercepting Russian Soldiers’ Cell Phone Calls, Critical Microsoft Code-Execution Vulnerability, Hacking the

JFK Airport Taxi Dispatch System, LastPass Breach, Arresting IT Administrators, QR Code Scam, Recovering Smartphone Voice from the Accelerometer, Breaking RSA with a Quantum Computer, Decarbonizing Cryptocurrencies through Taxation, Remote Vulnerabilities in Automobiles, Schneier on Security Audiobook Sale, Identifying People Using Cell Phone Location Data, ChatGPT-Written Malware, Experian Privacy Vulnerability, Threats of Machine-Generated Text, Booklist Review of A Hacker's Mind, Upcoming Speaking Engagements

December 15, 2022: Another Event-Related Spyware App, Russian Software Company Pretending to Be American, Failures in Twitter's Two-Factor Authentication System, Successful Hack of Time-Triggered Ethernet, First Review of A Hacker's Mind, Breaking the Zeppelin Ransomware Encryption Scheme, Apple's Device Analytics Can Identify iCloud Users, The US Has a Shortage of Bomb-Sniffing Dogs, Computer Repair Technicians Are Stealing Your Data, Charles V of Spain Secret Code Cracked, Facebook Fined $276M under GDPR, Sirius XM Software Vulnerability, LastPass Security Breach, Existential Risk and the Fermi Paradox, CAPTCHA, CryWiper Data Wiper Targeting Russian Sites, The Decoupling Principle, Leaked Signing Keys Are Being Used to Sign Malware, Security Vulnerabilities in Eufy Cameras, Hacking Trespass Law, Apple Is Finally Encrypting iCloud Backups, Obligatory ChatGPT Post, Hacking Boston's CharlieCard, Reimagining Democracy

November 15, 2022: New Book: A Hacker's Mind, Hacking Automobile Keyless Entry Systems, Qatar Spyware, Museum Security, Interview with Signal's New President, Adversarial ML Attack that Secretly Gives a Language Model a Point of View, On the Randomness of Automatic Card Shufflers, Australia Increases Fines for Massive Data Breaches, Critical Vulnerability in Open SSL, Apple Only Commits to Patching Latest OS Version, Iran's Digital Surveillance Tools Leaked, NSA on Supply Chain Security, The Conviction of Uber's Chief Security Officer, Using Wi-FI to See through Walls, Defeating Phishing-Resistant Multifactor Authentication, An Untrustworthy TLS Certificate in Browsers, NSA Over-surveillance, A Digital Red Cross, Upcoming Speaking Engagements

October 15, 2022: Relay Attack against Teslas, Massive Data Breach at Uber, Large-Scale Collection of Cell Phone Data at US Borders, Credit Card Fraud That Bypasses 2FA, Automatic Cheating Detection in Human Racing, Prompt Injection/Extraction Attacks against AI Systems, Leaking Screen Information on Zoom Calls through Reflections in Eyeglasses, Leaking Passwords through the Spellchecker, New Report on IoT Security, Cold War Bugging of Soviet Facilities, Differences in App Security/Privacy Based on Country, Security Vulnerabilities in Covert CIA Websites, Detecting Deepfake Audio by Modeling the Human Acoustic Tract, NSA Employee Charged with Espionage, October Is Cybersecurity Awareness Month, Spyware Maker Intellexa Sued by Journalist, Complex Impersonation Story, Inserting a Backdoor into a Machine-Learning System, Recovering Passwords by Measuring Residual Heat, Digital License Plates, Regulating DAOs, Upcoming Speaking Engagements

September 15, 2022: $23 Million YouTube Royalties Scam, Remotely Controlling Touchscreens, Zoom Exploit on MacOS, USB "Rubber Ducky" Attack Tool, Hyundai Uses Example Keys for Encryption System, Signal Phone Numbers Exposed in Twilio

Hack, Mudge Files Whistleblower Complaint against Twitter, Man-in-the-Middle Phishing Attack, Security and Cheap Complexity, Levels of Assurance for DoD Microelectronics, FTC Sues Data Broker, High-School Graduation Prank Hack, Clever Phishing Scam Uses Legitimate PayPal Messages, Montenegro Is the Victim of a Cyberattack, The LockBit Ransomware Gang Is Surprisingly Professional, Facebook Has No Idea What Data It Has, Responsible Disclosure for Cryptocurrency Security, New Linux Cryptomining Malware, FBI Seizes Stolen Cryptocurrencies, Weird Fallout from Peiter Zatko's Twitter Whistleblowing, Upcoming Speaking Engagements

August 15, 2022: San Francisco Police Want Real-Time Access to Private Surveillance Cameras, Facebook Is Now Encrypting Links to Prevent URL Stripping, NSO Group's Pegasus Spyware Used against Thailand Pro-Democracy Activists and Leaders, Russia Creates Malware False-Flag App, Critical Vulnerabilities in GPS Trackers, Apple's Lockdown Mode, Securing Open-Source Software, New UEFI Rootkit, Microsoft Zero-Days Sold and Then Used, Ring Gives Videos to Police without a Warrant or User Consent, Surveillance of Your Car, Drone Deliveries into Prisons, SIKE Broken, NIST's Post-Quantum Cryptography Standards, Hacking Starlink, A Taxonomy of Access Control, Twitter Exposes Personal Information for 5.4 Million Accounts, Upcoming Speaking Engagements

July 15, 2022: M1 Chip Vulnerability, Attacking the Performance of Machine Learning Systems, Tracking People via Bluetooth on Their Phones, Hertzbleed: A New Side-Channel Attack, Hidden Anti-Cryptography Provisions in Internet Anti-Trust Bills, Symbiote Backdoor in Linux, On the Subversion of NIST by the NSA, On the Dangers of Cryptocurrencies and the Uselessness of Blockchain, 2022 Workshop on Economics and Information Security (WEIS), When Security Locks You Out of Everything, Ecuador's Attempt to Resettle Edward Snowden, ZuoRAT Malware Is Targeting Routers, Analyzing the Swiss E-Voting System, NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, Ubiquitous Surveillance by ICE, Apple's Lockdown Mode, Nigerian Prison Break, Security Vulnerabilities in Honda's Keyless Entry System, Post-Roe Privacy, New Browser De-anonymization Technique, Upcoming Speaking Engagements

June 15, 2022: The NSA Says that There are No Known Flaws in NIST's Quantum-Resistant Algorithms, Attacks on Managed Service Providers Expected to Increase, iPhone Malware that Operates Even When the Phone Is Turned Off, Websites that Collect Your Data as You Type, Bluetooth Flaw Allows Remote Unlocking of Digital Locks, The Onion on Google Map Surveillance, Forging Australian Driver's Licenses, The Justice Department Will No Longer Charge Security Researchers with Criminal Hacking, Manipulating Machine-Learning Systems through the Order of the Training Data, Malware-Infested Smart Card Reader, Security and Human Behavior (SHB) 2022, The Limits of Cyber Operations in Wartime, Clever -- and Exploitable -- Windows Zero-Day, Remotely Controlling Touchscreens, Me on Public-Interest Tech, Long Story on the Accused CIA Vault 7 Leaker, Leaking Military Secrets on Gaming Discussion Boards, Smartphones and Civilians in Wartime, Twitter Used Two-Factor Login Details for Ad Targeting, Cryptanalysis of ENCSecurity's Encryption Implementation, Hacking Tesla's Remote Key Cards, Upcoming Speaking Engagements

Earlier issues of Crypto-Gram are available here:
https://www.schneier.com/crypto-gram/

Significant Articles about Schneier

“What If Generative AI Destroys Biometric Security?,” *The Economist*, May 31, 2023.

“Book Review: A Hacker’s Mind by Bruce Schneier,” *Web Informant*, May 27, 2023.

“Is This A Hack? Increased AirBnB Bookings,” *Cybercrime Magazine*, May 20, 2023.

“AppSec Decoded: Bruce Schneier on the Future of AI,” *Synopsys Software Integrity*, May 1, 2023.

“Is This A Hack? Cheaper Travel Expenses,” *Cybercrime Magazine*, May 1, 2023.

“Bruce Schneier’s Plan to Reinvent Democracy,” *SiliconANGLE*, May 1, 2023.

“Sounds About Right: Audiobooks to Help Us Understand the World,” *Sounds About Right*, April 24, 2023.

“Is This A Hack? Password Sharing On Netflix,” *Cybercrime Magazine*, April 21, 2023.

“Bruce Schneier on His New Book, *A Hacker’s Mind*,” *GrowthPolicy*, April 20, 2023.

“Hacking Procedure,” *California Litigation Vol. 36 Iss. 1 (2023)*, April 19, 2023.

“Is the Future Secure?,” *The Futurists Podcast*, April 14, 2023.

“Is This A Hack? Beating The Customer Service Phone Line,” *Cybercrime Magazine*, April 3, 2023.

“No Name Podcast with Bruce Schneier,” *No Name Podcast*, March 28, 2023.

“Is This A Hack? Generating Income From Your Home,” *Cybercrime Magazine*, March 24, 2023.

“Bruce Schneier Wants to Recreate Democracy,” *Harvard Kennedy School Ash Center*, March 19, 2023.

“Thought Leadership: Bruce Schneier on *A Hacker’s Mind*,” *Cyber Security America*, March 14, 2023.

“Is This a Hack? Theme Park Rides,” *Cybercrime Magazine*, March 7, 2023.

“Sociotechnical Exploitation with Bruce Schneier,” *BarCode*, March 3, 2023.

“*A Hacker’s Mind*. New Book. Bruce Schneier, Security Technologist and Cryptographer,” *Cybercrime Magazine*, March 2, 2023.

“Inside the ‘Hacker’ Culture of the Rich and Powerful,” *Marketplace*, February 28, 2023.

“"Hacker’s Mind" Meets Lawyer’s Mind,” *Cyberlaw Podcast*, February 24, 2023.

“An Interview with Bruce Schneier (Part of the World-leaders in Cryptography series),” *Bill Buchanan OBE*, February 24, 2023.

“A Hacker’s Mind: How the Powerful Bend Society’s Rules, and How to Bend Them Back,” *Dispatches from the War Room*, February 17, 2023.

“How Hacking Benefits the Rich and Powerful With Bruce Schneier,” *Executive Security*, February 13, 2023.

“A Hacker’s Mind—How the Elites Exploit the System,” *Financial Times*, February 10, 2023.

“Hacking and the Social Contract,” *Science*, February 10, 2023.

“Bruce Schneier Goes Inside the Minds of Hackers in New Book,” *Cool Science Radio*, February 9, 2023.

“Review: Digital Tech Advances, AI Spur Hacking of Society,” *Associated Press*, February 8, 2023.

“A Hacker’s Mind: Bruce Schneier on How the Powerful Bend Society’s Rules and How to Bend Them Back,” *Keen On*, February 7, 2023.

“Artificial Intelligence,” *Disinformation*, February 7, 2023.

“The Lawfare Podcast: The Hacker’s Mind,” *Lawfare*, February 7, 2023.

“How to Know if You’re a Hacker, and Other Life Hacks,” *New York Times*, February 7, 2023.

“Pluralistic: Bruce Schneier’s *A Hacker’s Mind* (06 Feb 2023),” *Pluralistic*, February 6, 2023.

“Hacking to Harm and Heal Democracy,” *Harvard Kennedy School Ash Center*, January 31, 2023.

“Understanding The Hacker’s Mind and Your Ever Shrinking Attention Span,” *Something You Should Know*, January 27, 2023.

“*A Hacker’s Mind* (Book Review),” *Publishers Weekly*, January 20, 2023.

“Secure Democratic Election Technology,” *Type One Planet*, January 12, 2023.

“*A Hacker’s Mind* (book review),” *Booklist*, January 1, 2023.

“*Firewalls Don’t Stop Dragons* 300th Episode” (podcast) November 28, 2022.

“Book Review: *A Hacker’s Mind*,” *Kirkus Reviews*, November 16, 2022.

“‘Hacking’ the Legal System,” Bruce Schneier interview, *Aiming for the Moon* podcast, September 11, 2022.

“Bruce Schneier on the Crypto/Blockchain Disaster,” *Cyber Protection Magazine*, August 11, 2022.

“Understanding Crypto 6: Bruce Schneier: Security, Trust, and Blockchain,” *Rational Reminder*, July 8, 2022.

“Schneier: “Le votazioni elettroniche? Non fatelo, non è sicuro”,” *Cybersecurity 360*, July 04, 2022.

“Expert Interviews: Hacktivism,” *Cyber.RAR*, June 29, 2022.

“Why AIs Will Become Hackers,” *Dark Reading*, June 09, 2022.

“Schneier on Security for Tomorrow’s Software,” *The Changelog*, May 20, 2022.

“Unscripted with Bruce Schneier,” *PSICC Data Privacy Week 2022*, February 04, 2022.

“Bruce Schneier on Regulating at the Pace of Tech,” *Transform*, February 01, 2022.

“History of Hacking,” *Cybercrime Magazine*, January 29, 2022.

“We Have to Trust Technology,” *Conversation with Nobel Minds*, January 09, 2022.

“Bruce Schneier on Regulating at the Pace of Tech,” *Transform*, December 30, 2021.

“*Click Here to Kill Everybody*,” *Conversation with Nobel Minds*, December 26, 2021.

“Who’s Controlling the Internet?” *Project Save the World*, October 28, 2021.

“Bruce Schneier’s book *Secrets and Lies*,” *Byte*, October 18, 2021.

“"העשירים אלא האקרים מבצעים לא ביותר המסוכנות הפריצות את"," *Calcalist*, September 08, 2021.

“Click Here To Kill Everybody,” *Power Corrupts*, September 07, 2021.

“Bruce Schneier: We Are Asking the Wrong Cybersecurity Questions,” *CDO Trends*, August 23, 2021.

“Secure Ventures Podcast,” *Secure Ventures with Kyle McNulty*, July 27, 2021.

“Going Meta: A Conversation and AMA with Bruce Schneier,” *8th Layer Insights*, July 20, 2021.

“The Coming AI Hackers. How Will They Put Society At Risk?,” *Cybercrime Magazine*, June 15, 2021.

“The Coming AI Hackers,” *Exponential View*, June 09, 2021.

"The Next Phase in Cyber Warfare," *The Red Line*, May 16, 2021.

"When AI Becomes the Hacker," *Dark Reading*, May 13, 2021.

"Hacking Is a Task AI Will Excel at (And We Are Not Far from That Point)," *ZDNet*, May 06, 2021.

"Bruce Schneier Wants You to Make Software Better," *IEEE Spectrum*, April 28, 2021.

"Data, Surveillance & Internet Security with Bruce Schneier," *CSINT Conversations*, March 03, 2021.

"Artificial Intelligence in Politics," *Unpublished Cafe*, February 19, 2021.

"Cybersecurity: Same Threats, New Challenges," *Forbes*, January 19, 2021.

"Bruce Schneier on Technology Security, Social Media, and Regulation," *GrowthPolicy*, January 13, 2021.

"The Solarwinds Hack Is Stunning. Here's What Should Be Done," *CNN*, January 5, 2021.

"The US Has Suffered a Massive Cyberbreach. It's Hard to Overstate How Bad It Is," *Guardian*, December 24, 2020.

"The Peril of Persuasion in the Big Tech Age," *Foreign Policy*, December 11, 2020.

"What Makes Trump's Subversion Efforts So Alarming? His Collaborators," *New York Times*, November 23, 2020.

"The Unrelenting Horizonlessness of the Covid World," *CNN*, September 25, 2020.

"The Twitter Hacks Have to Stop," *Atlantic*, July 18, 2020.

"Bruce Schneier says we need to embrace inefficiency to save our economy," *Quartz*, June 30, 2020.

"The Public Good Requires Private Data," *Foreign Policy*, May 16, 2020.

"Heise Webinar," *Heise Events*, April 15, 2020.

"An Interview with Bruce Schneier, Renowned Security Technologist," *The Politic*, April 1, 2020.

"Breaking Down the Huawei v. Pentagon Dispute," *Federal Drive*, March 26, 2020.

"How to Detect Coronavirus Myths, Scams and Fake News: Security Guru Bruce Schneier Weighs In On COVID-19," *Seattle 24x7*, March 15, 2020.

"#RSAC: How to Hack Society," *Infosecurity*, February 27, 2020.

"What's the Best Way to Use the Cloud to Store Personal Data?," *The Wall Street Journal*, February 23, 2020.

“Bruce Schneier: On the Future of Public-Interest Tech,” *Humans of InfoSec*, February 19, 2020.

“Not Just about the Data,” *Science Node*, February 17, 2020.

“Bruce Schneier on How Insecure Electronic Voting Could Break the United States—and Surveillance Without Tyranny,” *80000 Hours*, October 25, 2019.

“‘Click Here To Kill Everybody’ Book Review by Cybersecurity Expert Scott Schober,” *YouTube*, October 18, 2019.

“What You Need to Know about Security in Government,” *Code for America*, August 29, 2019.

“Wanted: ‘Public-Interest Technologists’ to Inform Raging Debates on Cybersecurity Policy,” *Inside Cybersecurity*, August 12, 2019.

“Autonomous Vehicle Security Deep Dive w/Bruce Schneier,” *Thinking through Automony*, August 7, 2019.

“Bruce Schneier Talks the Cybersecurity Risks of an Autonomous Future,” *Thinking Through Automony*, July 22, 2019.

“‘Tu Coche Ya Está Conectado a Internet y Ahora Cualquiera Puede Usarlo para Matarte,’” *El Confidencial*, July 11, 2019.

“Bruce Schneier Is Leaving IBM,” *SecureWorld*, July 3, 2019.

“Bruce Schneier Moves on from IBM,” *SecurityWeek*, July 2, 2019.

“Don’t Tell Alice and Bob: Security Maven Bruce Schneier Is Leaving IBM,” *The Register*, July 1, 2019.

“SwigCast, Episode 2: Encryption,” *The Daily Swig*, June 27, 2019.

“Apocalipsis digital: cómo evitar que el ser humano se extinga por culpa de internet,” *El Mundo*, June 25, 2019.

“How Government Can Secure Us in the Internet+ Era,” *The Government We Need*, June 18, 2019.

“Bruce Schneier on Cybersecurity,” *Challenging Opinions*, June 3, 2019.

“Scrambled Hidden Potato Device with Bruce Schneier,” *Random but Memorable*, May 21, 2019.

“Black Hat Q&A: Bruce Schneier Calls For Public-Interest Technologists,” *Dark Reading*, May 20, 2019.

“Summit 2019: Cybersecurity and Public Interest Tech with Bruce Schneier,” *Code for America*, April 24, 2019.

"Is Online Convenience Worth the Trade-Off for Less Cybersecurity?," *BYU Radio*, April 15, 2019.

"傳奇密碼學大師專訪：別輕信物聯網," *Business Weekly*, April 10, 2019.

"Collective Intelligence Podcast, Bruce Schneier on Public-Interest Tech ," *Flashpoint*, April 1, 2019.

"Q&A: Crypto-Guru Bruce Schneier on Teaching Tech to Lawmakers, Plus Privacy Failures—and a Call to Techies to Act," *The Register*, March 15, 2019.

"Security Concerns Rise As More Household Items Join The Internet World," *Wisconsin Public Radio*, January 29, 2019.

"The Existential Threat of Hyper-Connecting the World," *Decentralize This!*, January 29, 2019.

"Data Privacy Day Episode of 'Firewalls Don't Stop Dragons,'" *Firewalls Don't Stop Dragons*, January 28, 2019.

"The Missing Piece in Cybersecurity is Government," *Defence24*, January 25, 2019.

"The Security Book Everyone in Government Must Read in 2019," *GovFresh*, December 23, 2018.

"Ben's Book of the Month: Review of 'Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,'" *RSA Conference Blog*, November 30, 2018.

"Has Your Toaster Got Cyber-Security? It May Soon Need It," *Catholic Herald*, November 29, 2018.

"Click Here to Kill Everybody, IoT Security and Cryptography," *The NULLCON Podcast*, November 26, 2018.

"Click Here to Kill Everybody: Security, Privacy, Social Media and Politics," *Fringe.fm*, November 12, 2018.

"Harry Shearer Interviews Bruce Schneier," *Le Show*, November 11, 2018.

"'Click Here to Kill Everybody,'" *The Cyberwire*, November 9, 2018.

"'Click Here To Kill Everybody,' with Bruce Schneier," *Steal This Show*, November 1, 2018.

"A Future Where Everything Becomes a Computer Is as Creepy as You Feared," *The New York Times*, October 10, 2018.

"How to Keep the Internet of Things From Killing Us All," *Pacific Standard*, October 9, 2018.

"The Biggest Cybersecurity Threat You Never Thought That Much About Is the Factory," *Marketplace*, October 9, 2018.

“Bruce Schneier’s Click Here to Kill Everybody Reveals the Looming Cybersecurity Crisis,” *CSO*, October 3, 2018.

“Cybersecurity, the Internet of Things, and Social Media,” *Social Media and Politics Podcast*, September 30, 2018.

“‘Click Here to Kill Everybody’: A Berkman Klein Center Book Talk,” *Berkman Klein Center*, September 25, 2018.

“Publisher’s Weekly Review of *Click Here to Kill Everybody*,” *Publisher's Weekly*, September 24, 2018.

“Cyberattacks and Survival in a Hyperconnected World,” *Hidden Forces Podcast*, September 18, 2018.

“The Lawfare Podcast: Bruce Schneier on ‘Click Here to Kill Everybody,’” *The Lawfare Podcast*, September 18, 2018.

“Bruce Schneier Book Talk with Ben Wizner,” *Center on National Security at Fordham Law*, September 17, 2018.

“Open Letters Review on *Click Here to Kill Everybody*,” *Open Letters Review*, September 14, 2018.

“Internet Plus: Now Everything Can Be Hacked!,” *CBC Radio*, September 14, 2018.

“The Cyberlaw Podcast: Click Here to Kill Everybody,” *The Cyberlaw Podcast*, September 11, 2018.

“Takeaways from Bruce Schneier’s New Book,” *Politico*, September 11, 2018.

“Podcast Episode 111: Click Here to Kill Everybody and CyberSN on Why Security Talent Walks,” *The Security Ledger*, September 10, 2018.

“Book Launch at The Aspen Institute,” *The Aspen Institute*, September 10, 2018.

“For Safety’s Sake, We Must Slow Innovation in Internet-Connected Things,” *MIT Technology Review*, September 6, 2018.

“Book Review: Click Here to Kill Everybody,” *Virus Bulletin*, September 6, 2018.

“Vulnerabilities of an Inter-connected World ,” *Midday on WNYC*, September 5, 2018.

“Book Review: ‘Click Here To Kill Everybody,’” *Harris Online*, September 4, 2018.

“Schneier’s ‘Click Here To Kill Everybody,’” *Boing Boing*, September 4, 2018.

“Hackers Used a Fish Tank to Break into a Vegas Casino. We’re All in Trouble.,” *The Washington Post*, September 4, 2018.

“Kirkus Review: Click Here To Kill Everybody,” *Kirkus Reviews*, September 4, 2018.

“Radio Interview on ‘Click Here To Kill Everybody,’” *NPR 1A*, September 4, 2018.

“How to Survive in a Hyperconnected World,” *Ford Foundation*, August 29, 2018.

“Governments Want Your Smart Devices to Have Stupid Security Flaws,” *Nature*, August 28, 2018.

“Click Here to Kill Everybody by Bruce Schneier,” *Financial Times*, August 26, 2018.

“Newsmaker Interview: Bruce Schneier on ‘Going Dark’ and the Crypto Arms Race,” *Threatpost*, July 16, 2018.

“[Book Review] Data and Goliath by Bruce Schneier ,” *Center for Digital Society*, May 9, 2018.

“Schneier Talks Cyber Regulations, Slams U.S. Lawmakers,” *SearchSecurity*, April 19, 2018.

“Collective Intelligence Podcast, Bruce Schneier on Data Collection and Privacy,” *Flashpoint*, April 17, 2018.

“The Truth About Terrorism with Bruce Schneier,” *Kensington TV*, January 11, 2018.

“Schneier: It’s Time to Regulate IoT to Improve Cyber-Security,” *eWeek*, November 15, 2017.

“An Interview with Bruce Schneier on the Internet of Things, Global Surveillance, and Cybersecurity,” *ExpressVPN*, October 24, 2017.

“The Cybersecurity Canon: Data and Goliath,” *Palo Alto Networks*, October 8, 2017.

“On Internet Privacy, Be Very Afraid,” *Harvard Gazette*, August 24, 2017.

“Is It Time To Regulate the IoT?,” *SecTor*, August 11, 2017.

“‘Surveillance Is the Business Model of the Internet,’” *OpenDemocracy*, July 18, 2017.

Earlier news articles are available here: https://www.schneier.com/news/

Previous Declarations and Depositions

Anibal Rodrigues, Sal Cataldo, Julian Santiago, and Susan Lynn, , individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-04688-RS, United States District Court for the Northern California District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2023).

Chasom Brown, William Byatt, Jeremy David, Christopher Castillo, and Monique Trujillo, individually and on behalf of all similarly situated v. Google LLC, Case No. 4:20-cv-03664-YGR-SVK, United States District Court for the Northern California

District. Expert witness for Brown et. al., Susman Godfrey LLP, attorneys. Declarations and deposition (2022).

Mon Cheri Bridals, LLC and Maggie Sottero Designs, LLC v. Cloudflare, Inc., Case No. 2:18-cv-09453-MWF-AS, United States District Court for the Central District of California. Expert witness for Cloudflare, Inc., Fenwick & West, LLP, attorneys. Declarations (2020 and 2021).

Fortinet, Inc. v. BT Americas, Inc., Case No. IPR2019-01324, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 7,895,641. Expert witness for BT Americas, Inc., Proskaur Rose LLP, attorneys. Declaration (2019).

United to Protect Democracy et al. v. Presidential Advisory Commission on Election Integrity et al., Civil Action No. 1:17-cv-02016, United States District Court for the District of Columbia. Declaration (2017).

Koninklijke Philips N.V. and U.S. Philips Corp. v. HTC Corp. and HT America, Civil Action No. 15-1126-GMS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 8.543.819 and 9.436.809. Expert witness for HTC Corp., Perkins Coie LLP, attorneys. Declaration (2017).

Ex parte reexamination of U.S. Patent No. 6,760,752. Expert witness for the patent holder Zix Corp., Haynes and Boone, LLC attorneys. Declaration (2017).

Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co. v. Transpacific IP Ltd, Case No. IPR2015-00x, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 8,929,555. Expert witness for Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co., Sidley Austin LLP attorneys. Declaration (2015).

Unikey Technologies, Inc. v. Assa Abloy AB, Cases No. IPR2015-01440 and IPR2015-01441, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 7,706,778 and 8,150,374. Expert witness for UniKey Technologies, Inc., Proskauer Rose LLP attorneys. Declaration (2015).

Epicor Software Corp. v. Protegrity Corp., Case Nos. CBM2015-00002 and CBM2015-00006, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,321,201 and 8,402.281. Expert witness for Epicor Software Corp., Cantor Colborn LLP attorneys. Declaration (2015) and deposition (2015).

Quantum World Corp. v. Dell, Inc. Civil Action No. A-11-CA-688-SS, United States District Court for the Western Division of Texas regarding U.S. Patent Nos. 6,763,364, 7,096,242, and 7,752,247. Expert witness for Dell, Inc., Alston & Bird attorneys. Declaration and deposition (2015).

Entrust, Inc. v. Secure Axcess, LLC, Case No. CBM2015-0027, Covered Business Method Review United States Patent and Trademark Office before the Patent Trial and Appeal Board concerning Patent No. 7,631,191. Expert witness for Entrust, Inc., Crowell & Morning LLP attorneys. Declaration (2014) and deposition (2015).

Apple, Inc. v. Achates Reference Publishing, Inc., Case Nos. IPR 13-00080 and IPR 13-00081, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,173,403 and 5,982,889. Expert witness for Apple, Inc., DiNovo Price LLP and Sidley Austin LLP attorneys. Declaration and deposition.

Research in Motion Corp. v. Innovative Sonic, Docket No. 377211US, Inter Partes Review, United States Patent and Trademark Office regarding Patent No. 6,925,183. Expert witness for Research In Motion Corp., Expert witness for Research in Motion Corp., Oblon Spivak attorneys. Declaration.

Walker Digital, LLC v. MySpace, Inc., et al., Civil Action No. 1:11-cs-00318-LPS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 5,884,270 and 5,884,272. Deposition as patent author.

Walker Digital, LLC v. Google, Inc., et al., Civil Action No. 11-309-SLR, United States District Court for the District of Delaware, concerning U.S. Patent No. 5,768,382. Deposition as patent author.

TecSec, Inc. v. International Business Machines Corp., et al., Civil Action No. 1:10-cv-00115-LMB/TCB, United States District Court for the Eastern District of Virginia (Alexandria) concerning U.S. Patents No. 5,369,702 and 6,549,623. Expert witness for TecSec, Inc., Hunton & Williams LLP, attorneys for TecSec, Inc. Declaration and deposition.

Luciano F. Paone v. Microsoft Corp., Civil Action No. CV-07-2973 (E.D. NY), United States District Court for the Northern District of California concerning U.S. Patent No. 6,259,789. Expert witness for Microsoft Corp., Kirkland & Ellis attorneys. Declaration and deposition.

Fred and Kathleen Stark v. The Seattle Seahawks LLC, Civil Action No. CV-06-1719 JLR, United States District Court for the Western District of Washington at Seattle concerning the efficacy of pat-down searches. Expert witness for Stark, Danielson Harrigan Leyh & Tollefson LLC, attorneys for Stark. Declaration and deposition.

Gordon Johnston v. The Tampa Sports Authority et al., Civil Action No. 8-05-cv-02191-JDW-MAP, United States District Court for the Middle District of Florida Tampa Division. concerning the efficacy of pat-down searches. Expert witness for Johnston. Declaration.