UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORTINET INC.,
Petitioner,

v.

BT AMERICAS INC.,
Patent Owner.

Case IPR2019-01325
Patent 7,159,237

DECLARATION OF BRUCE SCHNEIER IN SUPPORT OF BT AMERICAS INC.'S PRELIMINARY RESPONSE UNDER 35 U.S.C. §313 AND 37 C.F.R. §42.107(a)

1. My name is Bruce Schneier and I am the first-named inventor on United States Patent Nos. 7,159,237 and 7,895,641 (respectively, the " '237 and '641 patents").

2. I am a well-known security technologist. I am currently 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, and the Tor Project, an advisory board member of EPIC and VerifiedVoting.org, and the chief security architect at Inrupt, Inc. In addition to the hundreds of articles, essays, and academic articles I have written that relate to cybersecurity, I also author a newsletter and blog (Schneier on Security) that is read by over 250,000 people. A copy of a current CV, which I have reviewed and is accurate, is attached as Exhibit A.

3. In the summer of 1999, my partner Tom Rowley and I formed Counterpane Internet Security, Inc., a managed security monitoring service. Counterpane's successful implementation of technology described in the '237 and '641 patents spawned an entirely new product category -- called Managed Security Monitoring -- which has since come to be a very large commercial space.

.

4. Jon Callas and Andrew Gross, both of whom are named as co-inventors in the '237 and '641 patents, were among the first people hired by Counterpane. Both were talented and knowledgeable experts in network security even at the time Counterpane hired them.

5. The systems architecture and method of operation described in the '237 and '641 patents, including the source code for the software, was being developed and operated as we wrote the patent application that resulted in the '237 and '641 patents.

6. That architecture and those methods of operation, including the analysis of residual status data to identify potential security events for further analysis, was built, operated and offered as a managed security service for customers in and after the year 2000. That business was quite successful, and built upon the technology described in the '237 and '641 patents.

7. As a result of Counterpane's success, BT became interested in Counterpane, and acquired the company in 2006.

8. I continued to work at Counterpane after its acquisition by BT until

2012. At the time I left the company to pursue other interests, BT/Counterpane was still operating a successful business built upon technology described in the '237 and '641 patents.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Dated: 26 August 2019

Bruce Schneier

EXHIBIT A

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 author of 14 books—including the *New York Times* best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*—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 and the Tor Project, and an advisory board member of EPIC and VerifiedVoting.org. He is also a special advisor to IBM Security and the Chief Technology Officer of IBM Resilient.

Professional Experience

2016+, Chief Technology Officer, IBM Resilient (formerly Resilient: an IBM Company) 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, John F. Kennedy School of Government, Harvard University.

2016+, 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

2016+, Board Member, Tor Project, Cambridge, MA.

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

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

Education

M.S. Computer Science, American University, 1986.

B.S. Physics, University of Rochester, 1984.

Books

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

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

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*, 2017, to appear.

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

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

"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 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

April 15, 2019: Critical Flaw in Swiss Internet Voting System, Upcoming Speaking Engagements, I Was Cited in a Court Decision, CAs Reissue Over One Million Weak Certificates, Triton, An Argument that Cybersecurity Is Basically Okay, Zipcar Disruption, First Look Media Shutting Down Access to Snowden NSA Archives, Enigma, Typex, and Bombe Simulators, Mail Fishing, Personal Data Left on Used Laptops, Programmers Who Don't Understand Security Are Poor at Security, Malware Installed in Asus Computers through Hacked Update Process, NSA-Inspired Vulnerability Found in Huawei Laptops, Recovering Smartphone Typing from Microphone Sounds, Hacking Instagram to Get Free Meals in Exchange for Positive Reviews, How Political Campaigns Use Personal Data, Adversarial Machine Learning against Tesla's Autopilot, Former Mozilla CTO Harassed at the US Border, Unhackable Cryptography?, Ghidra: NSA's Reverse-Engineering Tool, Hey Secret Service: Don't Plug Suspect USB Sticks into Random Computers, How the Anonymous Artist Banksy Authenticates His or Her Work, TajMahal Spyware, New Version of Flame Malware Discovered, Maliciously Tampering with Medical Imagery,

March 15, 2019: Cataloging IoT Vulnerabilities, I Am Not Associated with Swift Recovery Ltd., Estonia's Volunteer Cyber Militia, Details on Recent DNS Hijacking, Reverse Location Search Warrants, Gen. Nakasone on US Cyber Command, On the Security of Password Managers, Attacking Soldiers on Social Media, “Insider Threat” Detection Software, Can Everybody Read the US Terrorist Watch List?, Data Leakage from Encrypted Databases, The Latest in Creepy Spyware, Cybersecurity for the Public Interest, Digital Signatures in PDFs Are Broken, Letterlocking, Detecting Shoplifting Behavior, Cybersecurity Insurance Not Paying for NotPetya Losses, Videos and Links from the Public-Interest Technology Track at the RSA Conference, Russia Is Testing Online Voting, On Surveillance in the Workplace, Judging Facebook's Privacy Shift, DARPA Is Developing an Open-Source Voting System, Upcoming Speaking Engagements,

February 15, 2019: Alex Stamos on Content Moderation and Security, El Chapo's Encryption Defeated by Turning His IT Consultant, Prices for Zero-Day Exploits Are Rising, Evaluating the GCHQ Exceptional Access Proposal, Clever Smartphone Malware Concealment Technique, Hacking Construction Cranes, The Evolution of Darknets, Military Carrier Pigeons in the Era of Electronic Warfare, Hacking the GCHQ Backdoor, Japanese Government Will Hack Citizens' IoT Devices, iPhone FaceTime Vulnerability, Security Analysis of the LIFX Smart Light Bulb, Security Flaws in Children's Smart Watches, Public-Interest Tech at the RSA Conference, Facebook's New Privacy Hires, Major Zcash Vulnerability Fixed, Using Gmail “Dot Addresses” to Commit Fraud, China's AI Strategy and its Security Implications, Blockchain and Trust, Cyberinsurance and Acts of War, USB Cable with Embedded Wi-Fi Controller, Reconstructing SIGSALY,

January 15, 2019: New Shamoon Variant, Teaching Cybersecurity Policy, Congressional Report on the 2017 Equifax Data Breach, Fraudulent Tactics on Amazon Marketplace, Drone Denial-of-Service Attack against Gatwick Airport, MD5 and SHA-1 Still Used in

2018, Glitter Bomb against Package Thieves, Human Rights by Design, Stealing Nativity Displays, Massive Ad Fraud Scheme Relied on BGP Hijacking, *Click Here to Kill Everybody* Available as an Audiobook, China's APT10, Long-Range Familial Searching Forensics, Podcast Interview with Eva Galperin, New Attack Against Electrum Bitcoin Wallets, Machine Learning to Detect Software Vulnerabilities, EU Offering Bug Bounties on Critical Open-Source Software, Security Vulnerabilities in Cell Phone Systems, Using a Fake Hand to Defeat Hand-Vein Biometrics, Why Internet Security Is So Bad, Upcoming Speaking Engagements,

December 15, 2018: Chip Cards Fail to Reduce Credit Card Fraud in the US, Hidden Cameras in Streetlights, Mailing Tech Support a Bomb, Israeli Surveillance Gear, Worst-Case Thinking Breeds Fear and Irrationality, What Happened to Cyber 9/11?, The PCLOB Needs a Director, Information Attacks against Democracies, Using Machine Learning to Create Fake Fingerprints, How Surveillance Inhibits Freedom of Expression, Propaganda and the Weakening of Trust in Government, Distributing Malware By Becoming an Admin on an Open-Source Project, FBI Takes Down a Massive Advertising Fraud Ring, That Bloomberg Supply-Chain-Hack Story, Three-Rotor Enigma Machine Up for Auction Today, *Click Here to Kill Everybody* News, The DoJ's Secret Legal Arguments to Break Cryptography, Bad Consumer Security Advice, Security Risks of Chatbots, Your Personal Data is Already Stolen, Banks Attacked through Malicious Hardware Connected to the Local Network, Back Issues of the NSA's *Cryptolog*, 2018 Annual Report from AI Now, New Australian Backdoor Law, Marriott Hack Reported as Chinese State-Sponsored, Real-Time Attacks Against Two-Factor Authentication,

November 15, 2018: How DNA Databases Violate Everyone's Privacy, Privacy for Tigers, Government Perspective on Supply Chain Security, West Virginia Using Internet Voting, Are the Police Using Smart-Home IoT Devices to Spy on People?, On Disguise, China's Hacking of the Border Gateway Protocol, Android Ad-Fraud Scheme, Detecting Fake Videos, Security Vulnerability in Internet-Connected Construction Cranes, More on the Supermicro Spying Story, Cell Phone Security and Heads of State, ID Systems Throughout the 50 States, Was the Triton Malware Attack Russian in Origin?, Buying Used Voting Machines on eBay, How to Punish Cybercriminals, Troy Hunt on Passwords, Security of Solid-State-Drive Encryption, *Consumer Reports*Reviews Wireless Home-Security Cameras, iOS 12.1 Vulnerability, Privacy and Security of Data at Universities, The Pentagon Is Publishing Foreign Nation-State Malware, Hiding Secret Messages in Fingerprints, New IoT Security Regulations, Oracle and “Responsible Disclosure,” More Spectre/Meltdown-Like Attacks, Upcoming Speaking Engagements,

October 15, 2018: NSA Attacks Against Virtual Private Networks, Public Shaming of Companies for Bad Security, Pegasus Spyware Used in 45 Countries, Security Vulnerability in ESS ExpressVote Touchscreen Voting Computer, AES Resulted in a $250-Billion Economic Benefit, New Findings About Prime Number Distribution Almost Certainly Irrelevant to Cryptography, New Variants of Cold-Boot Attack, Evidence for the Security of PKCS #1 Digital Signatures, Counting People through a Wall with Wi-Fi, Yet Another IoT Cybersecurity Document, Major Tech Companies

Finally Endorse Federal Privacy Regulation, More on the Five Eyes Statement on Encryption and Backdoors, Facebook Is Using Your Two-Factor Authentication Phone Number to Target Advertising, Sophisticated Voice Phishing Scams, Terahertz Millimeter-Wave Scanners, The Effects of GDPR's 72-Hour Notification Rule, Helen Nissenbaum on Data Privacy and Consent, Chinese Supply Chain Hardware Attack, Conspiracy Theories around the "Presidential Alert," Detecting Credit Card Skimmers, Defeating the "Deal or No Deal" Arcade Game, The US National Cyber Strategy, Access Now Is Looking for a Chief Security Officer, Security Vulnerabilities in US Weapons Systems, Another Bloomberg Story about Supply-Chain Hardware Attacks from China, Security in a World of Physically Capable Computers, Upcoming Speaking Engagements,

September 15, 2018: New Book Announcement: *Click Here to Kill Everybody*, Speculation Attack Against Intel's SGX, New Ways to Track Internet Browsing, James Mickens on the Current State of Computer Security, "Two Stage" BMW Theft Attempt, Good Primer on Two-Factor Authentication Security, John Mueller and Mark Stewart on the Risks of Terrorism, Future Cyberwar, NotPetya, CIA Network Exposed through Insecure Communications System, Cheating in Bird Racing, Eavesdropping on Computer Screens through the Webcam Mic, Using a Smartphone's Microphone and Speakers to Eavesdrop on Passwords, Five-Eyes Intelligence Services Choose Surveillance Over Security, Reddit AMA, Using Hacked IoT Devices to Disrupt the Power Grid, Security Vulnerability in Smart Electric Outlets, Security Risks of Government Hacking, Quantum Computing and Cryptography, *Click Here to Kill Everybody* Reviews and Press Mentions, Upcoming Speaking Engagements,

August 15, 2018: New Book Announcement: Click Here to Kill Everybody, Reasonably Clever Extortion E-mail Based on Password Theft, Installing a Credit Card Skimmer on a POS Terminal, Defeating the iPhone Restricted Mode, Suing South Carolina Because Its Election Machines Are Insecure, New Report on Chinese Intelligence Cyber-Operations, 1Password's Travel Mode, Nicholas Weaver on Cryptocurrencies, On Financial Fraud, Major Bluetooth Vulnerability, DARPA Wants Research into Resilient Anonymous Communications, Google Employees Use a Physical Token as Their Second Authentication Factor, Third Annual Cybercrime Conference, New Report on Police Digital Forensics Techniques, Identifying People by Metadata, The Poor Cybersecurity of US Space Assets, Hacking a Robot Vacuum, Backdoors in Cisco Routers, GCHQ on Quantum Key Distribution, Using In-Game Purchases to Launder Money, How the US Military Can Better Keep Hackers, Three of My Books Are Available in DRM-Free E-Book Format, Hacking the McDonald's Monopoly Sweepstakes, Measuring the Rationality of Security Decisions, SpiderOak's Warrant Canary Died, Detecting Phishing Sites with Machine Learning, Don't Fear the TSA Cutting Airport Security. Be Glad That They're Talking about It., xkcd on Voting Computers, Identifying Programmers by their Coding Style, Google Tracks its Users Even if They Opt-Out of Tracking, My Speaking Engagements,

July 15, 2018: Important: Crypto-Gram Has Moved to MailChimp, Thomas Dullien on Complexity and Security, Ridiculously Insecure Smart Lock, Are Free Societies at a

Disadvantage in National Cybersecurity, Perverse Vulnerability from Interaction between 2-Factor Authentication and iOS AutoFill, Algeria Shut Down the Internet to Prevent Students from Cheating on Exams, Domain Name Stealing at Gunpoint, The Effects of Iran's Telegram Ban, Secure Speculative Execution, Bypassing Passcodes in iOS, IEEE Statement on Strong Encryption vs. Backdoors, Manipulative Social Media Practices, Conservation of Threat, Traffic Analysis of the LTE Mobile Standard, California Passes New Privacy Law, Beating Facial Recognition Software with Face Makeup, The NSA's Domestic Surveillance Centers, PROPagate Code Injection Seen in the Wild, Recovering Keyboard Inputs through Thermal Imaging, Department of Commerce Report on the Botnet Threat, WPA3, Gas Pump Hack, Schneier News

June 15, 2018: Important: Crypto-Gram Is Moving to MailChimp, Router Vulnerability and the VPNFilter Botnet, E-Mail Vulnerabilities and Disclosure, News, Russian Censorship of Telegram, Security and Human Behavior (SHB 2018), Schneier News, Another Spectre-Like CPU Vulnerability, An Example of Deterrence in Cyberspace, New Data Privacy Regulations

May 15, 2018: Securing Elections, Details on a New PGP Vulnerability, News, Two NSA Algorithms Rejected by the ISO, Ray Ozzie's Encryption Backdoor, Schneier News, Supply-Chain Security

April 15, 2018: Facebook and Cambridge Analytica, News, Israeli Security Company Attacks AMD by Publishing Zero-Day Exploits, Schneier News, Obscure E-Mail Vulnerability, The Digital Security Exchange Is Live

March 15, 2018: Artificial Intelligence and the Attack/Defense Balance, News, Writings on the Encryption Debate, Schneier News, Can Consumers' Online Data Be Protected?

February 15, 2018: The Effects of the Spectre and Meltdown Vulnerabilities, News, After Section 702 Reauthorization, Schneier News, Cabinet of Secret Documents from Australia

January 15, 2018: Spectre and Meltdown Attacks Against Microprocessors, News, Susan Landau's New Book: “Listening In,” Schneier News, New Book Coming in September: “Click Here to Kill Everybody,” Daniel Miessler on My Writings about IoT Security

Earlier issues of Crypto-Gram are available here:
https://www.schneier.com/crypto-gram/

Significant Articles about Schneier

“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.

"'Surveillance Shouldn't Be the Business Model of the Internet. We Can Change It,'" *The Times of India*, May 28, 2017.

"Cybersecurity Talk with Bruce Schneier: How to Start Your Career in Cybersecurity?," *CQURE Academy*, April 13, 2017.

"This Is Your Brain on Terrorism," *Vox*, March 20, 2017.

"Bruce Schneier on New Security Threats from the Internet of Things," *Linux.com*, March 17, 2017.

"3 Important Things to Know about Big Brother Watching Us," *The List*, March 15, 2017.

"Cybersecurity Expert on Latest Wikileaks: Nothing to See Here," *Metro*, March 7, 2017.

"Video Review of *Data and Goliath*," *YouTube*, March 6, 2017.

“Bruce Schneier on IoT Regulation,” *Threatpost*, March 6, 2017.

“Cyber Security Blogs You Need to See,” *Focus Training*, February 24, 2017.

“Bruce Schneier and the Call for ‘Public Service Technologists,’” *Network World*, February 23, 2017.

“Bruce Schneier Says Government Involvement in Coding Is Coming,” *Softpedia News*, February 15, 2017.

“Schneier Brings Campaign for IoT Regulation to RSA,” *Threatpost*, February 14, 2017.

“Bruce Schneier: The US Government Is Coming for YOUR Code, Techies,” *The Register*, February 14, 2017.

“IoT Security: ‘The Market has Failed,’” *T-Systems*, January 26, 2017.

“Reflecting on 2016: The Year in Cybersecurity,” *Radio Boston*, December 27, 2016.

“Cybersecurity Expert Bruce Schneier: American Elections Will Be Hacked,” *Democracy Now*, November 30, 2016.

“Security Experts Call For Regulation On IoT Cybersecurity,” *Dark Reading*, November 17, 2016.

“Not a Matter of ‘If’ on IoT Cybersecurity Rules, Experts Say,” *Morning Consult*, November 16, 2016.

“Can the American Election Be Hacked?,” *The Economist*, October 26, 2016.

“Hacking: What Journalists Need to Know. A Conversation with Bruce Schneier,” *Journalist's Resource*, October 24, 2016.

“Can You Hack an Election? Can You Stop Terrorism by Spying?,” *David Pakman Show*, October 15, 2016.

“Bruce Schneier—Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World,” *Neural*, September 21, 2016.

“«Quelqu’un Apprend à Détruire Internet», Selon Bruce Schneier,” *SciencePost*, September 15, 2016.

“Espionage Insiders: Welcome to the Post-Forgetting World,” *Salon*, September 13, 2016.

“After the DNC Hack, What’s Stopping Russian Hackers from Accessing Voting Machines?,” *Boston Public Radio*, August 4, 2016.

“Ask Me Anything,” *Reddit*, August 2, 2016.

"RSA Conference Asia Pacific & Japan 2016 Interview," *RSA Conference*, August 1, 2016.

"Schneier: Next President May Face IoT Cyberattack That Causes People to Die," *Computerworld*, July 25, 2016.

"Securing the World-Sized Web," *InfoRisk Today*, July 22, 2016.

"Adam Ruins Everything: Security and Big Data with Bruce Schneier," *Adam Ruins Everything*, July 5, 2016.

"Going Dark or Getting Personal? The Battle Between Data, Privacy & Intrusion," *The Legal Edition*, June 25, 2016.

"Bruce Schneier at Infosecurity Europe 2016," *Tripwire*, June 20, 2016.

"IoT Security: Lack of Expertise Will Hurt, Says Bruce Schneier," *Computer Weekly*, June 10, 2016.

"Government Regulation Will Clip Coders' Wings, Says Bruce Schneier," *The Register*, June 10, 2016.

"#Infosec16: Securing the IoT is the Next Big Challenge, Says Bruce Schneier," *Infosecurity*, June 9, 2016.

"InfoSec 2016: Two Worlds Are Colliding, and I Don't Have the Answer, Says Bruce Schneier," *TechWeek Europe*, June 9, 2016.

"Bruce Schneier: Governments Have a 'Stark' Lack of Expertise in IoT Security," *V3*, June 9, 2016.

"Internet of Things Security: Ask Bruce, Episode Nine," *ResilienTV*, May 9, 2016.

"Bruce Schneier: Building Cryptographic Systems," *Computer*, April 2016.

"Bruce Schneier on the FBI/Apple Outcome," *TWiT Netcast Network*, April 5, 2016.

"Bruce Schneier on the Integration of Privacy and Security," *Threatpost*, March 23, 2016.

"Rise of the Machines: The Threat Posed by Growing Connectivity," *Irish Times*, March 17, 2016.

"Reacting Fast is Not Enough (RSA 2016)," *CloudPassage*, March 17, 2016.

"RSA 2016 Interview with Bruce Schneier," *ITProTV*, March 15, 2016.

"Overcoming the Cyber Security Skills Gap: Ask Bruce, Episode Eight," *ResilienTV*, March 11, 2016.

"Q&A: Bruce Schneier on Joining IBM, IoT Woes, and Apple v. the FBI," *The Register*, March 4, 2016.

"Bruce Schneier: We're Sleepwalking towards Digital Disaster and Are Too Dumb to Stop," *The Register*, March 2, 2016.

"Bruce Schneier on IBM Grabbing Him Up with Resilient Systems," *SearchSecurity*, March 2, 2016.

"Building a Security Culture: Ask Bruce, Episode Seven," *ResilienTV*, February 25, 2016.

"How to Prevent the Normalization of Deviance: Ask Bruce, Episode Six," *ResilienTV*, February 18, 2016.

"Study Finds That Anti-Crypto Laws Won't Work on an International Stage," *CSO*, February 12, 2016.

"Most Encryption Products Far beyond Reach of US Law Enforcement," *Christian Science Monitor*, February 11, 2016.

"Backdoor Laws Can't Contain Global Encryption, Says New Report," *The Verge*, February 11, 2016.

"Strong Crypto Is Widely Available Outside The US, So Restrictions Are Unlikely To Thwart Terrorism," *Forbes*, February 11, 2016.

"Global Crypto Survey Proves Govt Backdoors Completely Pointless," *Iain Thomson*, February 11, 2016.

"New Survey Suggests US Encryption Ban Would Just Send Market Overseas," *The Intercept*, February 11, 2016.

"New Report Contends Mandatory Crypto Backdoors Would Be Futile," *Ars Technica* , February 11, 2016.

"Press Release: International Encryption Product Survey Finds 546 Non-US Products from 54 Countries," Press Release, February 11, 2016.

"Talk on Strategies for Combating Cyber-Terrorism," *Boston Global Forum*, February 11, 2016.

"Incident Response Orchestration: Ask Bruce, Episode Five," *ResilienTV* , February 3, 2016.

"On the Wire Podcast: Bruce Schneier," *On the Wire*, February 1, 2016.

"The Security Reading Room: The Best Information Security Books of 2015," *RSA Conference Blog*, December 23, 2015.

"Bruce Schneier on the Golden Age of Surveillance," *The Technoskeptic*, December 22, 2015.

"Cyberattack Prediction: Hackers Will Target a US Election Next Year," *CSO*, December 18, 2015.

"Bruce Schneier Receives the Business Leader in Cybersecurity Award from Boston Global Forum," *Boston Global Forum*, December 13, 2015.

"Holiday Gift Guide: Good Reads Worth the Investment," *Vancouver Sun*, December 4, 2015.

"Datenschutz in Rücklage," *Neue Zürcher Zeitung*, December 12, 2015.

"Making Your Mark as a CISO: Ask Bruce, Episode Four," *ResilienTV*, November 20, 2015.

"Rolling Back Mass Surveillance," *Engineering Ethics Blog*, November 16, 2015.

"Today's Trends in Cyber Resilience: Ask Bruce, Episode Three," *ResilienTV*, November 2, 2015.

"A Conversation with Bruce Schneier," *CyberSeed 2015*, October 29, 2015.

"Panel Discussion on Terrorism and Surveillance," *C-SPAN*, October 24, 2015.

"The Second Annual Cato Surveillance Conference," *Cato Institute*, October 21, 2015.

"Incident Response and the Rise of Organizational Doxing: Ask Bruce, Episode Two," *ResilienTV*, October 13, 2015.

"Automation in Incident Response: Ask Bruce, Episode One," *ResilienTV*, October 8, 2015.

"Data Privacy, One of These Days," *BetaBoston*, October 7, 2015.

"Video: Why The TSA Doesn't Stop Terrorist Attacks," *Adam Ruins Everything*, October 5, 2015.

"Video: Panel at Free and Safe in Cyberspace 2015," *Free and Safe in Cyberspace*, September 24, 2015.

"Video: Trust, Society, and Technology," *Free and Safe in Cyberspace*, September 24, 2015.

"Audio: How Big Brother Snuck Up On Us," *The Social Network Station*, September 7, 2015.

"Data and Goliath by Bruce Schneier (Book Review)," *Living with the Future*, September 5, 2015.

"Audio: Security and Privacy with Bruce Schneier," *Software Engineering Daily*, September 3, 2015.

"Internet das Coisas Poderá Criar Caos Em Segurança Digital, Diz Especialista," *Folha de S.Paulo*, August 25, 2015.

"'A Lot of Attacks from Western Countries Go through China,' Says Bruce Schneier," *Computing*, August 20, 2015.

"Bruce Schneier: The Cyberwar Arms Race Is On," *ZDNet*, August 20, 2015.

"Bruce Schneier: 'We're in Early Years of a Cyber Arms Race,'" *The Register*, August 19, 2015.

"Video: Private Thoughts – Bruce Schneier on the Ephemeral, Privacy, and Data," *Restore the Fourth*, August 18, 2015.

"The New America: Little Privacy, Big Terror," *The New York Review*, August 13, 2015.

"Bruce Schneier on Security Metrics that Matter," *Tenable Blog*, August 10, 2015.

"Video: Bruce Schneier on Jeep Hack and Encryption," *Boom Bust*, August 7, 2015.

"Video: How Vulnerable are Airlines to Hackers?," *Bloomberg Business*, August 7, 2015.

"Bruce Schneier: 'Hacking Team is a Dangerous Company,'" *L'Espresso*, July 29, 2015.

"Bruce Schneier: It's Time to Start Prioritizing IT Security," *Work Intelligent.ly*, July 24, 2015.

"Bruce Schneier: Get Ready for More 'Organizational Doxing,'" *Cyber Risk Network*, July 21, 2015.

"Infosec Influencers: An Interview with Bruce Schneier," *Tripwire*, July 16, 2015.

"Is iPhone Banking Safe? An Expert Answers," *Money Nation*, July 15, 2015.

"Bruce Schneier: IT Teams Need Cyberattack Response Planning More Than Prevention," *Linux.com*, July 14, 2015.

"Bruce Schneier: David Cameron's Proposed Encryption Ban Would 'Destroy the Internet,'" *Business Insider*, July 6, 2015.

"I Read *Data and Goliath* Because of Barbara Fister," *Inside Higher Ed*, July 6, 2015.

"Video: Army Cyber Institute," *Army Cyber Institute*, June 29, 2015.

"This Security Expert Reckons Mass Surveillance Doesn't Stop Terror Attacks," *Vice*, June 26, 2015.

"Video: Keynote: Data and Goliath," *Norwegian Developers Conference*, June 18, 2015.

"Terrifying Action Movie Plots About...Encryption," *Slate,* June 16, 2015.

"20 Top Security Influencers," *eSecurity Planet,* June 11, 2015.

"Audio: Cybersecurity: Are We Ever Safe From Hackers?," *BBC,* June 8, 2015.

"Review: Data and Goliath by Bruce Schneier," *Strife,* June 5, 2015.

"Surveillance, Bulk Data Collection and Intelligence: an Interview with Bruce Schneier," *Strife,* June 5, 2015.

"We Stand on the Brink of Global Cyber War, Warns Encryption Guru," *The Register,* June 4, 2015.

"We Are in Early Years of International Cyber War Arms Race, Says Security Expert Bruce Schneier," *ComputerWeekly,* June 4, 2015.

"Video: Expert: TSA Airport Security Is 'A Lot of Theater,'" *CNN,* June 2, 2015.

"Bruce Schneier on Privacy and the Data Free-for-All," *Wired,* May 26, 2015.

"Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World, by Bruce Schneier," *Times Higher Education,* May 21, 2015.

"Audio: Spy-wear?" *BBC Tech Tent,* May 15, 2015.

"Audio: Stuxnet, Sexism, CEOs and Surveillance," *Cybersecurity Initiative,* May 14, 2015.

"Book Review: Data and Goliath, by Bruce Schneier," *Virus Bulletin,* May 11, 2015.

"Video: Security in an Age of Catastrophic Risk," *RSA Conference 2015,* May 8, 2015.

"Book Review: Data and Goliath—You Don't Have Any Secrets Anymore," *Publishers Newswire,* May 8, 2015.

"Audio: Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World," *Financial Sense Newshour,* May 8, 2015.

"Audio: Schneier v. Baker Puts Mayweather v. Pacquiao in the Shade," *Steptoe Cyberlaw Podcast,* May 5, 2015.

"Review: 'Data and Goliath' Delves into Brave New World of Big Data, Hacking and Cyber Crime," *The Post and Courier,* May 3, 2015.

"Bruce Schneier's Data and Goliath—Solution or Part of the Problem?," *The Register,* May 3, 2015.

"Against an Adequately Skilled, Adequately Funded Adversary, Our Defenses Don't Work," *The Irish Times,* April 30, 2015.

“Identifying Perpetrators of Cyberattacks ‘Getting Tougher,’” *TradeArabia*, April 29, 2015.

“Insights from Security Leader at GISEC Event in Dubai,” *InfoRisk Today*, April 29, 2015.

“Video: Schneier: Incident Response Management Key to Surviving a Data Breach,” *SearchSecurity*, April 27, 2015.

“Book review: Data and Goliath (Bruce Schneier),” *Firewalls Don’t Stop Dragons*, April 25, 2015.

“Video: Cloud Computing Trade-Offs,” *Tenable Blog*, April 24, 2015.

“RSAC—Schneier Details Ways to Survive Catastrophic Attack,” *IT Security Guru*, April 24, 2015.

“What Bruce Schneier Learned from the Sony Breach,” *eSecurity Planet*, April 22, 2015.

“Audio: What Does It Take To Feel Secure?,” *TED Radio Hour (NPR)*, April 17, 2015.

“What Do You Use to Get Stuff Done?,” *The Setup*, April 14, 2015.

“Audio: The Hidden Struggles to Control Your Data,” *Late Night Live (Australian Broadcasting Corporation)*, April 14, 2015.

“Schneier on “Really Bad” IoT Security: ‘It’s Going to Come Crashing Down,’” *Network World*, April 13, 2015.

“Video: Schneier: Turn Data Over to Those With Greatest Data Security Knowledge,” *Boom Bust*, April 8, 2015.

“Review of Data and Goliath,” *Computing Reviews*, April 8, 2015.

“Ced Kurtz’s Techman Texts: Computer Surveillance Is a Trade-off,” *Pittsburgh Post-Gazette*, April 7, 2015.

“Video: Book Talk at NYU,” *New York University*, April 6, 2015.

“The Ends of Privacy,” *The New Rambler*, April 6, 2015.

“Collecting Private Information,” *The Economist*, April 4, 2015.

“Review: Choking on Digital Exhaust,” *Reuters Breakingviews*, April 2, 2015.

“Fixing the Surveillance-Industrial Complex,” *Inside Higher Ed*, April 1, 2015.

“Data and Goliath, Book Review: A Handbook for the Information Age,” *ZDNet UK Book Reviews*, March 31, 2015.

“David and Goliath: What Do We Do about Surveillance?,” *New Scientist,* March 30, 2015.

“Bruce Schneier Talks Privacy, Politics, Books and More,” *The Fortinet Blog,* March 30, 2015.

“Video: Panel Discussion of Data and Goliath at Harvard’s Berkman Center,” *Berkman Center, Harvard University,* March 30, 2015.

“The Essential Guide To Digital Life: Bruce Schneier’s Data And Goliath,” *The Cryptosphere,* March 30, 2015.

“Audio: Bruce Schneier, Data and Goliath,” *Paul Harris Online,* March 27, 2015.

“Wanted: Slingshots,” *Dissent NewsWire,* March 24, 2015.

“‘We the People Have a Lot of Work to Do’ Says Schneier in a Must-Read Book on Security and Privacy,” *Forbes,* March 24, 2015.

“Review of Data and Goliath,” *The Boston Globe,* March 24, 2015.

“All the Secret Ways You’re Being Tracked That You Don’t Even Realize,” *Mic,* March 23, 2015.

“Audio: Metadata Retention and Privacy,” *2ser Radio,* March 23, 2014.

“Expert Bruce Schneier: It’s Hard Not to Despair over the State of IT Security,” *IT World Canada,* March 23, 2015.

“Cyberattack Is Easier than Cyberdefence—Bruce Schneier,” *Arabian Gazette,* March 22, 2015.

“Video: Data and Goliath,” *Sunrise on 7 (Australia),* March 21, 2015.

“Two Books Look at How Modern Technology Ruins Privacy,” *Washington Post,* March 20, 2015.

“Audio: How Secure Is Your Data?,” *MPR News,* March 20, 2015.

“Verschlüsselungs-Experte Bruce Schneier ‘Dein Handy weiß alles über dich,’” *Süddeutsche.de,* March 15, 2015.

“Audio: ALP Supports Amended Version of Govt’s ISP Data Bill,” *PM (Australian Broadcasting Corporation),* March 17, 2015.

“Security Guru Bruce Schneier: Your Privacy is Already Gone,” *InfoWorld,* March 17, 2015.

“The Hard Questions,” *The Wall Street Journal,* March 16, 2015.

"Audio: Personal Data Collection and Your Technology Footprint," *Radio New Zealand*, March 16, 2015.

"Book Review of Data and Goliath by Bruce Schneier," *The New York Times—DealBook*, March 16, 2015.

"Video: Part 2: Bruce Schneier on the Hidden Battles to Collect Your Data and Control Your World," *Democracy Now!*, March 13, 2015.

"Video: Data and Goliath: Bruce Schneier on the Hidden Battles to Collect Your Data and Control Your World," *Democracy Now!*, March 13, 2015.

"Computer Security Expert Bruce Schneier Is Here to Answer Questions," *Gizmodo*, March 13, 2015.

"Data and Goliath: Confronting the Surveillance Society," *Federation of American Scientists*, March 11, 2015.

"Video: Toppling Our Surveillance-Based Society," *TalkingStickTV*, March 9, 2015.

"Video: Interview: Online Security Expert Bruce Schneier," *Lateline (Australian Broadcasting Corporation)*, March 10, 2015.

"Video: Data and Goliath," *Talks at Google*, March 10, 2015.

"Video: Bruce Schneier: Why We Should Reform Surveillance Policies," *WGBHForum*, March 9, 2015.

"*Data and Goliath*: The Hidden Battles to Collect Your Data and Control Your World," *Slashdot*, March 9, 2015.

"Bruce Schneier on the Sony Hack," *International Cyber Security Strategy Congress*, March 8, 2015.

"A Way Forward: Bruce Schneier's *Data and Goliath* Explains Where Our Privacy is Now, and How We Fix It," *EFF Deeplinks Blog*, March 6, 2015.

"Balancing Surveillance: Privacy and Security in the Digital Age," *Science Friday*, March 6, 2015.

"Trying to Make Sense of the World of Ubiquitous Surveillance," *LA Times*, March 5, 2015.

"Bruce Schneier Presents *Data and Goliath*," *Internet Society*, March 5, 2015.

"Bruce Schneier's Important New Book," *Lawfare*, March 4, 2015.

"There is Actually One Thing You Can Do to Fight the Surveillance Machine," *New Tech City*, March 4, 2015.

"Book Debut: *Data and Goliath*," *Freedom to Connect*, March 3, 2015.

"Bruce Schneier's *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (Book Review)," *Boing Boing*, March 2, 2015.

"*Data and Goliath*: A Portrait of Big Data Abuses," *Datanami*, March 2, 2015.

"Book Review," *ISSA Journal*, March 2015.

"*Data and Goliath* (Book Review)," *Booklist*, March 1, 2015.

"How to Sabotage Encryption Software (And Not Get Caught)," *Wired*, February 27, 2015.

"Big Data: The Revolution Is Digitized," *Nature*, February 26, 2015.

"'Where's the Data Going?'," *CTV News*, February 9, 2015.

"Kirkus Review of *Data and Goliath*," *Kirkus Reviews*, January 22, 2015.

"Top Influencers in Security You Should Be Following in 2015," *Tripwire*, January 8, 2015.

"Passwords," *Science for the People*, January 2, 2015.

"Once More Undo the Breach," *CFA Institute Magazine*, January/February 2015.

Earlier news articles are available here: https://www.schneier.com/news/

Previous Declarations and Depositions

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.

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.