Bibliography

Legislation and Treaties

California Business and Professions Code (United States).
Canada Act 1982 (UK) 1982, c 11.
Canadian Charter of Human Rights and Freedoms.
Canadian Criminal Code, R.S.C. 1985, c.46.
Computer Fraud and Abuse Act 1986 (United States).
Computer Misuse Act 1990 (United Kingdom).
Computer Misuse and Cybersecurity Act Ch 50A (Rev Ed 2007) (Singapore).
Convention to the International Covenant on Civil and Political Rights, 999 UNTS 302 (1967).
Council of Europe Convention on Cybercrime, 22296 UNTS 167 (2001).
Criminal Code Act 1995 (Australia).
Espionage Act (1917) (United States).
German Criminal Code (1914).
Information and Electronic Transaction Law (2008) (Indonesia).
Model Criminal Code (January 2001) (Australia).
Penal Law (1977) (Israel).
Stored Communications Act (1986) (United States).
Uniform Code of Military (United States).
Youth Criminal Justice Act S.C. 2002, c. 1 (Canada).

Case Law

1-800 Contacts v. WhenU.com (2005) 414 F.3d 400.

1-800 Solutions v. Zone Labs.

Alberta (Education) v Canadian Copyright Licensing Agency (Access Copyright) [2012] 2 SCR 345.

Anat Kamm v State of Israel [2012] Case 17959-01-10 (Israel Supreme Court).

Auernheimer v. United States of America, No. 13-1816 (United States, Third US Circuit Court of Appeals).

Ashdown v Telegraph Group Ltd [2001] EWCA Civ 1142.

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd (2001) 185 ALR 1.

Bank Julius Baer & Co. Ltd. v. WikiLeaks (2008) No. C 08-00824 JSW (February 29, 2008) (US District Court for the Northern District of California); see https://www.eff.org/files/filenode/baer_v_wikileaks/wikileaks102.pdf.

Cadbury Schweppes v FBI Foods [1999] 1 SCR 142.

Campbell v Acuff-Rose Music (1994) 510 U.S. 569.

Cassava (CasinoOnNet) v. Sunbelt Software.

CCH Canadian Ltd. v Law Society of Upper Canada [2004] 1 SCR.

Claria (Gator) v Internet Advertising Bureau.

Collier Constructions Pty Ltd v Foskett Pty Ltd (1991) 20 IPR 666.

Commonwealth v John Fairfax (1980) 147 CLR 39.

Corrs Pavey v Collector of Customs [1987] FCA 26.

Dagenais v. Canadian Broadcasting Corp. [1994] 3 S.C.R. 835.

E360 Insight and David Linhardt v. The Spamhaus Project (2007) 500 F. 3d 594 (United States Court of Appeals for the Seventh Circuit).

E360 Insight, LLC et al v. The Spamhaus Project (2006) Case No. 06 C 3958 (United States District Court, Northern District of Illinois, September 13, 2006). Access to default judgment at http://www.spamhaus.org/archive/legal/Kocoras_order_to_Spamhaus.pdf.

Edmonton Journal v. Alberta (A.G.) [1989] 2 S.C.R. (Canada).

Hyde Park Residence v Yelland, [2001] Ch. 143.

IceTV Limited v Nine Network Australia Pty Limited [2009] HCA 14.

IceTV Limited v Nine Network Australia Pty Limited [2008] HCATrans 358.

Imutran Ltd v Uncages Campaigns Ltd, [2001] CP Rep. 28.

In re § 2703(d) Order (2013) No. 11-5151 (US Court of Appeals Fourth Circuit) (January 25 2013).

See also Justia US Law, *In re 2703(d) Application, No. 11-5151* (Fourth Cir. 2013), available at https://law.justia.com/cases/federal/appellate-courts/ca4/11-5151/11-5151-2013-01-25.html.

Legal documents also available at, Electronic Privacy Information Center, *In re Twitter Order Pursuant to 2703(d)*, available at https://www.epic.org/amicus/twitter/wikileaks/.

In re § 2703(d) Order (2011) 830 F. Supp. 2d 114 (US District Court, Eastern District of Virginia, Alexandria Division) (November 10, 2011).

Irwin Toy v. Quebec [1989] 1 S.C.R. 927 (Canada).
James Raj Arokiasamy v Public Prosecutor [2014] 2 SLR 307 ("James Raj") (Singapore, States Courts).
Lauri Love v. the Government of the United States of America [2018] EWHC 172, see https://freelauri.com/wp-content/uploads/2018/02/lauri-love-v-usa.pdf.
Libertad.de (2006) File reference 1 Ss 319/05, March 22, 2006 (Germany, Higher Regional Court, Frankfurt am Main).
Lion Laboratories v Evans, [1985] QB 526.
McAuliffe v The Queen [1995] 183 CLR 108.
McCabe v British American Tobacco Services Limited [2002] VSC 73.
Microsoft Corporation v. John Does 1027 (Feb. 22, 2010) United States District Court for the State of Victoria, Civil Action 1:10 cv 156 (LMB/JFA).
Microsoft Corporation v. Newport Internet Marketing Corporation Does 2-20 (2005) No. 03-2-12648-9 SEA (United States, King County Superior Court Seattle, Washington).
Lavigne v. Ontario Public Service Employees Union [1991] 2 S.C.R. 211.
Little Sisters Book and Art Emporium v. Canada (Minister of Justice) [2000] 2 S.C.R. 1120.
Paracha v. Obama (2011) No. 04-2022 (PLF) (April 29, 2011) (US District Court for the District of Columbia).
Case:
https://scholar.google.com.au/scholar_case?case=7165402973414950017&q=Paracha+wikileaks&hl=en&as_sdt=2006&as_vis=1#r[1].
Petitioner's (Paracha's) emergency application: https://fas.org/sgp/jud/par/042711-access.pdf.
Respondents' (Obama et al.'s) response: https://fas.org/sgp/jud/par/061511-response376.pdf.
Regan Gerard Gilmour v Director of Public Prosecutions (Commonwealth) [1996] NSWSC 55.
R v. Caffrey (2006).
R v Christopher Weatherhead, Ashley Rhodes, Peter Gibson, and Jake Birchall (January 24, 2013) (United Kingdom, Southwark Crown Court in London).
R v Cleary, Davis, Al-Bassam and Ackroyd (May 16 and 24, 2013) (United Kingdom Southwark Crown Court in London).
R v Glen Steven Mangham (February 17, 2012) (United Kingdom, Southwark Crown Court in London).
R v Glen Steven Mangham Court of Appeal [2012] EWCA Crim 973 (April 4, 2012) (England and Wales Court of Appeal (Criminal Division)), see http://www.bailii.org/ew/cases/EWCA/Crim/2012/973.html.
R v. Keegstra [1990] 3 S.C.R. 697.
R v National Post [2010] 1 SCR 477.
R v. Sharpe [2001] 1 S.C.R. 45.

R v Stevens [1999] NSWCCA 69.
R v Walker [2008] NZHC 1114.
R v. Zundel [1992] 2 S.C.R. 731.
Rocket v. Royal College of Dental Surgeons of Ontario [1990] 2 S.C.R. 232 (Canada).
R.W.D.S.U. v. Dolphin Delivery Ltd. [1986] 2. S.C.R. 573.
Salter v DPP [2008] NSWSC 1325.
Sierra Corporate Design Inc. v. David Ritz (2007) File No. op-05-C-01660 (United States, District Court, County of Cass, State of North Dakota). See www.spamsuite.com.com/node/351.
Society of Composers, Authors and Music Publishers of Canada v Bell Canada [2012] 2 SCR 326.
Sony Computer Entertainment, Inc. v. Connectix Corporation (2000) 203 F. 3d 596, Ninth Circuit.
Soyke v R [2016] NSWCCA 112 (June 10, 2016).
Specht v. Netscape Communications Corp. (2002) 306 F. 3d 17, Court of Appeals, Second Circuit.
State of Israel v. Anat Kamm (2010) Case 17959-01-10 (Israel, District Court of Tel Aviv Jaffa). See http://www.maannews.net/eng/ViewDetails.aspx?ID=275114.
Théberge v. Galerie d'Art du Petit Champlain [2002] 2 S.C.R. 336.
U.F.C.W., Local 1518 v. Kmart Canada Ltd. [1999] 2 S.C.R. 1083.
United States of America v. Aaron Swartz, 1:11-cr-10260 (US District Court for the District of Massachusetts).
United States of America v. Bradley Manning E., PFC (2013) (United States, Army Military District of Washington).
United States of America v. Daniel Spitler and Andrew Alan Escher Auernheimer, Mag. No. 11-4022 (CCC) (United States, District of New Jersey). Criminal Complaint, available at http://www.justice.gov/usao/nj/Press/files/pdffiles/2011/Spitler,%20Daniel%20et%20al.%20Complaint.pdf.
United States of America v. Dennis Collins, et al (2011), No. CR 11-00471 DLJ (United States District Court, Northern District of California, San Jose Division). For indictment, see http://ia600502.us.archive.org/24/items/gov.uscourts.cand.242989/gov.uscourts.cand.242989.1.0.pdf.
United States of America v. Ford, 765 F.2d 1088, 1090 (11th Cir.1985).
United States of America v. Gorshkov (2001) WL 1024026 (United States, Western District Washington).
United States of America v. Jarrett (2003) 338 F. 3d 339, No. 02-4953 (July 29, 2003) (United States, Court of Appeals, Fourth Circuit). See http://scholar.google.com.au/scholar_case?case=7704360326371177621.
United States of America v. Jeremy Hammond (2013) 12 Cr. 185 (LAP) (United States District Court of Southern District of New York).

Case, available at http://www.justice.gov/usao/nys/pressreleases/May13/HammondJeremyPleaPR/U.S.%20v.%20Jeremy%20Hammond%20S2%20Information.pdf.

Free Jeremy (website), legal documents: https://freejeremy.net/category/legal/ including Sentencing Letter by Jeremy Hammond.

United States of America v Kevin George Poe (2011) CR 11 01166 (United States, District Court for the Central District of California).

United States of America v. Kretsinger (2:11-cr-00848) (US Central District of California (Los Angeles)).

United States of America v. Lauri Love (US District Court for the District of New Jersey), see https://www.scribd.com/doc/179595899/Love-Lauri-Indictment.

United States of America v. Raynaldo Rivera, CR No. 12-798-JAK (US District Court for the Central District of California).

Plea agreement: https://freeanons.org/wp-content/uploads/court-documents/Raynaldo-Rivera.pdf.

United States of America v. Steiger (2003) 318 F. 3d 1039, Nos. 01-15788, 01-16100 and 01-16269 (January 14, 2003) (United States, Court of Appeals 11th Circuit). See http://scholar.google.com.au/scholar_case?case=5611821785646747519.

Zitierung: BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1–333), see http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

Books

Aitchison, R. "DNS Records." In *Pro DNS and BIND*, Apress Publishers, 2003.

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Indianapolis: Wiley Publishing, 2008.

Athanasopoulos, E., Anagnostakis, K., and Markatos, E. "Misusing Unstructured P2P Systems to Perform DoS attacks: The Network that Never Forgets" Lecture Notes in Computer Science for *Applied Cryptography and Network Security*. Springer Berlin, 2006. Available at http://www.springerlink.com/content/xk82663475474857/.

Atkin, T. et al. *Information Security Management Handbook*. CRC Press, 2006.

Barlow, J. P. "Crime and Puzzlement," Appendix 1 in Ludlow, P. (ed.), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. MIT Press, 1996.

Barton, P., and Yegneswaran, V. "An Inside Look at Botnets." In Somesh, J., Maughan, D., Song, D., and Wang, C. (eds.), *Malware Detection*. New York: Springer, 2007.

Bentham, J. *Panopticon*, in Miran Bozovic (ed.), *The Panopticon Writings*. London: Verso, 1995), 29-95.

Blount, S. *Electronic Contracts: Principles for the Common Law*. Australia: Reed International Books, 2009.

Bowrey, K. *Law & Internet Cultures*. Cambridge University Press, 2005.
Brenner, S. W. *Law in an Era of "Smart" Technology.* Oxford University Press, 2007.
Brown, A. J. *Whistleblowing in the Australian Public Sector: Enhancing the theory and practice of internal witness management in public sector organisations.* ANU Press, Canberra. Available at http://epress.anu.edu.au/anzsog/whistleblowing/mobile_devices/index.html, accessed February 10, 2014.
Chan, J., Goggin, G., and Bruce, J. "Internet Technologies and Criminal Justice." In Jewkes, Y., and Yar, M., *Handbook of Internet Crime.* Willan Publishing, 2010.
Chiesa, R., Ducci, S., and Ciappi, S. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. UNICRI and CRC Press, 2009.
Clayton, R. "Failures in a Hybrid Content Blocking System." In Danezis, G., and Martin, D. (eds.), *Privacy Enhancing Technologies*. PET 2005. Lecture Notes in Computer Science, vol 3856. Springer, Berlin, Heidelberg, pp. 78–92. https://doi.org/10.1007/11767831_6.
Cohen, F. *A Short Course on Computer Viruses*, 2nd ed. Wiley, 1994.
Corones, S., and Clarke, P. *Consumer Protection and Product Liability Law*, 3rd ed. Thomson Lawbook, 2008.
Curcereau, D. *Aspects of Regulating Freedom of Expression on the Internet.* Intersentia, 2006.
Dreyfus, S., and Assange, J. *Underground*. Random House Australia, 2011.
Dunham, K., and Melnick, J. *Malicious Bots: An Inside Look into the Cyber-Criminal Underground of the Internet.* CRC Press, 2009.
Fitzgerald, B., Fitzgerald, A., Middleton, G., Lim, Y., and Beale, T. *Internet and E-Commerce Law: Technology, Law and Policy.* Thomson 2007.
Fleming, J. *The Law of Torts*, 8th ed. The Law Book Company, 1992.
Garfinkel, S., and Spafford, G. *Practical UNIX & Internet Security*, 2nd ed. California: O'Reilly, 1996.
Geist, M. (ed.). *The Copyright Pentalogy: How the Supreme Court of Canada Shook the Foundations of Canadian Copyright Law.* Ottawa: Ottawa University Press, 2013.
Godwin, M. "Some 'Property' Problems in a Computer Crime Prosecution." In Ludlow, P. (ed.), *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*. MIT Press, 1996.
Grabosky, P. *Electronic Crime*. Prentice Hall, 2007.
Harris, S., Harper, A., Eagle, C., and Ness, J. *Grey Hat Hacking: The Ethical Hacker's Handbook.* McGraw Hill, 2008.
Himanen, P. *The Hacker Ethic: and the Spirit of the Information Age.* Random House, 2001.
Kerr, I., and Gilbert, D. "The Role of ISPs in the Investigation of Cybercrime." In MENDINA, T., and BRITZ, J. (eds.), *Information Ethics in an Electronic Age: Current Issues in Africa and the World*. McFarland Press, 2004.
Levy, S. *Hackers: Heroes of the Computer Revolution.* New York: Doubleday, 1984.

Levy, A. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age.* Viking, 2001.

Libicki, M. *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge, 2007.

Li, Z., Liao, Q., and Striegel, A. *Botnet Economics: Uncertainty Matters.* Springer, 2009.

Ludwig, M. *The Giant Black Book of Computer Viruses*, 2nd ed. American Eagle, 1998.

Lynch, A., and Williams, G. *What Price Security?* UNSW Press, 2006.

Malcom, J. *Multi-Stakeholder Governance and the Internet Governance Forum.* Termium Press, 2008.

Matswshyn, A. (ed.). *Harboring Data: Information Security, Law, and the Corporation.* Stanford University Press, 2009.

Maurushat, A. "Australia." In *Freedom on the Internet: A Global Assessment of Internet and Digital Media*, Cook S. (ed.). New York: Freedom House, 2011.

——. *Disclosure of Security Vulnerabilities.* Springer, 2013.

Moon, R. *The Constitutional Protection of Freedom of Expression.* University of Toronto Press, 2000.

Mueller, M. *Ruling the Root: Internet Governance and the Taming of Cyberspace.* Massachusetts Institute of Technology, 2002.

Oram, A. (ed.). *Peer-to-Peer: Harnessing the Power of Disruptive Technologies.* O'Reilly Media: Sebastopol, 2001.

Oxford Pocket Dictionary of Current English, 4th ed. Oxford University Press, 2009.

Pfleeger, C., and Pfleeger, S. *Security in Computing*, 4th ed. Prentice Hall, 2006.

Phair, N. *Cybercrime: The Reality of the Threat.* Privately published, 2007.

Poulsen, K. *Kingpin: The True Story of Max Butler, the Master Hacker Who Ran a Billion Dollar Cyber Crime Network.* Hachette, 2011.

Provos, N., and Holz, T. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection.* Safari, 2008.

Raymond, E. *The Cathedral & the Bizaar: Musings on Linux and Open Source By an Accidental Revolutionary.* O'Reilly Media, 2001.

Reyes, A., O'Shea, K., Steele, J., Hansen, J., Jean, B., and Ralph, T. *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Syngress, 2007.

Rice, D. *Geekonomics: The Real Cost of Insecure Software.* Addison-Wesley, 2008.

Ross, S. *UNIX System Security Tools.* McGraw-Hill, 1999.

Saltzer, J., Reed, D., and Clark, D. "End-to-End Arguments in System Design." In Partridge, C. (ed.), *Innovations in Internetworking.* Artech House, 1988.

Samuel, A. "Hacktivism and the Future of Political Participation." PhD thesis, Harvard, 2004.

Schiller, C., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C., and Cross, M., *Botnets: The Killer Web App.* Syngress, 2007.

Schneier, B. *Secrets and Lies.* Robert Ipsen, 2000.

Singh, S. The *Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptopgraphy.* Doubleday, 1999.

Smith, R., Grabosky, P., and Urbas, G. *Cyber Criminals on Trial.* Cambridge University Press, 2004.

Taylor, P. "Hacktivism: In Search of Lost Ethics?" In *Crime and the Internet.* London & New York: Routledge.

Taylor, R., Caeti, T., Loper, K., Fritsch, E., and J. R. Liederbach. *Digital Crime and Digital Terrorism.* Pearson, United Kingdom, 2005.

Thoreau, H. D. *Resistance to Civil Government* (original title, 1849; also known as *Civil Disobedience: On the Duty of Civil Disobedience).* In N. Rosenblum (Ed.), Thoreau: Political Writings(Cambridge Texts in the History of Political Thought, pp. 1-22). Cambridge: Cambridge University Press.

Tien, L. "Architectural Regulation and the Evolution of Social Norms." In Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., and Zarsky, T. (eds.), *Cybercrime: Digital Cops and Laws in a Networked Environment.* New York University Press, 2006.

Walden, I. "Computer Forensics and the Presentation of Evidence in Criminal Cases." In JEWKES, Y., and YAR, M., *Handbook of Internet Crime.* Willan Publishing, 2010.

Wall, D. *Cybercrime: Crime and Society Series.* Polity Press, 2007.

Yar, M. "The Private Policing of Internet Crime." In Jewkes, Y., and Yar, M. (eds.). *Handbook of Internet Crime.* Willan Publishing, 2010.

——. "Public Perception and Public Opinion about Internet Crime." In Jewkes, Y., and Yar, M., *Handbook of Internet Crime.* Willan Publishing, 2010), 104-120.

Yegneswaran, V., and Barford, P. "An Inside Look at Botnets." In Christodorescu, M., Jha, S., Maughan, D., Song, D., and Wang, C. (eds.), *Advances in Information Security: Malware Detection.* Springer, 2007.

Journal Articles

Bambauer, D., and Day, O., "The Hacker Aegis," 60 *Emory Law Journal* (2011).

Bond, C., "There's Nothing Worse Than a Muddle in all the World: Copyright Complexity and Law Reform in Australia," 34 *UNSWLJ* 1145 (2011).

——, "Commonwealth v Wikileaks: Fairfax Revisisted," 18 *M&ALR* 310 (2013).

Brenner, S. W., Carrier, B., and Henninger, J., "The Trojan Horse Defense in Cybercrime Cases," 21 *Santa Clara Computer and High Technology Law Journal* (2004).

Broadhurst, R., "Developments in the Global Law Enforcement of Cyber-Crime," 29(3) *Policing: An International Journal of Police Strategies and Management* 408, 418 (2006).

Chandler, J., "Security in Cyberspace: Combating Distributed Denial of Service Attacks," 1 *University of Ottawa Law & Technology Journal* 231 (2003–2004).

——, "Liability for Botnet Attacks," *Canadian Journal of Law and Technology* (2006).

Chandler, J., "Technological Self-Help and Equality in Cyberspace," 55 *McGill Law Journal* (2010).

Clarke, R., "Information Technology and Dataveillance," 31(5) *Communications of the ACM* 499 (1988).

Clarke, R., and Maurushat, A., "Who Will Bear the Cost of Insecure Devices," 18 *Journal of Law, Information and Science* 8 (2007).

——, "The Feasibility of Consumer Device Security," *UNSW Law Review Series* 5 (2009).

Cohen, F., "Computer Viruses: Theory and Experiments," 6(1) *Computers & Security* (1987).

Colangelo, A., and Maurushat, A., "Exploring the Limits of Computer Code as a Protected Form of Expression: A Suggested Approach to Encryption, Computer Viruses and Technological Protection Measures," 1 *McGill Law Journal* 51(2006).

Davis, N., "Presumed Assent: The Judicial Acceptance of Clickwrap," 22 *Berkeley Technology Law Journal* 577 (2007).

Demetriou, C., and Silke, A., "A Criminological Internet 'sting': Experimental Evidence of Illegal and Deviant Visits to a Website Trap," 43 *British Journal of Criminology* 213 (2003).

De Villiers, M., "Virus Ex Machine Res Ipsa Loquitor," *Stanford Technology Law Review* 1 (2003).

——, "Free Radicals in Cyberspace: Complex Liability Issues in Information Warfare," 4 *Northwestern Journal of Technology and Intellectual Property* 1 (2005).

——, "Distributed Denial of Service: Law, Technology & Policy," 39(3) *World Jurist Law/Technology Journal* (2006).

——, "Reasonable Foreseeability in Information Security Law: A Forensic Analysis" 30 *Hastings Communications and Entertainment Law Journal* (2008).

Dupont, B., "Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime," 67 *International Centre for Comparative Criminology* 103 (2017).

Dworkin, T. M., and Baucas, M., "Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes," 17(12) *Journal of Business Ethics* (1998).

Edwards, L. "Dawn of the death of Distributed Denial of Service: How to Kill Zombies," 24(1) *Cardozo Journal of Arts and Entertainment Law* 23 (2006).

Epstein, R., "The Theory and Practice of Self-Help," 1(1) *Journal of Law, Economics and Policy* 1 (2005).

Evron, G., "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," 9(1) *Georgetown Journal of International Affairs* (2008).

Fitri, N., "Democracy Discourses Through the Internet Communication: Understanding the Hacktivism for the Global Changing," 1 *Online Journal of Communication and Media Technologies* 2 (2011).

Freedman, J., "Protecting State Secrets as Intellectual Property: A Strategy for Prosecuting WikiLeaks," 48(1) *Stanford Journal of International Law* 185 (2012).

Geist, M., "Is There a There There: Toward Greater Certain for Internet Jurisdiction," *Berkeley Technology Law Journal* (Fall 2001).

Gervais, D., and Maurushat, A., "Fragmented Copyright, Fragmented Management: Proposals to Defrag Copyright Management," 2(1) *Canadian Journal of Law and Technology* (2003).

Gilbert, D., and Kerr, I., "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers," 51(4) *Criminal Law Quarterly* (2006).

Gobert, J., and Punch, M., "Whistleblowers, the Public Interest, and the Public Interest Disclosure Act 1998," 63(1) *The Modern Law Review* (2000).

Guzman, L., "Unleashing a Cure for the Botnet Zombie Plague," 59(2) *Catholic University Law Review* 527 (2010).

Halberstam, M., "Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks," 46 *George Washington International Law Review* 199 (2013).

Hardy, K., "Operation Titstorm: Hacktivism or Terrorist Act?," 16(1) *University of New South Wales Law Journal* (2010).

Hutchinson, W., and Warren, M., "Attitudes of Australian Information System Managers Against Online Attackers," 9(3) *Information Management & Computer Security* 106 (2001).

Jenkins, J. "Copyright Law and Political Theology: Censorship and the Forebear's Desire," 25(1) *Law and Literature* 165 (2013).

Johnston, L., "What is Vigilantism?," 26(2) *British Journal of Criminology* (1996).

Jordan, T., "Mapping Hacktivism," 4 *Computer Fraud and Security* (2001).

Kallberg, J., "A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs," 17(1) *IT Professional* 30 (2015).

Katyal, N., "Criminal Law in Cyberspace," 149 *University of Pennsylvania Law Review* 1004 (2001).

Kerr, O., "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes," 78(53) *New York University Law Review* (2003).

——, "Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability," 1 *Journal of Law, Economics and Policy* 197 (2005).

Kesan, J. P., and Hayes, C. M., "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," 25 *Harvard Journal of Law & Technology* 482 (2012).

Lessig, L., "Reading the Constitution in Cyberspace," 45 *Emory Law Journal* 1 (1997).

——, "The Law of the Horse: What Cyberlaw Might Teach," 113 *Harvard Law Review* 501 (1999).

Lin, P., "Anatomy of the Mega-D Takedown," 12 *Network Security* 4–7 (December 2009).

Maurushat, A., "Hong Kong Anti-Terrorism Ordinance and the Surveillance Society: Privacy and Free Expression Implications," 1(12/3) *Asia Pacific Media Educator* (2002).

——, "Data Breach Notification Law Across the World from California to Australia," *Privacy Law and Business International* (April 2009).

——, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in the Era of Obfuscation Crime Tools," 16(1) *University of New South Wales Law Journal* (2010).

——, "Forced Transparency: Should We Keep Secrets in Times of Weak Law, and Should the Law do More?," 17(2) *Media and Arts Law Review* 239 (2012).

Maurushat, A., and Watt, R., "Australia's Internet Filtering Proposal in the International Context," 12(2) *Internet Law Bulletin* 18 (2009).

Messerschmidt, J. E., "Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm," 52 *Columbia Journal of Transnational Law* (2013).

Ohm, P., "The Rise and Fall of Invasive ISP Surveillance," *University of Illinois Law Review* (2008), available at http://ssrn.com/abstract=1261344 (last accessed April 15, 2009).

Oleson, K., and Darley, J., "Community Perceptions of Allowable Counterforce in Self-Defense and Defense of Property," 23(6) *Law and Human Behavior* (1999).

Posner, R., "Killing or Wounding to Protect a Property Interest," 14(1) *Journal of Law and Economics* 201 (1971).

Rychlicki, T., "Legal Issues of Criminal Acts Committed Via Botnets," 12(5) *Computer and Telecommunications Law Review* 163 (2006).

Rose, C., and Gordon, J., "Internet Security and the Tragedy of the Commons," 1 *Journal of Business and Economics Research* 11 (2003).

Salgado, R., "The Legal Ramifications of Operating a Honeypot," 1 *IEEE Magazine Security and Privacy* (2005).

Shock, J., and Hupp, J., "The 'Worm' Programs—Early Experience with a Distributed Computation," 25(3) *Communications of the ACM* (1982).

Smith, B., "Hacking, Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help," 1(1) *Journal of Law, Economics and Policy* 185 (2005).

Smith, H., "Self-help and the Nature of Property," 1(1) *Journal of Law, Economics and Policy* 69 (2005).

Soghoian, Christopher, "Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era," 8 *Journal on Telecommunications and High Technology Law.* 359 (August 17, 2009); Berkman Center Research Publication No. 2009-07, 361, available at https://ssrn.com/abstract=1421553.

Solove, D., "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 *Stanford Law Review* 1393 (2001).

Steel, A., "The Meaning of Dishonesty in Theft," 38(2) *Common Law World Review* (2009).

Tamanaha, B., "Socio-Legal Positivism and a General Jurisprudence," 21(1) *Oxford Journal of Legal Studies* 21 (2001).

Thomas, J., "Ethics of Hacktivism," SANS Institute, 2000-2002, available at http://www.dvara.net/hk/Julie_Thomas_GSEC.pdf.

Thomas, T. L.,"The Internet in China: Civilian and Military Uses," (2001) 7 *Information & Security: An International Journal*, 159–173, available at http://fmso.leavenworth.army.mil/documents/china-internet.htm.

Trottier, D., "Digital Vigilantism as Weaponisation of Visibility" 30(1) *Philosophy & Technology* 55 (2016).

US-Cert (United States Computer Emergency Readiness Team), *Quarterly Trends and Analysis Report* 2(4) (2007).

Walden, I., and Flanagan, A., "Honeypots: A Sticky Legal Landscape?," 29 *Rutgers Communications and Technology Law* 315 (2003).

Warren, S., and Brandeis, L., "The Right to Privacy," 4 *Harvard Law Review* 193 (1890).

Winn, J., "Are 'Better' Security Breach Notification Laws Possible?," 24(3) *Berkeley Technology Law Journal* (2009).

Wu, T., "Application-Centered Internet Analysis," 85 *Vanderbuilt Law Review* 1163 (1999).

Young, J., "Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation," 9 *International Journal of Communications Law and Policy* (2004).

——, "Surfing While Muslim: Privacy, Freedom of Expression and the Unintended Consequences of Cybercrime Legislation—A Critical Analysis of the Council of Europe Convention on Cybercrime and the

Canadian Lawful Access Proposal," *Yale Journal of Law and Technology* 346 (2004–2005).

Websites and Articles Published Online

Abovetopsecret, "Is Serco Behind Stuxnet" (ongoing thread, started September 2010), available at http://www.abovetopsecret.com/forum/thread615788/pg1 (last accessed February 7, 2011).

ACLU Northern California, "Bank Julius Baer & Co. Ltd. v. WikiLeaks" (March 6, 2008), available at https://www.aclunc.org/our-work/legal-docket/bank-julius-baer-co-ltd-v-wikileaks.

ACLU Virginia, "In re § 2703(d) Orders," available at https://acluva.org/en/cases/re-ss2703d-orders.

Anderson, K., "Hacktivism and Politically Motivated Computer Crime" (Ensurve, 2008), available at http://politicalhacking.blogspot.com.

Anonnews, "Operation Rainbow Dark," available at http://anonnews.org/?p=press&a=item&i=1162 (accessed January 5, 2012).

Azsecure, "Other forums," available at http://www.azsecure-data.org/other-forums.html.

——, "Other data," available at http://www.azsecure-data.org/other-data.html.

Baloch, R., "Android Browser Same Origin Policy Bypass < 4.4—CVE-2014-6041," Rafay Hacking Articles, available at https://www.rafaybaloch.com/2017/06/android-browser-same-origin-policy.html.

Barlow, J. P., "A Declaration of Independence in Cyberspace," 1996, available at http://editions-hache.com/essais/pdf/barlow1.pdf (last accessed December 10, 2011).

Bendrath, R., "Frankfurt Appellate Court Says Online Demonstration is Not Coercion," EDRi, June 7, 2006, available at https://edri.org/edrigramnumber4-11demonstration/.

Berners-Lee, T., *Net Neutrality: This is Serious Blog* (2006), previously available at www.dig.csail.mit.edu/breadcrumbs/node/144 (last accessed March 3, 2010).

Boydon, C., "Building a Botnet Empire in Two Days," June 30, 2006, available at http://images.google.com.au/imgres?imgurl=http://blog.spywareguide.com/upload/2006/05/ISTAdwareThroughWMVFile/ActiveX-thumb.GIF&imgrefurl=http://blog.spywareguide.com/2006/06/&usg=__aA8hJy8hCGm0aUesHouq5e9kMzM=&h=97&w=128&sz=10&hl=en&start=13&tbnid=sxNZtB3wnM9qmM:&tbnh=69&tbnw=91&prev=/images%3Fq%3Ddollarrevenue%2Bpopup%2Bactive%2BX%26gbv%3D2%26hl%3Den.

Brandeis University, "Justice Louis J. Brandeis," Louis D. Brandeis Legacy Fund for Social Justice, available at http://www.brandeis.edu/legacyfund/bio.html (accessed March 17, 2011).

Brenner, S., "Hackback as Self-Defense, CYB3RCRIM3: Observations on Technology, Law and Lawnessness," March 24, 2007, available at http://cyb3rcrim3.blogspot.com/2007/03/hackback-as-self-defense.html (last accessed April 16, 2010).

Chaos Computer Club (CCC), "Chaos Computer Club analyzes government malware," 2011, available at http://ccc.de/en/updates/2011/staatstrojaner.

Clarke, R., "Peer-to-Peer (P2P)—An Overview," 2004, available at http://rogerclarke.com/EC/P2POview.html (last accessed February 6, 2011).

——, "Categories of Malware," September 2009, available at http://www.rogerclarke.com/II/MalCat-0909.html (last accessed February 7, 2011).

Clayton, R., "Missing the Wood for the Trees," comments on ICANN fast-flux-report, February 2009, available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

Cyberberkut, "CyberBerkut gained access to the documents of Joseph Biden's delegation officials," November 25, 2014, available at http://cyber-berkut.org/en/.

——, "CyberBerkut has blocked German Chancellor and the Bundestag's websites," January 7, 2015, available at http://cyber-berkut.org/en/.

Darknet Market Archives, available at https://www.gwern.net/DNM-archives.

Hacking Alert, "White Hat and Grey Hat Hacking: What is the Real Difference?," previously available at http://www.hackingalert.com/hacking-articles/grey-hat-hackers.php.

Derienzo, P., "Eating its Own: Hack Attack," available at http://pdr.autono.net/message2c.html (last accessed January 5, 2012).

DVLabs, "Owning Kraken Zombies: A Detailed Dischapter," April 2008, available at http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (last accessed November 11, 2010).

EDRi, "Frankfurt Appellate Court says online demonstration is not coercion," June 7, 2006, available at https://edri.org/edrigramnumber4-11 demonstration/.

E-Li, "Anti-Gay Website Hacked by Anonymous," lezbelib.over-blog.com, June 4, 2011, available at http://lezbelib.over-blog.com/article-anti-gay-website-hacked-by-anonymous-75636306.html (last accessed June 5, 2011).

El Universo, "Website of the Presidency of Ecuador suffered cyber attacks," June 20, 2011, available at http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html?p=1354&m=638 (last accessed June 21, 2011).

Falliere, N., "Stuxnet Introduces the First Known Rootkit for Industrial Control Systems," Symantec, August 6, 2010, available at http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (last accessed February 7, 2011).

Free Anons, "Interview: Ryan Ackroyd AKA Kayla of LulzSec," April 15, 2014, available at https://freeanons.org/interview-ryan-ackroyd-aka-kayla-lulzsec/.

Generic Names Supporting Organisation, "WHOIS Task Forces 1 2 3," June 7, 2005, available at https://gnso.icann.org/en/meetings/minutes-whoistf-07jun05.html (last accessed November 29, 2018).

Green Voice Of Freedom, "Who are the 'Iranian Cyber Army,'" December 15, 2010, previously available at http://en.irangreenvoice.com/article/2010/feb/19/1236 (last accessed December 16, 2010).

Gutman, P., "The Commercial Malware Industry," available at www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf (last accessed February 4, 2011).

H4ck3d By 3xp1r3 Cyber Army, Pastebin, February 12, 2012, available at http://pastebin.com/GRAmd7qq.

"Hacker History & Culture," H@cker's Handbook, available at http://www.telefonica.net/web2/vailankanni/HHB/HHB_CH03.htm (last accessed January 5, 2012).

Hackers Media, "Subordinate Court of Bangladesh Hacked," previously available http://www.hackersmedia.com/2011/11/subordinate-courts-of-bangladesh-hacked.html.

Hackerone, "Vulnerability Disclosure Guidelines, Vulnerability Disclosure Philosophy," January 10, 2018, available at https://www.hackerone.com/disclosure-guidelines.

Harrington, J., "Hacktivism: What is the Chaos Computer Club?," Suite101, September 8, 2011, previously available at http://joharrington.suite101.com/hacktivism-what-is-the-chaos-computer-club-a387917.

Himma, K., "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?," ETHICOMP Conference, Linkoping, Sweden (2005), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=799545.

Huang, S., "Same Origin Policy Bypass Vulnerability Has Wider Reach Than Thought on TREND MICRO," *Security Intelligence Blog*, September 29, 2014, available at http://blog.trendmicro.com/trendlabs-security-intelligence/same-origin-policy-bypass-vulnerability-has-wider-reach-than-thought/.

Honeynet Project, "About the Project," available at http://old.honeynet.org/misc/project.html (last accessed November 12, 2010).

——, Riden, J. "How Fast-Flux Service Networks Work," available at http://www.honeynet.org/node/132 (last accessed February 6, 2011).

Honker Union Of China, available at http://replay.web.archive.org/20010405092345/http://www.cnhonker.com/cnhonker.htm.

Luther King, Jr., M., "Letters From a Birmingham Jail" (April 16, 1963), available at The Martin Luther King, Jr. Research and Education Institute.

Available at http://mlkkpp01.stanford.edu/index.php/resources/article/annotated_letter_from_birmingham.

Krebs, B., "Ragebooter: 'Legit' DdoS Service, or Fed Backdoor?," *Krebs on Security*, May 13, 2016, available at https://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor/ (last accessed April 20, 2017).

Lara, T., "Hackers Attack Government Website in Ecuador to Protest President's Policies Against Freedom of Expression," Knight Center for Journalism in the Americas, *Journalism in the Americas Blog*, August 10, 2011, available at http://knightcenter.utexas.edu/blog/hackers-attack-news-website-ecuador.

LavaSoft, "Waledac Questions Answered," previously available at http://www.lavasoft.com/mylavasoft/company/blog/waledac-questions-answered.

Mangham, M., "The Facebook Hack: What Really Happened," *Gmangham Blog*, April 23, 2012, available at http://gmangham.blogspot.co.uk/2012/04/facebook-hack-what-really-happened.html (last accessed December 21, 2016).

Martin, M., and Kirschbaum, E., "Pro-Russian Group Claims Cyber Attack on German Government Websites," January 7, 2015, available at https://www.reuters.com/article/us-germany-cyberattack/pro-russian-group-claims-cyber-attack-on-german-government-websites-idUSKBN0KG15320150107.

Martin, P., "Australian Government Website Hacked in Protest," Technorati, February 10, 2010, available at http://technorati.com/politics/article/australian-government-website-hacked-in-protest/ (last accessed February 11, 2010).

National Cyber-Forensics Training Alliance, https://www.ncfta.net (last accessed March 2, 2011).

National Cyber Security Centrum, "Leidraad Responsible Disclosure," 2013, available at https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html.

Opsahl, K. "Cryptome's Publication of Microsoft's Compliance Manual is a Fair Use," Electronic Frontier Foundation, February 26, 2010, available at https://www.eff.org/deeplinks/2010/02/cryptomes-publication-microsofts-compliance-manual.

Pagerghost, "How to Build a Botnet Empire in Two Days," *Security Lab blog. SpywareGuide*, previously available at http://blog.spywareguide.com/2006/06/building_a_botnet_empire_in_tw_1.html (last accessed May 31, 2010).

Parliament Of Australia, www.aph.gov.au.

Pastebin, "OPCartel Proceeds," November 3, 2011, available at http://pastebin.com/XZRpjUZq.

Pospisilli, J., "Cyber Criminals Turn to P2P for DoS Attacks," July 20, 2007, available at http://tech.blorge.com/Structure:%20/2007/07/20/cyber-criminals-turn-to-p2p-for-dos-attacks? (last accessed July 1, 2010).

QMI Agency, "Hacktivist group shuts down child porn sites," Canoe Technology, October 24, 2011, available at http://technology.canoe.ca/2011/10/24/18871656.html (last accessed October 25, 2011).

Rahm, E., and Hai Do, H., "Data Cleanings: Problems and Current Approach" (2009), available at https://www.betterevaluation.org/sites/default/files/data_cleaning.pdf.RFC 1392 Internet Users Glossary. Available at https://datatracker.ietf.org/doc/rfc1392/.

Rogers, M., "Psychological Theories of Crime and Hacking," December 15, 2006, *Telematic Journal of Clinical Criminology*. Available at https://www.researchgate.net/publication/2438130_Psychological_Theories_of_Crime_and_Hacking.

Romano, M., Rosignoli, S., and Giannini, E., "Robot Wars—How Botnets Work," Window Security, October 20, 2005, available at http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html (last accessed June 17, 2010).

Rouse, M., "Definition: Back door," TechTarget, June 2007, available at http://searchsecurity.techtarget.com/definition/back-door (last accessed December 21, 2016).

Sawyer, J., "Tech Insight: The Enterprise Hacks Back!" *Dark Reading*, available at http://darkreading.com/security/attacks/showArticle.jhtml?articleID=223100750.

Schneier, B., "Stuxnet," Schneier on Security, October 7, 2010, available at http://www.schneier.com/blog/archives/2010/10/stuxnet.html (last accessed November 12, 2010).

——, "Crypto-Gram Newsletter, September 15, 2003: Benevolent Worms," available at https://www.schneier.com/crypto-gram/archives/2003/0915.html#8 (last accessed November 12, 2010).

Security Beyond Borders, "Salami technique," available at http://securitybeyondborders.org/global-security-glossary/global-security-glossary-s/ (last accessed March 18, 2011).

Stratfor, "Dispatch: Anonymous' Online Tactics Against Mexican Cartels," November 1, 2011, available at https://worldview.stratfor.com/article/dispatch-anonymous-online-tactics-against-mexican-cartels#ixzz1cj0LSuso.

Sypnowich, C., "Law and Ideology," Stanford Encyclopedia of Philosophy, October 22, 2001 (revised October 24, 2014), available at https://plato.stanford.edu/entries/law-ideology/.

Technofriends, "TechCrunch Hacked? (yes, Techcrunch got hacked)," January 26, 2010, available at http://technofriends.in/2010/01/26/did-techcrunch-got-hacked/ (last accessed November 15, 2010).

The Anonymous Log, Facebook, January 4, 2015, available at https://www.facebook.com/TheAnonymousLog.

"The Complete History of Hacking," Scribd.com, previously available at http://www.scribd.com/doc/48245151/The-Complete-History-of-Hacking-1980-2010 (last accessed January 5, 2012).

"The Gospel According To Tux," republished from newsgroup posting to various websites such as the New Hacker's Dictionary, available at http://www.fullbooks.com/The-New-Hacker-s-Dictionary-version-4-219.html.

The Old Computer, available at http://www.theoldcomputer.com/blog/index.php?start=60.

The Wrong Guy, "Activists hack French ruling party's phone numbers," WhyWeProtest, November 10, 2011, available at http://forums.whyweprotest.net/threads/activists-hack-french-ruling-partys-phone-numbers.96206/.

Tippingpoint, "Kraken Botnet Infiltration," April 2008, available at http://www.dvlabs.tippingpoint.com/blog/2008/04/28/kraken-botnet-infiltration (last accessed Nov. 12, 2010).

Tor Project, "Anonymity Online," available at https://www.torproject.org (last accessed March 17, 2011).

Tyson, J., and Crawford, S., "How Virtual Private Networks Work," April 14, 2011, available at https://computer.howstuffworks.com/vpn.htm (last accessed November 29, 2018).

Von Leitner, F., "Chaos Computer Club Clarifications," Tasty Bits from the Technology Front, February 17, 1997, available at http://tbtf.com/resource/felix.html.

Williams, Jeff, "Dismantling Waledac," *Microsoft Malware Protection Centre—Threat Research & Response Blog*, February 25, 2010, http://blogs.technet.com/b/mmpc/archive/2010/02/25/dismantling-waledac.aspx.

Zakalwe, C., "Turkish Government Websites Hacked in Protest at Internet Censorship," *Stop Turkey—BlogSpot*, July 7, 2011, available at http://stopturkey.blogspot.com/2011/07/turkish-government-websites-hacked-in.html.

Zand, J., "Indictment Alleges DDoS Attack on Gene Simmons' Web Site by Anonymous Supporter," *Justia Law Blog*, December 14, 2011, available at http://techlaw.justia.com/2011/12/14/indictment-alleges-ddos-attack-on-gene-simmons-web-site/.

Zeroday Emergency Response Team, available at https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Zeroday_Emergency_Response_Team.html.

Zorz, Z., "Anonymous shuts down child porn sites, leaks usernames," Help Net Security, October 24, 2011, available at http://www.net-security.org/secworld.php?id=11831&utm_source=twitterfeed&utm_medium=twitter&utm_campaign=s3cb0t (last accessed October 31, 2011).

Chatham House Rules Conference Presentations

Chatham House Organisation, available at http://www.chathamhouse.org.uk/about/chathamhouserule/ (last accessed February 7, 2011).

Chatham House Rules, "Internet Filtering and Censorship Proposal Forum," November 2008, Cyberspace Law and Policy Centre, the University of New South Wales, Sydney, Australia.

Closed panel on Cybercrime at AusCERT 2008 with Chatham House Rules. Law-enforcement agents from the Australian Federal Police, New South Wales, Germany and the Federal Bureau of Investigation attended.

Internet Security Operations and Intelligence 5 (ISOI5), Tallin, Estonia, 2008, Chatham House Rules.

Forensics training by Nick Klein, forensics expert and former member of the Australian Federal Police, "Cybercrime, Cyber Security and Digital Law Enforcement" Sydney, March 2010.

Technical/Industry/Academic Reports

Aycock, J., and Maurushat, A., "'Good' Worms and Human Rights" (2006), *Technical Report* 2006-846-39, Department of Computer Science, University of Calgary.

Balatazar, J., Costoya, J., and Flores, R., "Infiltrating WALEDAC Botnet's Covert Operations" (2009), TREND MICRO.

Centre For Homeland Security, George Washington University, *Into the Grey Zone: The Private Sector and Active Defense Against Cyber Threats Report 2016*, available at https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

Denning, D., "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" (2001), available at http://www.nautilus.org/infor-policy/workshop/papers/denning.html.

Hafele, D., "Three Different Shades of Ethical Hacking: Black, White and Grey" (February 23, 2004), available at http://www.sans.org/reading_room/whitepapers/hackers/shades-ethical-hacking-black-white-grey_1390.

Hancock-White, K., "Ethical Hacking," (2008) available at casper182.atspace.com/HancockWhite_ethics_paper.doc.

Imperva, "Hacker Intelligence Initiative" (October 2011), *Monthly Trend Report* #5.

Kaspersky, E., "Cruncher—the First Beneficial Virus?, " *Virus Bulletin* (1993).

Opennet Initiative, *Internet Filtering in China in 2004-2005: A Country Study*, available at https://opennet.net/studies/china.

Owens, W., Dam, K., and Lin, H. (eds.), *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities* (National Academic Press, 2009), available at https://www.nap.edu/read/12651/chapter/1.

Perriot, F., and Knowles, D., "W32.Welchia.Worm," *Symantec Security Center* (August 11, 2017), available at https://www.symantec.com/security-center/writeup/2003-081815-2308-99.

Panda Security, Quarterly Report PandaLabs (January–March 2010), available at http://www.pandasecurity.om/img/enc/Quarterly_Report_Pandalabs_Q1_2010.pdf (last accessed June 24, 2010).

Security Spotlight, "Even Governments are not Immune to Hacktivism" (February 8, 2010).

Seltzer, W., "Infrastructures of Censorship and Lessons from Copyright Resistance" (2011), USENIX, available at https://wendy.seltzer.org/pubs/seltzer-censorship.pdf.

Solomon, A., and Evron, G., "The World of Botnets," *Virus Bulletin*. (September 2008).

Symantec, *Report on the Underground Economy* (November 2008), available at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf (last accessed June 28, 2010).

TrustDefender, "In-Depth Analysis of Mebroot/Torpig Trojan Available," available at http://www.trustdefender.com/trustdefender-labs-blog-in-depth-analysis-of-mebroot-torpig-trojan-available.html (last accessed January 31, 2011).

Wheeler, D., and Larsen, G., "Techniques for Cyber Attack Attribution" (2003), *Institute for Defense Analysis*, available at https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution.

United States Department Of Justice, Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, "A Framework for a Vulnerability Disclosure Program for Online Systems" (July 2017), available at https://www.justice.gov/criminal-ccips/page/file/983996/download.

Briefing Papers/Working Papers/White Papers/Theses/Research Projects

Barroso, D., "Botnets—The Silent Threat" (2007), European Union Agency for Network and Information Security, available at https://www.enisa.europa.eu/publications/archive/botnets-2013-the-silent-threat (last accessed January 29, 2010).

Brunea, G., "DNS Sinkhole" (August 7, 2010), SANS Institute InforSec Reading Room, 2, available at http://www.sans.org/reading_room/whitepapers/dns/dns-sinkhole_33523 (last accessed February 20, 2011).

Cate, F., "Information Security Breaches: Looking Back & Thinking Ahead," Centre for Information Policy Leadership (2008), available at https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?referer=https://

www.google.com/&httpsredir=1&article=1235&context=facpub (last accessed November 29, 2018).

Clayton, R., "Complexities in Criminalising Denial of Service Attacks" written for the *Legal Subgroup of the Internet Crime Forum* (February 2006), available at www.cl.cam.ac.uk/~rnc1/complexity.pdf.

Clayton, R., "Missing the Wood for the Trees," comments on ICANN fast-flux-report (February 2009), available at http://forum.icann.org/lists/fast-flux-initial-report/msg00022.html (last accessed February 7, 2011).

Connelly, C., Maurushat, A., Vaile, D., and Van Dijk, P., "Cyber-Security Education Research Project" (2010).

Honeypot Project, "Know Your Enemy" series of whitepapers, available at http://old.honeynet.org/papers/index.html (last accessed November 12, 2010).

Krogoth, "Botnet Construction, Control and Concealment: Looking into the Current Technology and Analysing Tendencies and Future Trends" (2008), available at http://www.shadowserver.org/wiki/uploads/Information/thesis_botnet_krogoth_2008_final.pdf (last accessed July 5 2010).

Lessig, L., and Resnick, P., "The Architectures of Mandated Access Controls," available at http://cyber.law.harvard.edu/works/lessig/Tprc98_d.pdf.

Lovet, Guillaume, "Fighting Cybercrime: Technical, Juridical and Ethical Challenges," paper presented at the Virus Bulletin Conference 2009, Geneva, September 23, 2009.

Lumby, C, Green, L., and Hartley, J., "Untangling the Net: The Scope of Content Captured by Mandatory Internet Filtering" (December 2009), report written for Google Australia, available at http://www.saferinternetgroup.org/pdfs/lumby.pdf (last accessed January 3, 2011).

Martin, D. (eds.), *Privacy Enhancing Technologies* (June 30 2005). Vol. 3856 of Lecture Notes of Computer Science. Springer 2005. Available at https://link.springer.com/content/pdf/bfm%3A978-3-540-34746-0%2F1.pdf.

Maurushat, A. "Freedom House Report on Internet Freedom: Australia" (2011).

Nazario, J, "Politically Motivated Denial of Service Attacks," The Virtual Battlefield: Perspectives on Cyber Warefare, Arbor Networks, available at http://www.ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf.

Rudesill, D. S., Caverlee, J., and Sui, D., "The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box" (October 20, 2015), *Woodrow Wilson International Center for Scholars*, STIP 03, October 2015; Ohio State Public Law Working Paper No. 314, 6, available at https://ssrn.com/abstract=2676615 (last accessed November 2018).

Samuelson, P., 'Copyright, Commodification, and Censorship: Past as Prologue—But to What Future?,' Conference on the Commodification

of Information, Haifa University, 1999, available at http://www.people.ischool.berkeley.edu/~pam/papers/haifa_priv_cens.pdf.

Trend Micro, "Zeus: A Persistent Criminal Enterprise" (March 2010), available at https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_zeus-persistent-criminal-enterprise.pdf (last accessed December 2010).

Van Eeten, M., Bauer, J., Asghari, H., and Tabatabaie, S., "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data" (2010) *OECD Science, Technology and Industry Working Papers*, 2010/5, OECD Publishing.

Vaughn, Z., "Hacktivism: Civil Rights Activism in the Digital Age" (2005). University of Texas at Tyler. Available at http://zaxxon.net/eportfolio/projects/philo/HacktivismResearch_ZV.pdf [Last accessed 20 April 2011].

Wray, S., "Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics" (November 1998), available at http://nknu.pbworks.com/f/netaktivizam.pdf.

Yip, M., and Webber, C., "Hacktivism: a theoretical and empirical exploration of China's cyber warriors" paper presented at ACM WebSci '11, Third International Conference on Web Science, Koblenz, Germany, June 14–17, 2011, available at https://dl.acm.org/citation.cfm?doid=2527031.2527053.

Zenz, K., "Cyber Crime Within the Russian Federation," presentation at AusCERT 2008.

Zhao, X., Howe, D., Nissenbaum, H., and Mazeres, D., "Phantom Access Agent: a Client-Side Approach to Personal Information Control" (December 2004), available at https://nissenbaum.tech.cornell.edu/papers/paa.pdf.

Media Releases

Conroy, Stephen (Senator), "Budget provides policing for Internet safety" (May 13, 2008), available at http://www.minister.dbcde.gov.au/media/media_releases/2008/033.

Di Jiang Innovations, "DJI To Offer 'Bug Bounty' Rewards For Reporting Software Issues" (August 28, 2017), available at https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues.

FBI, "Sixteen Individuals Arrested in the United States for Alleged Roles in Cyber Attacks" (July 19, 2011), available at http://www.fbi.gov/news/pressrel/press-releases/sixteen-individuals-arrested-in-the-united-states-for-alleged-roles-in-cyber-attacks (last accessed November 10, 2011).

——, "Member of Hacking Group LulzSec Arrested for June 2011 Intrusion of Sony Pictures Computer Systems" (September 22, 2011), available at http://www.fbi.gov/losangeles/press-releases/2011/member-of-hacking-

group-lulzsec-arrested-for-june-2011-intrusion-of-sony-pictures-computer-systems (last accessed October 20, 2011).

——, "Two Men Charged in New Jersey with Hacking AT&T's Servers" (January 18, 2011), available at http://www.fbi.gov/newark/press-releases/2011/nk011811.htm (last accessed November 11, 2011).

——, "Second Member of Hacking Group Sentenced to More Than a Year in Prison for Stealing Customer Information from Sony Pictures Computers" (FBI press release, August 8, 2013), available at https://archives.fbi.gov/archives/losangeles/press-releases/2013/second-member-of-hacking-group-sentenced-to-more-than-a-year-in-prison-for-stealing-customer-information-from-sony-pictures-computers.

Sopho, "Sopho Assists Computer Crime Unit in Bringing Botnet Master to Justice" (June 12, 2008), available at http://www.sophos.com/pressoffice/news/articles/2008/06/bentley-imprisoned.html.

US Attorney's Office, Northern District of California, "Thirteen Defendants Plead Guilty For December 2010 Cyber-Attack Against PayPal" (December 6, 2013), available athttp://www.justice.gov/usao/can/news/2013/2013_12_06_thirteen.guiltyplea.press.html.

US Department Of Justice, Western District of Washington, "California Man Pleads Guilty in 'Botnet' Attack That Impacted Seattle Hospital and Defense Department" (May 4, 2006), available at https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/maxwellPlea.htm (last accessed November 2018).

US Division—Center, "Soldier Faces Criminal Charges" (July 6, 2010), available at http://www.cbsnews.com/htdocs/pdf/ManningPreferralofCharges.pdf.

Magazine and Newspaper Articles

Abad-Santos, A., "Susan G. Komen Foundation was Hacked Last Night," *Atlantic Wire*, February 2, 2012, available at http://www.theatlanticwire.com/national/2012/02/susan-g-komen-foundation-website-was-hacked-last-night/48192/.

ABC News, "Japanese Web Sites Hacked," January 25, 2001, available at http://abcnews.go.com/Technology/story?id=99306&page=1 (last accessed November 14, 2011).

Aegerter, G., "13 Alleged Members of Anonymous Hacking Group indicted, accused of Participating in Operation Payback," *NBC News*, November 3, 2015, available at https://www.nbcnews.com/news/world/13-alleged-members-anonymous-hacking-group-indicted-accused-participating-operation-flna8C11332039.

Alizar, A., "AOSP Browser SOP," *Xakep*, September 18, 2014, available at http://xakep.ru/news/aosp-browser-sop/.

Allen, J., "Ethical hacker points out security concerns with using home baby monitors," *7News Denver*, January 28, 2015, available at http://www.thedenverchannel.com/news/local-news/ethical-hacker-points-out-security-concerns-with-using-home-baby-monitors01282015.

Anderson, N., "Vint Cerf: one quarter of all computers part of a botnet," *Ars Technica*, January 26, 2007, available at http://www.arstechnica.com/news.ars/post/20070125-8707.html. (last accessed May 31, 2011).

Andy, 'Sports Streamers, Indexes and Broadcast Tools Hit By DDoS Attacks', *Torrent Freak*, June 11, 2013, available at https://torrentfreak.com/sports-streamers-indexes-and-broadcast-tools-hit-by-ddos-attacks-130611/.

AnonWatcher, "GCHQ Hacked. North Korea Claimed," *AnonHQ*, January 3, 2015, available at http://anonhq.com/gchq-hacked-north-korea-claimed/.

Arthur, C., "Alleged LulzSec hacker of Sony Pictures faces trial data in December," *Guardian*, October 18, 2011, available at http://www.guardian.co.uk/technology/2011/oct/18/lulzsec-alleged-recursion-hacker-trial.

——, "Hacking Group Claiming to be LulzSec Targets US Military Dating Website," *Guardian*, March 28, 2012, available at http://www.guardian.co.uk/technology/2012/mar/28/hacking-group-lulzsec-dating-website.

——, "LulzSec Hacker Arrested Over Sony Attack," *Guardian*, August 29, 2012, available at http://www.guardian.co.uk/technology/2012/aug/29/lulzsec-hacker-arrest-sony-attack.

——, "Microsoft and Symantec Take Out Botnet Responsible for More Than $1m of Fraud," *Guardian*, February 7, 2013, available at http://www.guardian.co.uk/technology/2013/feb/07/microsoft-symantec-botnet-fraud-pcs.

Ashford, W., "Chinese university targeted by Islamic State hacktivist," *Computer Weekly*, January 18, 2016, available at http://www.computerweekly.com/news/4500271103/Chinese-university-targeted-by-Islamic-State-hacktivist.

Associated Press, "Panel Says WikiLeaks Suspect is Competent to Stand Trial," *New York Times*, April 29, 2011, A11, available at http://www.nytimes.com/2011/04/30/us/30brfs-PANELSAYSWIK_BRF.html?_r=1&ref=bradleyemanning.

Australian (The), "'Anonymous' hackers hit Visa, Mastercard and Sarah Palin in WikiLeaks revenge," December 9, 2010, available at http://www.theaustralian.com.au/in-depth/wikileaks/anonymous-hackers-hit-visa-mastercard-in-wikileaks-revenge/story-fn775xjq-1225968083650 (last accessed December 10, 2010).

Bajak, F., "Anonymous Hackers Claim They Were Infiltrated," *Bellingham Herald*, February 29, 2012, available at http://bellinghamherald.com/2012/02/29/2415830/anonymous-hackers-claim-they-were.html.

Baker, K., "Anonymous outs members of alleged Steubenville High School 'Rape Crew,'" *Jezebel*, December 24, 2012, available at http://jezebel.

com/5970975/anonymous-outs-members-of-alleged-steubenville-high-school-rape-crew.

——, "Hacking group Anonymous to target paedophiles using the 'dark web' to carry out child abuse," *Daily Mail*, January 25, 2015, available at http://www.dailymail.co.uk/news/article-2924864/Hacking-group-Anonymous-target-paedophiles.html.

Ball, J., "WikiLeaks Publishes Stratfor Emails Linked to Anonymous Attack," *Guardian*, February 27, 2012, available at http://www.guardian.co.uk/media/2012/feb/27/wikileaks-publishes-stratfor-emails-anonymous.

Baloch, F., "Online Security: Pakistani helps Google avoid privacy disaster," *Express Tribune*, September 20, 2014, available at http://tribune.com.pk/story/764713/online-security-pakistani-helps-google-avoid-privacy-disaster/.

Banyan, "Messiah complicated," *The Economist*, December 7, 2013, available at http://www.economist.com/blogs/banyan/2013/12/hacking-singapore.

——, "Two Steps Back," *The Economist*, February 25, 2014, available at http://www.economist.com/blogs/banyan/2013/06/regulating-singapores-internet.

Barlow, J. P., "Is there a there in Cyberspace?" *Utne Reader*, 1995, available at https://www.utne.com/community/isthereathereincyberspace (last accessed November 2018).

Barakat, A., and Khattab, S. "A Comparative Study of Traditional Botnets Versus Super-Botnet," in INFOSEC 2010.

Bastone, W., and Goldberg, A., "Autistic Hacker Helped FBI Nail Anonymous Boss," *The Smoking Gun*, May 13, 2014, available at http://www.thesmokinggun.com/documents/eekdacat-and-the-fbi-576432 (last accessed March 11, 2014).

Bates, D., "Anonymous threaten to unmask boys who 'drove 17-year-old girl to hang herself after they gang raped her and put photo on web,'" *Daily Mail*, April 11, 2013, available at http://www.dailymail.co.uk/news/article-2307266/Rehtaeh-Parsons-gang-rape-Anonymous-threaten-unmask-boys-drove-girl-hang-herself.html.

Batty, D., "Hacking suspect Ryan Cleary suffers from Autism, Court told," *Guardian*, June 26, 2011, available at http://www.theguardian.com/technology/2011/jun/25/hacker-ryan-cleary-diagnosed-autism (last accessed March 11, 2015).

BBC News, "A-Z Hack Attack," February 11, 2000, available at http://news.bbc.co.uk/2/hi/uk_news/639248.stm.

——, "Baidu hacked by 'Iranian cyber army,'" January 12, 2010, available at http://news.bbc.co.uk/2/hi/8453718.stm (last accessed January 13, 2010).

——, "Questions Cloud Cyber Crime Cases," October 17, 2003, available at http://www.bbc.co.uk/2/hi/technology/3202116.stm (last accessed April 27, 2010).

——, "Stuxnet Worm Hits Iran Nuclear Plant Staff Computers," September 26, 2010, available at http://www.bbc.co.uk/news/world-middle-east-11414483 (last accessed November 12, 2010).

——, "York Facebook hacking student Glenn Mangham jailed," February 17, 2012, available at https://www.bbc.com/news/uk-england-york-north-yorkshire-17079853.

——, "Anonymous hits UK government websites in Assange protest," August 21, 2012, available at http://www.bbc.com/news/technology-19330592.

——, "Anonymous hacking group target police web forum," October 24, 2012, available at http://www.bbc.com/news/uk-20072981.

——, "Lauri Love case: Hacking Suspect Wins Extradition Appeal," February 5, 2018, available at https://www.bbc.com/news/uk-england-42946540.

Bergen, J., "Anonymous hacktivists take down MasterCard.com again in support of WikiLeaks," *Geek*, June 28, 2011, available at http://www.geek.com/articles/news/anonymous-hacktivists-take-down-mastercard-com-again-in-support-of-wikileaks-20110628/ (last accessed June 29, 2011).

Berinato, S., "Attack of the Bots," *Wired*, November 1, 2006, Issue 14.11.

Beschizza, R., "LulzSec claims FBI affiliate hacked, users and botnet are exposed," *Boing Boing*, June 3, 2011, available at http://boingboing.net/2011/06/03/lulzsec-claims-fbi-a.html.

Bloomberg, "An Evolving Crisis," *Business Week*, April 10, 2008, available at https://www.bloomberg.com/news/articles/2008-04-09/an-evolving-crisis.

Blue, V., "Anonymous Hacks US Sentencing Commission and Distributes Files," *ZDNet*, January 26, 2013, available at http://www.zdnet.com/anonymous-hacks-us-sentencing-commission-distributes-files-7000010369/.

——, "Feds Stumbling After Anonymous Launches Operation Last Resort," *ZDNet*, January 30, 2013, available at http://www.zdnet.com/feds-stumbling-after-anonymous-launches-operation-last-resort-7000010541/.

Bray, H., "Rapid7 of Boston warns of Android flaw," *Boston Globe*, September 15, 2014, available at http://www.bostonglobe.com/business/2014/09/15/rapid-boston-finds-android-flaw/JJ9iHJB6YTcs10a7O9TjpN/story.html.

Brewster, T., "Anonymous Strikes Downing Street and Ministry of Justice," *Tech Week Europe*, April 10, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-government-downing-street-moj-71979.

——, "Widespread Android Vulnerability 'A Privacy Disaster', Claim Researchers," *Forbes*, September 16, 2014, available at http://www.forbes.com/sites/thomasbrewster/2014/09/16/widespread-android-vulnerability-a-privacy-disaster-claim-researchers/.

Bright, P., "Android Browser flaw a 'privacy disaster' for half of Android users," *Ars Technica*, September 17, 2014, available at http://

arstechnica.com/security/2014/09/android-browser-flaw-a-privacy-disaster-for-half-of-android-users/.

Broad, W., Markoff, J., and Sander, D., "Israeli Test Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, A1.

Broersma, M., "Hacker Pleads Guilty to Abortion Website Attack," *Tech Week Europe*, March 12, 2012, available at http://www.techweekeurope.co.uk/news/hacker-pleads-guilty-to-abortion-website-attack-66295.

——, "Anonymous Claims Home Office Website Takedown," *Tech Week Europe*, April 8, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-home-office-ddos-71886.

Brown, B., "A sinister cyber-surveillance scheme exposed," *Guardian*, June 23, 2011, available at https://www.theguardian.com/commentisfree/cifamerica/2011/jun/22/hacking-anonymous.

Builder, "Metasploit: Major Android Bug is a Privacy Disaster (CVE-2014-6041)," *LinusTechTips*, September 15, 2014, available at http://linustechtips.com/main/topic/216087-metasploit-major-android-bug-is-a-privacy-disaster-cve-2014-6041/.

Burt, J., "Anonymous Defaces Many Chinese Government Websites," *Tech Week Europe*, April 6, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-defaces-chinese-websites-71791.

Camber, R., Collins, L., and Fernandez, C., "British teenager charged over cyber attack on CIA as pirate group takes revenge on 'snitches who framed him'," *Daily Mail UK*, June 22, 2011, available at http://www.dailymail.co.uk/sciencetech/article-2006118/Ryan-Cleary-charged-cyber-attack-CIA-LulzSec-takes-revenge.html (last accessed November 10, 2011).

CBC News, "'Tell Vic Everything' tweets protest online surveillance," February 18, 2012, available at https://www.cbc.ca/news/politics/tell-vic-everything-tweets-protest-online-surveillance-1.1187721.

Chesney, B., "Legislative Hackback: Notes on the Active Cyber Defense Certainty Act discussion draft," *Law Fare Blog* (March 7, 2017), available at https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft.

Chiaramonte, P., and Winter, J., "Hacker Group Anonymous Threatens to Attack Stock Exchange," *Fox News*, October 4, 2011, available at http://www.foxnews.com/scitech/2011/10/04/hacker-group-anonymous-threatens-to-attack-stock-exchange/ (last accessed October 4, 2011).

Cluley, G., "AnonPlus, Anonymous's social network, is hacked," *Naked Security*, July 22, 2011, available at https://nakedsecurity.sophos.com/2011/07/22/anonplus-anonymouss-social-network-is-hacked/.

CNN Tech, "Hackers attack US government Web sites in protest of Chinese embassy bombing," May 10, 1999, available at http://edition.cnn.com/TECH/computing/9905/10/hack.attack/ (last accessed November 10, 2011).

Comlay, E., "Hackers target Mexico government websites," *Reuters*, September 15, 2011, available at http://www.reuters.com/article/2011/09/15/us-mexico-hackers-idUSTRE78E7AC20110915 (last accessed September 18, 2011).

Constantin, L., "Sony Pictures Russian Website Compromised," *Softpedia*, June 6, 2011, available at http://news.softpedia.com/news/Sony-Pictures-Russian-Website-Compromised-204563.shtml.

——, "AntiSec Hackers Hit 77 Law Enforcement Websites," *Softpedia*, August 1, 2011, available at http://news.softpedia.com/news/AntiSec-Hackers-Hit-77-Law-Enforcement-Websites-214555.shtml.

——, "U.K. spy agency attacked hacktivist groups," *Computer World*, February 5, 2014, available at http://www.computerworld.com/article/2487354/cybercrime-hacking/u-k--spy-agency-attacked-hacktivist-groups.html.

——, "Many Android devices vulnerable to session hijacking through the default browser," *Computer World*, September 16, 2014, available at http://www.computerworld.com/article/2684059/many-android-devices-vulnerable-to-session-hijacking-through-the-default-browser.html.

Couts, A., "Citibank hacked, more than 200,000 bank customers at risk," *Digital Trends*, June 9, 2011, available at http://www.digitaltrends.com/computing/citibank-hacked-more-than-200000-bank-customers-at-risk/.

——, "Hackers leak Citigroup CEO's personal data after Occupy Wall Street arrests," *Digital Trends*, August 18, 2011, available at http://www.digitaltrends.com/computing/hackers-leak-citigroup-ceos-personal-data-after-occupy-wall-street-arrests/.

Coyne, A., "How the AFP nabbed an Aussie Anonymous hacker," *It News*, March 20, 2017, available at https://www.itnews.com.au/news/how-the-afp-nabbed-an-aussie-anonymous-hacker-455142.

Currie, R., "Japanese Cyber Security Minister doesn't' know what USB Stick is," *The Register*, November 25, 2018, available at https://www.theregister.co.uk/2018/11/15/japanese_cyber_security_minister_doesnt_know_what_a_usb_stick_is/.

Curtis, S., "China Implicated in Hack of French G20 Files," *Tech Week Europe*, March 7, 2011, available at http://www.techweekeurope.co.uk/news/china-implicated-in-hack-of-french-g20-files-23062.

Daily Pakistan, September 17, 2014, available at http://dailypakistan.com.pk/daily-bites/17-Sep-2014/144263

Davis, J., "LulzSec's CIA hack just one of many high-profile hackings," *International Business Times*, June 15, 2011, available at http://www.ibtimes.com/articles/163678/20110615/google-lulzsec-s-cia-hack-just-one-of-many-high-profile-hackings.htm (last accessed June 20, 2011).

Dawn, "Pakistani researcher reveals privacy flaw in Android browsers," *Dawn*, September 20, 2014, available at http://www.dawn.com/news/1133178/pakistani-researcher-reveals-privacy-flaw-in-android-browsers.

Desjardin, M., "How a White Hat Hacker Saved Your Facebook Photos," *Reviewed*, February 19 2015, available at https://www.reviewed.com/cameras/news/how-a-hacker-saved-your-facebook-photos.

Dodd, V., and Halliday, J., "Teenager Ryan Cleary Charged Over LulzSec Hacking," *Guardian*, June 22, 2011, available at https://www.theguardian.com/technology/2011/jun/22/ryan-cleary-charged-lulzsec-hacking.

Ducklin, P., "'Shocking' Android browser bug could be a 'privacy disaster': here's how to fix it," *Naked Security*, September 16, 2014, available at http://nakedsecurity.sophos.com/2014/09/16/shocking-android-browser-bug-could-be-a-privacy-disaster-heres-how-to-fix-it/.

Dunn, J. E., "Alleged LulzSec Hacker 'Kayla' Arrested By UK Police," *CSO Online*, September 2, 2011, available at http://www.csoonline.com/article/689060/alleged-lulzsec-hacker-kayla-arrested-by-uk-police (last accessed November 10, 2011).

Eleftheriou-Smith, L., "Anonymous calls for activists to help expose international paedophile networks with 'Operation DeathEaters,'" *Independent*, January 23, 2015, available at http://www.independent.co.uk/news/uk/home-news/anonymous-calls-for-activists-to-help-expose-international-paedophile-networks-with-operation-deatheaters-9998350.html.

Elise, A., "China Hacktivists GreatFire Hit with DDoS Attack Costing Up to $30,000 Per Day," *International Business Times*, March 21, 2015, available at http://www.ibtimes.com/china-hacktivists-greatfire-hit-ddos-attack-costing-30000-day-1854692.

Enigmax, "New 4chan DDoS Targets Hated Anti-Piracy Law Firm," *Torrent Freak*, September 22, 2010, available at https://torrentfreak.com/new-4chan-ddos-targets-hated-anti-piracy-law-firm-100922/.

Ernesto, "Sports Streaming/Torrent Links Site Victorious in Court," *Torrent Freak*, May 10, 2010, available at https://torrentfreak.com/sports-streaming-torrent-links-site-victorious-in-court-100510/.

Errett, J., "Expecting Anonymous at #TMX," *Now Toronto*, November 7, 2011, available at http://www.nowtoronto.com/news/webjam.cfm?content=183319 (last accessed November 8, 2011).

Express Tribune, "Credit to our white-hats," September 21, 2014, available at http://tribune.com.pk/story/764925/credit-to-our-white-hats/.

Fan, X., "WikiLeaks accuses Union of 'censorship,"' *Cherwell News*, February 3, 2013, available at http://www.cherwell.org/news/world/2013/02/03/wikileaks-accuses-union-of-quotcensorshipquot.

Farberov, S., Pow, H., and Nye, J., "Revealed: Prosecutors turned down Reddit co-founder Aaron Swartz's request for plea deal over MIT

hacking case TWO DAYS before his suicide," *Daily Mail*, January 14, 2013, available at http://www.dailymail.co.uk/news/article-2262137/Aaron-Swartz-Reddit-founder-request-plea-deal-turned-Massachusetts-prosecutor.html#axzz2KkIHBHh6.

Farley, M., "Dissidents Hack Holes in China's New Wall," *Los Angeles Times*, January 4, 1999, available at http://articles.latimes.com/1999/jan/04/news/mn-60340.

Fernandez, C., "Second WikiLeaks payback vs. MasterCard: LulzSec or Anonymous?," *International Business Times*, June 29, 2011, available at http://www.ibtimes.com.au/second-wikileaks-payback-vs-mastercard-lulzsec-or-anonymous-1283014 (last accessed June 30, 2011).

Finkle, J., "Zombie Attack Exposes Security Flaws, Experts Say," *Sydney Morning Herald*, February 15, 2013, available at http://www.smh.com.au/technology/technology-news/zombie-attack-exposes-security-flaws-experts-say-20130215-2egpw.html.

Fisher, D., "Flaw in Android Browser Allows Same Origin Policy Bypass," *Threat Post*, September 15, 2014, available at http://threatpost.com/flaw-in-android-browser-allows-same-origina-policy-bypass/108265#comment-317786.

Fletcher, O., "China Hackers Seek to Rally Peers Against Cybertheft," *Wall Street Journal*, September 3, 2011, available at http://online.wsj.com/article/SB10001424053111903895904576546430870651962.html (last accessed September 5, 2011).

Fogarty, K., "Hackers come out of shadows to attack police, support Occupy protests," *IT World*, October 28, 2011, available at http://www.itworld.com/security/217561/hackers-come-out-shadows-attack-police-support-occupy-protests.

Fox News, "Cyberattack Targeted Personal Data of over 100,000 Federal Employees," May 26, 2012, available at https://www.foxnews.com/tech/cyberattack-targeted-personal-data-of-over-100k-federal-employees.

Franceschi-Bicchierai, L., "Anonymous claims first victim in 'Operation Charlie Hebdo,'" *Mashable*, January 11, 2015, available at http://mashable.com/2015/01/10/anonymous-operation-charlie-hebdo/.

Friedman, A., "Android bug called a 'privacy disaster,'" *Phone Arena*, September 16, 2014, available at http://www.phonearena.com/news/New-Android-bug-called-a-privacy-disaster_id60750.

Gallagher, P., "Abortion Website Hacker Caught," *Guardian*, March 11, 2012, available at http://www.guardian.co.uk/world/2012/mar/11/abortion-website-hacker-caught.

Gallagher, S., "Anonymous takes down darknet child porn site on Tor network," *Ars Technica*, October 24, 2011, available at http://arstechnica.com/business/news/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network.ars (last accessed October 31, 2011).

——, "White hat claims Yahoo and WinZip hacked by 'shellshock' exploiters," *Ars Technica*, October 7, 2014, available at http://arstechnica.com/security/2014/10/white-hat-claims-yahoo-and-winzip-hacked-by-shellshock-exploiters/.

Goldman, J., "Indonesian Government Sites Hacked Following Hacker's Arrest," *eSecurity Planet*, January 31, 2013, available at http://www.esecurityplanet.com/hackers/indonesian-government-sites-hacked-following-hackers-arrest.html.

Gover, D., "Anonymous Hackers Threaten Web War Against Hong Kong Police and Government," *International Business Times*, October 2, 2014, available at http://www.ibtimes.co.uk/anonymous-hackers-threaten-web-war-against-hong-kong-police-government-1468220.

Grant, D., "NYSE Hacked! Is The Anonymous Infrastructure Crumbling?," *New York Observer*, October 10, 2011, available at http://www.observer.com/2011/10/nyse-remains-unhacked-is-the-anonymous-infrastructure-crumbling-video/ (last accessed October 10, 2011).

Greenberg, A., "The Streisand Effect," *Forbes*, May 11, 2007, available at http://www.forbes.com/2007/05/10/streisand-digg-web-tech-cx_ag_0511streisand.html.

——, "Chinese Botnet Sells Point-And-Click Cyberattacks," *Forbes*, September 13, 2010, available at https://www.forbes.com/sites/andygreenberg/2010/09/13/chinese-botnet-sells-point-and-click-cyberattacks/#5ccf7aee3070.

Halliday, J., "Gene Simmons gets kiss of death from notorious web forum," *Guardian*, October 14, 2010, available at http://www.guardian.co.uk/technology/blog/2010/oct/14/gene-simmons-anonymous-attack-filesharing.

——, "Anonymous Teenager Hacker Spared Jail over Cyber Attacks," *Guardian*, February 1, 2013, available at http://www.guardian.co.uk/technology/2013/feb/01/anonymous-teenage-hacker.

——, "Briton Lauri Love faces hacking charges in US," *Guardian*, October 29, 2013, available at http://www.theguardian.com/world/2013/oct/28/us-briton-hacking-charges-nasa-lauri-love.

Halliday, J., and Arthur, C., "Anonymous' Release of Met and FBI Call Puts Hacker Group Back Centre Stage," *Guardian*, February 3, 2012, available at http://www.guardian.co.uk/technology/2012/feb/03/anonymous-hack-met-fbi-call.

Huffington Post, "Anonymous Claims Suspect Confessed To Rehtaeh Parsons' Rape," April 12, 2013, available at http://www.huffingtonpost.com/2013/04/12/anonymous-suspect-confession-rehtaeh-parsons-rape_n_3070615.html.

Hughes, M., "This Android Browser Bug Will Make You Upgrade To KitKat," *Make Use Of*, September 25, 2014, available at http://www.makeuseof.com/tag/this-android-browser-bug-will-make-you-upgrade-to-kitkat/.

Hunn, D., "How computer hackers changed the Ferguson protests," *St. Louis Post-Dispatch*, August 13, 2014, available at http://www.stltoday.com/news/local/crime-and-courts/how-computer-hackers-changed-the-ferguson-protests/article_d81a1da4-ae04-5261-9064-e4c255111c94.html.

IT Security Training, "First State Super in Breach of Privacy Act' June 7, 2012 available at https://www.itsecuritytraining.com.au/articles/first-state-super-breach-privacy-act.

Jardin, X., "Anonymous hacks BART after wireless shutdown; protests planned for Monday," *Boing Boing*, August 14, 2011, available at http://boingboing.net/2011/08/14/anonymous-hacks-bart-after-wireless-shutdown-protests-planned-for-monday.html.

Jerusalem Post, "Online activists hack into Syrian government websites," September 26, 2011, available at https://www.jpost.com/Middle-East/Online-activists-hack-into-Syrian-government-websites (last accessed September 27, 2011).

Jha, A. K., "#OpHK aka Operation Hong Kong: Anonymous hacks Chinese Government website," *Tech Worm*, 2014, available at http://www.techworm.net/2014/10/operation-hong-kong-anonymous-hacks-chinese-government-website.html.

——, "RedHack leaks email id's and password from Turkish Cooperation and Coordination Agency (TIKA)," *Tech Worm*, May 18, 2014, available at http://www.techworm.net/2014/05/redhack-leaks-email-ids-and-password.html.

——, "Pro-Russian Hackers leaks documents from Central Election Commission of Ukraine," *Tech Worm*, May 24, 2014, available at http://www.techworm.net/2014/05/pro-russian-hackers-leaks-documents.html.

——, "Russian Prime Minister's Twitter account hacked," *Tech Work*, August 14, 2014, available at http://www.techworm.net/2014/08/russian-prime-ministers-twitter-account.html.

Jidenma, N., "Naija Cyber Hactivists Hack EFCC website to protest proposed internet censor in Nigeria," *The Next Web*, September 28, 2011, available at http://thenextweb.com/africa/2011/05/26/nigerian-government-agency-website-hacked-by-cyberhacktivists/.

Jowitt, T. "Anonymous Attacks Polish Websites for ACTA Support," *Tech Week Europe*, January 26, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-attacks-polish-websites-for-acta-support-56450.

Karia, J., "Hacker exposes Three Million Iranian Bank Account Details," *Tech Week Europe*, available at http://www.techweekeurope.co.uk/news/hacker-three-million-iranian-bank-accounts-73161.

——, "Lebanese Hacktivists Take Down 15 Government Websites," *Tech Week Europe*, available at http://www.techweekeurope.co.uk/news/lebanese-hacktivists-15-government-websites-73313.

Keller, B., "Dealing with Assange and the Wikileaks Secrets," *New York Times*, January 26, 2011, MM32.

Kharel, G. C., "Hactivist Group Gator League Brings Down British GCHQ Website, Takes Blame for N Korean Internet Outage," *International Business Times*, December 24, 2014, available at http://www.ibtimes.co.in/gator-league-brings-down-british-gchq-website-takes-blame-n-korean-internet-outage-618166.

Kirk, J., "Iranian Cyber Army Moves Into Botnets," *PCWorld*, August 25, 2010, available at http://www.pcworld.com/businesscenter/article/208670/iranian_cyber_army_moves_into_botnets.html.

——, "Turkish Hackers Strike Websites with DNS Hack," *PCWorld*, September 5, 2011, available at http://www.pcworld.com/article/239501/turkish_hackers_strike_websites_with_dns_hack.html.

Kopstein, J., "Hacker with a cause," *New Yorker*, November 21, 2013, available at http://www.newyorker.com/online/blogs/elements/2013/11/jeremy-hammond-and-anonymous-hacker-with-a-cause.html.

Kovacs, E, "Anonymous Turns Green and Goes After Polluters," *Softpedia*, November 15, 2011, available at http://news.softpedia.com/news/Anonymous-Turns-Green-and-Goes-After-Polluters-234681.shtml.

——, "French Nuke Company Fined After Hacking Greenpeace," *Softpedia*, November 16, 2011, available at http://news.softpedia.com/news/French-Nuke-Company-Fined-After-Hacking-Greenpeace-234900.shtml.

——, "Anonymous Attacks Anonymous for Being Trolls," *Softpedia*, November 16, 2011, available at http://news.softpedia.com/news/Anonymous-Attacks-Anonymous-For-Being-Trolls-234949.shtml (last accessed November 18, 2011).

——, "Anonymous Threatens Congress Over SOPA," *Softpedia*, November 17, 2011, available at http://news.softpedia.com/news/Anonymous-Threatens-Congress-Over-SOPA-235201.shtml.

——, "NSA Website Disrupted Following PRISM Leak, Hackers Want to Troll Agency," *Softpedia*, June 12, 2013, available at https://news.softpedia.com/news/NSA-Website-Disrupted-Following-PRISM-Leak-Hackers-Want-to-Troll-Agency-360574.shtml.

——, "RedHack begins hack attacks in protest against Turkey's New Internet Law," *Softpedia*, February 10, 2014, available at http://news.softpedia.com/news/RedHack-Begins-Hack-Attacks-in-Protest-Against-Turkey-s-New-Internet-Law-425418.shtml.

——, "RedHack Begins Hack Attacks in Protest Against Turkey's New Internet Law," *Tech Worm*, March 28, 2014, available at http://www.techworm.net/2014/03/redhack-ddoses-turkish.html.

——, "Dangerous "Same Origin Policy" Bypass Flaw Found in Android Browser," *Security Week*, September 16, 2014, available at http://www.securityweek.com/dangerous-same-origin-policy-bypass-flaw-found-android-browser.

Kumar, M., "Sony Music Brazil Gets Defaced!," *Hacker News*, June 5, 2011, available at http://thehackernews.com/2011/06/sony-music-brazil-gets-defaced.html (last accessed June 6, 2011).

——, "Customs Authority of Yemen Hacked for Protests against Government," *Hacker News*, August 5, 2011, available at http://thehackernews.com/2011/08/customs-authority-of-yemen-hacked-for.html.

——, "Nepal Telecommunications Authority Hacked by w3bd3f4c3r," *Hacking Beast*, August 21, 2011, available at https://thehackernews.com/2011/08/nepal-telecommunications-authority.html (last accessed August 22, 2011).

——, "Operation OpIndependencia: Anonymous hit Mexican government official websites," *Hacker News*, September 16, 2011, available at http://thehackernews.com/2011/09/operation-opindependencia-anonymous-hit.html (last accessed September 30, 2011).

——, "International Foreign Government E-Mails Hacked by TeaMp0isoN," *Hacker News*, November 7, 2011, available at http://thehackernews.com/2011/11/international-foreign-government-e.html.

——, "Anonymous Hackers hack neo-Nazis websites & leak personal info of 16,000 Finns," *Hacker News*, November 8, 2011, available at http://thehackernews.com/2011/11/anonymous-hackers-hack-neo-nazis.html.

——, "Bangladesh Supreme Court website hacked," *Hacker News*, November 11, 2011, available at http://thehackernews.com/2011/11/bangladesh-supreme-court-website-hacked.html (last accessed November 12, 2011).

——, "Operation Brotherhood Shutdown: Multiple Sites taken down by Anonymous Hackers," *Hacker News*, November 12, 2011, available at http://thehackernews.com/2011/11/operation-brotherhood-shutdown-by.html (last accessed November 13, 2011).

——, "Vatican Radio Hacked by Anonymous Hackers," *Hacker News*, March 14, 2012, available at http://thehackernews.com/2012/03/vatican-radio-hacked-by-anonymous.html.

——, "New Android Browser Vulnerability Is a "Privacy Disaster" for 70% Of Android Users," *Hacker News*, September 16, 2014, available at http://thehackernews.com/2014/09/new-android-browser-vulnerability-is.html.

Lawson, L., "You say crackers; I say hacker: A hacking Lexicon," *Tech Republic*, April 13, 2001, available at https://www.techrepublic.com/article/you-say-cracker-i-say-hacker-a-hacking-lexicon/ (last accessed July 28, 2009).

Lemos, R., "Cisco, ISS file suit against rogue researcher Robert Lemos," *SecurityFocus*, July 27, 2005, available at http://www.securityfocus.com/news/11259 (last accessed February 10, 2014).

Lennon, M., "Hackers Used Sophisticated SMB Worm Tool to Attack Sony," *Security Week*, December 19, 2014, available at http://www.securityweek.com/hackers-used-sophisticated-smb-worm-tool-attack-sony (last accessed December 21, 2016).

Leyden, J., "EU climate exchange website hit by green-hat hacker," *The Register*, July 26, 2010, available at http://www.theregister.co.uk/2010/07/26/climate_exchange_website_hack/ (last accessed July 27, 2010).

——, "Anonymous attacks PayPal in 'Operation Avenge Assange,'" *The Register*, December 6, 2010, available at http://www.theregister.co.uk/2010/12/06/anonymous_launches_pro_wikileaks_campaign/.

——, "Anonymous hackers hacked by Young Turks," *The Register*, July 22, 2011, available at http://www.theregister.co.uk/2011/07/22/anonplus_hacked/ (last accessed July 23, 2011).

——, "German states defend use of 'Federal Trojan,'" *The Register*, October 12, 2011, available at http://www.theregister.co.uk/2011/10/12/bundestrojaner/.

——, "Hackers mistake French rugby site for German stock exchange," *The Register*, November 4, 2011, available at http://www.theregister.co.uk/2011/11/04/french_rugby_site_hacktivist_maul/.

Libbenga, J., "German court to examine Lufthansa attack," *The Register*, April 1, 2005, available at https://www.theregister.co.uk/2005/04/01/lufthansa_ddos_attack/.

Liebowitz, M., "Anonymous releases IP addresses of alleged child porn viewers," *NBC News*, November 3, 2011, available at http://www.nbcnews.com/id/45147364/ns/technology_and_sciencesecurity/t/anonymous-releases-ip-addresses-alleged-child-porn-viewers/#.XAAS7S1L1PM (last accessed November 4, 2011).

——, "Hackers Target Stock Index, Hit Rugby Team Instead," *Security News Daily*, November 4, 2011, available at http://www.securitynewsdaily.com/hackers-stock-index-rugby-team-1309/.

——, "Iranian 'Cyber Warriors Team' takes credit for NASA hack," *NBC News*, May 22, 2012, available at http://www.nbcnews.com/id/47522497/ns/technology_and_sciencesecurity/t/iranian-cyber-warriors-team-takes-credit-nasa-hack/#.XADd5y1L1PM.

Limer, E., "Anonymous follows through on BART hack, organises protest," *Geekosystems*, August 15, 2011, available at http://www.geekosystem.com/anon-hacks-bart/.

Lucas, D., "Exclusive: The Legendary #Anonymous PayPal 14 Speak Out Post-Sentencing," *The Cryptosphere*, October 31, 2014, available at https://thecryptosphere.com/2014/10/31/exclusive-the-anonymous-paypal-14-speak-out-post-sentencing/.

Lynch, D., "Pro-Russian Hacker Group CyberBerkut Claims Attack On German Government Websites," *International Business Times*, January 7, 2015, available at http://www.ibtimes.com/pro-russian-hacker-group-cyberberkut-claims-attack-german-government-websites-1775874.

Madrigal, A., "Ahmadinejad Publicly Acknowledges Stuxnet Disrupted Iranian Centrifuges," *The Atlantic*, November 29, 2010, available at http://www.theatlantic.com/technology/archive/2010/11/ahmadinejad-publicly-acknowledges-stuxnet-disrupted-iranian-centrifuges/67155/# (last accessed February 7, 2011).

Malhotra, S., "Android security flaw affects millions of users," *digit*, September 16, 2014, available at http://www.digit.in/mobile-phones/android-security-flaw-affects-millions-of-users-23921.html.

Mandell, N., "Anonymous hacker group threatens Mexican drug cartel Zetas in online video," *New York Daily News*, October 31, 2011, available at http://www.nydailynews.com/news/world/anonymous-hacker-group-threatens-mexican-drug-cartel-zetas-online-video-article-1.969859#ixzz1d4sAfvE6 (last accessed November 1, 2011).

Martin, A., "How Two LulzSec Hackers Slipped Up," *The Atlantic*, July 20, 2011, available at https://www.theatlantic.com/technology/archive/2011/07/how-two-lulzsec-hackers-slipped/353089/.

Masnik, M., "Collateral Censorship: Oxford Union Replaces Assange Speech Backdrop, Citing 'Copyright' Concerns," *Tech Dirt*, February 4, 2013, available at http://www.techdirt.com/articles/20130204/01405321873/collateral-censorshipoxford-union-replaces-assange-speech-backdrop-citing-copyright-concerns.shtml.

Mccaskill, S., "Anonymous Targets Vatican Website," *Tech Week Europe*, March 8, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-targets-vatican-website-65797.

Mccarthy, T., "Andrew Auernheimer's conviction over computer fraud thrown out," *Guardian*, April 12, 2014, available at https://www.theguardian.com/technology/2014/apr/11/andrew-auernheimers-weev-conviction-vacated-hacking.

Messmer, E., "Symantec vs. Hotbar: Who Won?" *Network World*, January 3, 2006, previously available at http://www.networkworld.com/weblogs/security/011312.html.

Mick, J., "Anonymous Engages in Sony DDoS Attacks Over GeoHot PS3 Lawsuit," *Daily Tech*, April 4, 2011, available at http://www.dailytech.com/Anonymous+Engages+in+Sony+DDoS+Attacks+Over+GeoHot+PS3+Lawsuit/article21282.htm.

Millman, R., "SCO hit by hacker protest," *SC Magazine*, November 29, 2004, available at http://www.scmagazineus.com/sco-hit-by-hacker-protest/article/31510/.

Mills, E., "Hackers taunt Sony with more data leaks, hacks," *CNET*, June 6, 2011, available at http://news.cnet.com/8301-27080_3-20069443-245/hackers-taunt-sony-with-more-data-leaks-hacks/.

——, "AT&T-iPad hacker pleads guilty to computer charges," *Cnet*, June 23, 2011, available at http://news.cnet.com/8301-27080_3-20073791-245/at-t-ipad-hacker-pleads-guilty-to-computer-charges/.

——, "AT&T-iPad site hacker to fight on in court (exclusive)," *Cnet*, September 12, 2011, available at http://news.cnet.com/8301-27080_3-20105097-245/at-t-ipad-site-hacker-to-fight-on-in-court-exclusive/.

Moses, A. "Operation Titstorm: hackers bring down government websites," *Sydney Morning Herald*, February 10, 2010, available at https://www.smh.com.au/technology/operation-titstorm-hackers-bring-down-government-websites-20100210-nqku.html.

——, "Super bad: First State set police on man who showed them how 770 000 accounts could be ripped off," *Sydney Morning Herald*, October 18, 2011, available at http://www.smh.com.au/it-pro/security-it/super-bad-first-state-set-police-on-man-who-showed-them-how--770000-accounts-could-be-ripped-off-20111018-1lvx1.html (last accessed October 18, 2011).

——, "Super sloppy: First State customers kept in the dark," *Sydney Morning Herald*, October 19, 2011, available at http://www.smh.com.au/it-pro/security-it/super-sloppy-first-state-customers-kept-in-the-dark-20111019-1m7g6.html (last accessed October 20, 2011).

Muncaster, P. "Chinese hacktivists launch cyber attack on Japan," *The Register*, September 21, 2012, available at http://www.theregister.co.uk/2012/09/21/japan_china_attack_sites_senkaku/.

——, "US software firm hacked for years after suing China," *The Register*, November 29, 2012, available at https://www.theregister.co.uk/2012/11/29/solid_oak_china_hacked_three_years/.

Muthiyah, L., "Deleting Any Album—How I Hacked Your Facebook Photos," *The Zero Hack*, November 8, 2015, available at https://thezerohack.com/how-i-hacked-your-facebook-photos#articlescroll.

NDTV Correspondent, "Android Browser Security Hole Affects Millions of Users, Says Expert," *Gadgets360*, September 16, 2014, available at http://gadgets.ndtv.com/mobiles/news/android-browser-security-hole-affects-millions-of-users-says-expert-592578.

Neal, D., "Team Poison hacks Blackberry after riots," *The Inquirer*, August 9, 2011, available at http://www.theinquirer.net/inquirer/news/2100557/team-poison-hacks-blackberry-riots.

Nuttall, C., "Chinese protesters attack Indonesia through Net," *BBC News*, August 19, 1998, available at http://connections-qj.org/article/internet-china-civilian-and-military-uses.

Ockenden, W., "Crime Stoppers website hacked, police email addresses published in spying scandal 'payback,'" ABC News, November 27, 2013, available at http://www.abc.net.au/news/2013-11-26/crime-stoppers-site-targeted-by-indonesian-hackers/5116856.

Olson, P., "How Twitter Helped Brazil Become a Hotbed for Hacktivists," *Forbes*, February 27, 2012, available at http://www.forbes.com/sites/parmyolson/2012/02/27/how-twitter-helped-brazil-become-a-hotbed-for-hacktivists/.

Oremus, Will., "No, Seriously, Just Disable Java in Your Browser Right Now," *Slate*, January 14, 2013, available at https://slate.com/technology/2013/01/java-zero-day-exploit-don-t-patch-just-disable-java-in-your-browser.html.

Panda Security, "Lulzsec and Anonymous Blur Lines Between 'Hacktivism' and Criminality, According to PandaLabs Q2 Report," *PR Newswire*, July 6, 2011, available at http://www.prnewswire.com/news-releases/lulzsec-and-anonymous-blur-lines-between-hacktivism-and-criminality-according-to-pandalabs-q2-report-125068654.html (last accessed July 8, 2011).

Pauli, D., "Aussies Hacked Pentagon, US Army, and Others," *IT News*, October 29, 2013, available at https://www.itnews.com.au/news/aussies-hacked-pentagon-us-army-and-others-362202.

Pauli, D., "THREE QUARTERS of Android mobiles open to web page spy bug," *The Register*, September 16, 2014, available at http://www.theregister.co.uk/2014/09/16/three_quarters_of_droid_phones_open_to_web_page_spy_bug/.

Penenberg, A., "Hacking Bhabha," *Forbes*, November 16, 1998, available at http://www.forbes.com/1998/11/16/feat.html (last accessed November 11, 2011).

Pfeffer, A, and Yaron, O., "Israel government, security services websites down in suspected cyber-attack," *Haaretz*, November 6, 2011, available at http://www.haaretz.com/news/diplomacy-defense/israel-government-security-services-websites-down-in-suspected-cyber-attack-1.394042 (last accessed November 7, 2011).

Pilger, J., "The War on Wikileaks: A John Pilger Investigation and Interview with Julian Assange," January 13, 2011, available at http://johnpilger.com/articles/the-war-on-wikileaks-a-john-pilger-investigation-and-interview-with-julian-assange.

Pilkington, E., "Jeremy Hammond: FBI directed my attacks on foreign government sites," *Guardian*, November 16, 2013, available at http://www.theguardian.com/world/2013/nov/15/jeremy-hammond-fbi-directed-attacks-foreign-government.

Poh, I., "Hacker who called himself 'The Messiah' jailed 4 years and 8 months," *Straits Times*, January 30, 2015, available at https://www.

straitstimes.com/singapore/courts-crime/hacker-who-called-himself-the-messiah-jailed-4-years-and-8-months.

Poulsen, K., "Ex-Hacker Adrian Lamo Institutionalized, Diagnosed with Asperger's," *Wired*, May 20, 2010, available at http://www.wired.com/2010/05/lamo/.

Poulsen, K. "First 100 Pages of Aaron Swartz's Secret Service File Released," *Wired*, December 8, 2013, available at http://www.wired.com/threatlevel/2013/08/swartz-foia-release/.

Poulsen, K., "Unprecedented 25-year sentence sought for TJX hacker," *Wired*, March 19, 2010, available at http://www.wired.com/2010/03/gonzalez-gov-memo/ (last accessed March 12, 2015).

Protalinski, E., "British student jailed for hacking into Facebook," *Zdnet*, February 18, 2012, available at http://www.zdnet.com/blog/facebook/british-student-jailed-for-hacking-into-facebook/9244 (last accessed December 21, 2016).

Quinn, B., "Interpol Website Suffers 'Anonymous Cyber-Attack,'" *Guardian*, March 29, 2012, available at http://www.guardian.co.uk/technology/2012/feb/29/interpol-website-cyber-attack.

Ragan, S., "CCC is at it again—hands out copies of German Interior Minister's fingerprint," *Tech Herald*, August 1, 2008, available at http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again-–-hands-out-copies-of-German-Interior-Minister-s-fingerprint.

——, "Iranian Cyber Army defaces Voice of America and 93 other domains (Update)," *Tech Herald*, February 22, 2011, available at http://www.thetechherald.com/article.php/201108/6849/Iranian-Cyber-Army-defaces-Voice-of-America-and-93-other-domains.

——, "PBS: LulzSec attack an attempt to chill journalism," *Tech Herald*, May 30, 2011, available at http://www.thetechherald.com/article.php/201122/7215/PBS-LulzSec-attack-an-attempt-to-chill-journalism.

Raman, M., "FBI Cracks Down on 'Anonymous' Over PayPal Hacking, Arrests 14," *International Business Times*, July 20, 2011, available at https://www.ibtimes.com/fbi-cracks-down-anonymous-over-paypal-hacking-arrests-14-300225 (last accessed July 21, 2011).

Rash, M. "Mother, May I?," *Security Focus*, January 23, 2008, available at https://www.securityfocus.com/columnists/463 (last accessed November 2018).

Rashid, F., "Anonymous Beards the Banks to Play Twisted Santa Claus," *Tech Week Europe*, December 21, 2011, available at http://www.techweekeurope.co.uk/news/anonymous-beards-the-banks-to-play-twisted-santa-claus-50922.

——, "Hackers Compromised Yahoo Servers Using Shellshock Bug," *Security Week*, October 6, 2014, available at http://www.securityweek.com/hackers-compromised-yahoo-servers-using-shellshock-bug.

Raywood, D., "Is the Mariposa Botnet Still Functioning?" *It News*, June 24, 2010, available at https://www.itnews.com.au/news/is-the-mariposa-botnet-still-functioning-217678 (last accessed June 26, 2010).

Reuters, "War Hack Attacks Tit For Tat," *Wired*, March 28, 2003, available at http://www.wired.com/politics/law/news/2003/03/58275 (last accessed November 10, 2011).

——, "Government Website Hacked By Anonymous Over Censorship," *Sydney Morning Herald*, February 10, 2010, available at https://www.news.com.au/technology/government-websites-hacked-by-anonymous-over-censorship/news-story/d362c3330a6dfeb5632f74208c8df022.

Reuters HK, "Hackers 'disable' Hong Kong Civil Referendum Website," *Guardian*, March 23, 2012, available at http://www.guardian.co.uk/world/2012/mar/23/hackers-hong-kong-civil-referendum.

Riley, M., "China Mafia-Style Attack Drives California Firm to Brink," *Bloomberg*, November 28, 2012, available at http://www.bloomberg.com/news/2012-11-27/china-mafia-style-hack-attack-drives-california-firm-to-brink.html.

Rising, G., "Cody Kretsinger Arizona College Student Charged in Sony Hacking Case," *Huffington Post*, January 12, 2010, available at http://www.huffingtonpost.com/2011/09/23/cody-kretsinger-arizona-c_n_977490.html.

Romney, L., "Bart drafts new policy on disruption of cellphone service," *LA Times*, October 19, 2011, available at http://latimesblogs.latimes.com/lanow/2011/10/bart-outlines-cell-phone-service-disruption-policy.html (last accessed October 20, 2011).

Ronson, J., "Gary Mckinnon: Pentagon hacker's worst nightmare comes true," *Guardian*, August 1, 2009, available at http://www.theguardian.com/world/2009/aug/01/gary-mckinnon-extradition-nightmare (last accessed March 11, 2015).

Ross, M., "Anonymous Indonesia hacker says RBA, AFP attacks were retaliation for spying scandal," ABC News, November 21, 2013, available at http://www.abc.net.au/news/2013-11-21/hacker-says-rba-afp-attacks-were-retaliation-for-spying-scandal/5108220.

RT, "Anonymous busts Internet pedophiles," November 3, 2011, available at http://rt.com/usa/news/anonymous-child-tor-porn-513/ (last accessed November 15, 2011).

——, "NSA Site went down due to 'internal errors,' not DDoS attack, agency claims," October 27, 2013, available at http://rt.com/usa/nsa-site-ddos-attack-754/.

——, "Eye for eye? N. Korea internet restored after 9.5hr blackout," December 23, 2014, available at http://rt.com/news/216887-north-korea-internet-blackout/.

——, "Hacktivist group 'takes down' GCHQ website, claims N. Korean blackout," December 24, 2014, available at http://rt.com/news/217211-gchq-website-down-hackers/.

——, "Hacktivist leak alleges 'extortion & money laundering' by Ukraine's Right Sector leader," February 1, 2015, available at http://rt.com/news/228387-ukraine-hacktivists-leak-yarosh/.

Rushe, D., "Anonymous Publishes Trove of Emails from Haditha Marine Law Firm," *Guardian*, February 7, 2012, available at http://www.guardian.co.uk/technology/2012/feb/06/anonymous-haditha-killings.

——, "Anonymous Sends Unhappy Valentine's Day Greetings," *Guardian*, February 14, 2012, available at http://www.guardian.co.uk/world/us-news-blog/2012/feb/14/anonymous-hacking-valentines-day-nasdaq.

Russon, M., "Anonymous brings down 30 Chinese government websites to support Hong Kong protesters," *International Business Times*, April 13, 2015, available at http://www.ibtimes.co.uk/anonymous-brings-down-30-chinese-government-websites-support-hong-kong-protesters-1496069.

Saarinen, J., "Aussie Anon sentenced to three years' prison," *IT News*, November 19, 2015, available at https://www.itnews.com.au/news/aussie-anon-sentenced-to-three-years-prison-411978.

Sanchez, F., "Hackers hijack Twitter accounts of Chavez critics," *NBC News*, September 27, 2011, available at http://www.nbcnews.com/id/44689342/ns/technology_and_sciencesecurity/t/hackers-hijack-twitter-accounts-chavez-critics/.

Satter, R., and Sullivan E., "North Korea outage a case study in online uncertainties," *Sydney Morning Herald*, December 25, 2014, available at http://www.smh.com.au/digital-life/digital-life-news/north-korea-outage-a-case-study-in-online-uncertainties-20141224-12dltr.html.

Schroeder, S., "LulzSec Hackers Take Down CIA Website," *Mashable*, June 16, 2011, available at http://mashable.com/2011/06/16/lulzsec-hackers-cia/.

Seltzer, S., "For-Profit Company Oversaw Davis's Execution, Had Prompted Complaint for Illegal Purchase of Lethal Injection Drugs," *Alternet*, August 22, 2011, available at http://www.alternet.org/newsandviews/article/670237/for-profit_company_oversaw_davis%27s_execution,_had_prompted_complaint_for_illegal_purchase_of_lethal_injection_drugs/.

Shane, S., and Burns, J. F., "U.S. Subpoenas Twitter Over WikiLeaks Supporters," *New York Times*, January 8, 2011, available at https://www.nytimes.com/2011/01/09/world/09wiki.html.

Singel, R., "Joining Pro-Wikileaks Attacks Is As Easy As Clicking A Button," *Wired*, October 12, 2010, available at http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/.

Sky News, "Cyber-Warfare: The New Global Battlefield," October 31, 2011, available at http://news.sky.com/home/technology/article/16099978 (last accessed November 2, 2011).

Smith, P., "Indonesian claims responsibility for RBA and AFP attack," *Australian Financial Review*, November 21, 2013, available at http://www.afr.com/p/technology/indonesian_claims_responsibility_Y8kgaLtlfixvXGV5V6FH3I.

Smoking Gun, "Plea Deal Struck Over Attack on Kiss Web Sites," February 5, 2013, available at http://www.thesmokinggun.com/documents/gene-simmons-ddos-plea-587912.

Smolaks, M., "Anonymous Hits Back Over LulzSec Arrests," *Tech Week Europe*, March 7, 2012, available at http://www.techweekeurope.co.uk/news/anonymous-hits-back-over-lulzsec-arrests-65265.

——, "Two Possible TeaMp0isoN Members Arrested," Tech Week Europe, April 13, 2012, available at http://www.techweekeurope.co.uk/news/teamp0ison-policeteampoison-arrested-72738.

Solon, O. "Anonymous 'hacktivists' attack ISIS—strike down terrorist propaganda and recruitment sites," *Mirror*, February 9, 2015, available at http://www.mirror.co.uk/news/technology-science/technology/anonymous-hacktivists-attack-isis---5130966.

Storm, S., "London court: LulzSec hackers called 'latter day pirates' at 'cutting-edge' of cybercrime," *Computer World*, May 15, 2013, available at https://www.computerworld.com/article/2475432/cybercrime-hacking/london-court--lulzsec-hackers-called--latter-day-pirates--at--cutting-edge--of-cy.html.

Sydney Morning Herald, "Telstra offshoot hires teen hacker 'Akill,'" March 24, 2009, available at http://www.smh.com.au/national/telstra-offshoot-hires-teen-hacker-akill-20090324-97yn.html (last accessed March 11, 2015).

——, "Man Arrested Over Bizarre Hacking Campaign Involving Cat," February 11, 2013, available at http://www.smh.com.au/technology/technology-news/man-arrested-over-bizarre-hacking-campaign-involving-cat-20130211-2e77o.html.

Takver, "European Climate Exchange website hacked," *Independent Media Centre Australia*, July 25, 2010, available at http://indymedia.org.au/2010/07/24/european-climate-exchange-website-hacked (last accessed July 29, 2010).

Talal, S., "Pakistani Researcher Helps Google in Preventing a Massive Security Disaster, *ProPakistani*, 2014, available at http://propakistani.pk/2014/09/23/pakistani-researcher-helps-google-preventing-massive-security-disaster/.

Tarantola, A., "US Nuke Stockpile Control Systems Are 'Under Constant Attack,'" *Gizmodo*, March 21, 2012, available at http://gizmodo.com/5895033/us-nuke-stockpile-control-systems-are-under-constant-attack.

The Age, "The Cyberspace Wars," June 22, 2003, available at http://www.theage.com.au/articles/2003/06/21/1056119529509.html (last accessed December 2010).

Tech Herald, "CCC is at it again—hands out copies of German Interior Minister's fingerprint," April 1, 2008, available at http://www.thetechherald.com/article.php/200814/581/CCC-is-at-it-again-hands-out-copies-of-German-Interior-Minister-s-fingerprint (last accessed July 15, 2010).

Ticehurst, J., "HSBC internet sites hacked," *V3*, September 20, 2000, available at http://www.v3.co.uk/v3-uk/news/2007500/hsbc-internet-sites-hacked.

Urdu Point, September 17, 2014, available at http://daily.urdupoint.com/livenews/2014-09-17/news-303641.html.

Walker, D., "Android bug allowing SOP bypass a 'privacy disaster,' researcher warns," *SC Magazine*, September 16, 2014, available at http://www.scmagazine.com/android-bug-allowing-sop-bypass-a-privacy-disaster-researcher-warns/article/371917/.

Waugh, D., "Rehtaeh Parsons Rape Case Solved by Anonymous in Less Than 2 Hours Despite 'No Evidence'" *PolicyMic*, April 12, 201, available at https://mic.com/articles/34491/rehtaeh-parsons-rape-case-solved-by-anonymous-in-less-than-2-hours-despite-no-evidence#.WX5PGa8pj.

Wecanchangetheworld, "4Chan Hacks Anti Piracy Lawfirm, Leaks Porn Downloaders' Names," *Buzzfeed*, November 29, 2010, available at http://www.buzzfeed.com/wecanchangetheworld/4chan-hacks-anti-piracy-lawfirm-leaks-porn-downlo-1q36 (last accessed November 21, 2011).

Whitcomb, D., "Hacker Gets a Year in Prison for Sony Attack," *Sydney Morning Herald*, April 19, 2013, available at https://www.smh.com.au/technology/hacker-gets-a-year-in-prison-for-sony-attack-20130419-2i4hl.html.

Whyte, S. "Meet the Hacktivist Who Tried to Take Down the Government," *Sydney Morning Herald*, March 14, 2011, available at https://www.smh.com.au/technology/meet-the-hacktivist-who-tried-to-take-down-the-government-20110314-1btkt.html (last accessed November 7, 2011).

Wilson, D., "Bank of England turns to 'ethical hackers' to fix financial security," *Tech Rader*, April 23, 2014, available at http://www.techradar.com/au/news/internet/web/bank-of-england-turns-to-ethical-hackers-to-fix-financial-sector-security-1244589.

Wisniewski, C., "Sony BMG Greece the latest hacked Sony site," *Naked Security*, May 22, 2011, available at http://nakedsecurity.sophos.com/2011/05/22/sony-bmg-greece-the-latest-hacked-sony-site/.

——, "PBS.org hacked... LulzSec targets Sesame Street?," *Naked Security*, May 30, 2011, available at http://nakedsecurity.sophos.com/2011/05/30/pbs-org-hacked-lulzsec-targets-sesame-street/ (last accessed May 31, 2011).

——, "Hong Kong stock exchange (HKEx) website hacked, impacts trades," *Naked Security*, August 10, 2011, available at http://naked

security.sophos.com/2011/08/10/hong-kong-stock-exchange-hkex-website-hacked-impacts-trades/.

——, "Hong Kong stock exchange attacked for second day in a row," *Naked Security*, August 12, 2011, available at http://nakedsecurity.sophos.com/2011/08/12/hong-kong-stock-exchange-attacked-for-second-day-in-a-row/.

Wyss, J., "Political hackers are one of Latin America's newest headaches," *Miami Herald*, November 3, 2011, available at http://www.miamiherald.com/2011/10/31/2481360/political-hackers-are-one-of-latin.html.

Xinhau, "Brazilian presidency's blog hacked in protest of corruption," October 14, 2011, *China Daily*, previously available at http://www.chinadaily.com.cn/xinhua/2011-10-14/content_4060557.html.

Zetter, K., "Router Flaw is a Ticking Bomb," *Wired*, August 1, 2005, available at https://www.wired.com/2005/08/router-flaw-is-a-ticking-bomb/.

Zorz, Z., "French Hacker and Alleged Anonymous Member Arrested After Bragging on TV," *Help Net Security*, April 13, 2011, available at http://www.net-security.org/secworld.php?id=10895.

Online Videos and Podcasts

"Activists deface Syrian official websites" (Al Jazeera English, September 26, 2011), available at http://www.youtube.com/watch?v=qX30M6gakQ4.

"Anonymous—A Message to Congress on SOPA you will not infringe on our rights" (November 18, 2011), available at http://www.youtube.com/watch?v=9rbyk0h3yeg.

"Anonymous—Antisec—OP PayPal" (July 27, 2011), available at http://www.youtube.com/watch?v=aa-h0HHp908.

"Anonymous attack on MasterCard, discussed on 4 News" (December 8, 2010), available at http://www.youtube.com/watch?v=i4HKk5yB8fU.

"Anonymous Hacks Westboro Baptist Church During LIVE" (February 24, 2011), available at http://www.youtube.com/watch?v=OZJwSjor4hM.

"Anonymous Members Allegedly Unmasked, Involved in Westboro Baptist Church Hacking Incident" (June 21, 2011), available at http://www.youtube.com/watch?v=QBExfh1oZCs.

"Anonymous Message to the Australian Government" (February 14, 2010), available at http://www.youtube.com/watch?v=yK1nsGFsvbo.

"Anonymous Message to the Oakland Police Department and City of Oakland" (January 31, 2012), available at http://www.youtube.com/watch?v=SzDuSaf55ek.

"Anonymous—Operation Brotherhood Shutdown" (November 7, 2011), available at http://www.youtube.com/watch?v=ZnPTBLbazAo.

"Anonymous Operation Last Resort Video" (January 26, 2013), available at http://www.youtube.com/watch?v=WaPni5O2YyI.

Anonymous—Operation Syria (September 12, 2011), available at http://www.youtube.com/watch?v=MGfF1ixk7S0.

"Anonymous—The Aftermath of Operation Brotherhood Shutdown" (November 12, 2011), available at http://www.youtube.com/watch?v=bBe9co3l9wI&feature=related.

"Anonymous to Australia," available at http://www.youtube.com/watch?v=eEc80U46hIQ (last accessed January 13, 2011).

"Anonymous v. Westboro Baptists" (February 22, 2011), available at http://www.youtube.com/watch?v=jUcW_8Ya32Q.

"An open letter from Anonymous to the Government of Israel" (November 4, 2011), available at http://www.youtube.com/watch?v=QNxi2lV0UM0.

"Chinese Regime Suspected in Lockheed Martin Hacking" (NTDTV, June 7, 2011), available at http://www.youtube.com/watch?v=1OXO0xgN1TU.

"DHS Thought Crime Tech, PBS and Lockheed Hacked, West in Libya" (May 31, 2011), available at https://www.youtube.com/watch?v=Rvw03tGwy74.

"EDF Hacking into Greenpeace" (November 10, 2011), available at http://www.youtube.com/watch?v=-70sjmTJlsQ.

Edry, R., "Israel and Iran: A Love Story?" TED Talks, December 2012, available at https://www.ted.com/speakers/ronny_edry.

"German hackers discover government spying" (Al Jazeera English, October 25, 2011), available at http://www.youtube.com/watch?v=lIwa_-jvbDQ.

Grey, P., Risky.biz Podcast, "RB2: AusCERT Podcast: Interview with Moscow-Based Cybercrime Analyst Kimberly Zenz" (May 20, 2009).

——, Risky.biz Podcast, "Interview on Risky Business with Michael Dwyer, Chief Executive of First State Superannuation" (October 14, 2011).

"Happy Hour: Weinergate, PBS Hacked" (June 1, 2011) http://www.youtube.com/watch?v=BiGEIPT8XFQ.

Insight, "Hacktivism" (SBS News, September 27, 2011), available at https://www.sbs.com.au/news/insight/tvepisode/hacktivism.

Kemmer, R. "How to Steal a Botnet and What Can Happen When You Do" (Google Tech Talk, September 2010), available at http://www.youtube.com/watch?v=2GdqoQJa6r4 (last accessed June 26, 2010).

Langill, J., "Stuxnet Worm Detailed Examination by SANS," available on a hacker website http://www.garage4hackers.com/showthread.php?604-Stuxnet-Worm-Detailed-Examination-by-SANS (last accessed February 7, 2011).

"LulzSec hacks Atlanta Infragard and challenges FBI" (June 3, 2011), available at http://www.youtube.com/watch?v=aROWwEIPgJA.

"LulzSec Hacks the CIA" (June 17, 2011), available at http://www.youtube.com/watch?v=QzQMBaIjo_w.

"LulzSec To Take Down CIA" (CNN, June 16, 2011), available at https://www.youtube.com/watch?v=fYNf7HG1SKA.
"Operation Invade Wall Street—A Message to the Media" (October 2, 2011), available at http://www.youtube.com/watch?v=lsLuYnEyFLw.
"Operation Titstorm—Anonymous Wants Their Small Boobs" (February 12, 2010), available at http://www.youtube.com/watch?v=FdPmbiK4JGY.
The Agenda, "Attack of the Hacktivists" (TVO, October 25, 2011).
"Twitter Hacked by Iranian Cyber Army (Poetry Reading)" (December 19, 2009), available at http://www.youtube.com/watch?v=rVHZ4MaCmmQ.
"VOICE of America News Website Hacked By Iranian Cyber Army" (February 22, 2011), available at http://www.youtube.com/watch?v=nDkVveI4G8Q.
"We are Anonymous—Sony hacked" (April 28, 2011), available at http://www.youtube.com/watch?v=370bq3VS5WU.
"Website for BART customers hacked by Anonymous" (ABC News [US], August 15, 2011), available at http://www.youtube.com/watch?v=DjFSq-aTMm8&feature=related.

Wikipedia

"Anat Kamm-Uri Blau Affair," available at http://en.wikipedia.org/wiki/Anat_Kamm-Uri_Blau_affair (last accessed October 20, 2018).
"Anonymous P2P," available at http://en.wikipedia.org/wiki/Anonymous_P2P (last accessed November 12, 2010).
"Application Programming Interface Key," available at https://en.wikipedia.org/wiki/Application_programming_interface_key (last accessed November 2018).
"Bennett Arron," available at http://en.wikipedia.org/wiki/Bennett_Arron (last accessed May 31, 2010).
"Chaos Computer Club," available at http://en.wikipedia.org/wiki/Chaos_Computer_Club.
"Click Fraud," available at http://en.wikipedia.org/wiki/Click_fraud (last accessed June 30, 2010).
"Denial of Service Attack (distributed)," available at http://en.wikipedia.org/wiki/Denial-of-service_attack#Distributed_attack (last accessed June 30, 2010).
"Denial-of-service (unintentional)," available at http://www.en.wikipedia.org/wiki/Denial-of-service_attack#Unintentional_denial_of _service (last accessed June 30, 2010).
"The Gifiles," available at https://wikileaks.org/the-gifiles.html.
"Internet of Things," available at https://en.wikipedia.org/wiki/Internet_of_things (last accessed November 2018).
"IP Address," available at https://en.wikipedia.org/wiki/IP_address (last accessed November 2018).

"Peer-to-peer," available at http://en.wikipedia.org/wiki/Peer-to-peer (last accessed December 2011).

"Skype and the Bavarian Trojan in the middle," available at http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle.

"SPAM," available at http://en.wikipedia.org/wiki/E-mail_spam (last accessed June 30, 2010).

"United States v. Bradley Manning" http://en.wikipedia.org/wiki/United_States_v._Bradley_Manning (last accessed July 25, 2018).

"URL," available at https://en.wikipedia.org/wiki/URL (last accessed November 2018).

"Virtual Private Network," available at http://www.en.wikipedia.org/wiki/Virtual_private_network (last accessed June 30, 2010).

Page left blank intentionally

Appendix: Interview Questions

Question 1: Has there been an erosion of a common hacker ethos or has the ethos merely evolved into many different sets of ethics?

Question 2: In your experience with hackers, does the law offer a deterrent?

Question 3: Based on your experience interviewing hackers, what are their perceptions of the illegality of their activity?

Question 4: What types of hacking activity would you consider "ethical"?

Question 5: Should ethical hacking be exempt from cybercrime provisions, and if so what kinds of ethical hacking?

Question 6: Do you equate some forms of ethical hacking as the electronic equivalent of civil disobedience (sit-ins, protests) and if so, should the current civil disobedience framework apply to the online setting?

Question 7: Is there a need for security research exemption in cybercrime provisions (unauthorised access)?

Question 8: Is there a need for a public interest exemption in cybercrime provisions (unauthorised access)?

Question 9: Is there any advice in general that you wish to impart to those engaged in ethical hacking?

Question 10: Is there any advice in general that you wish to impart to governments and organisations in dealing with ethical hacking?

About the Cover Image and the Artist

Serendipity brought scholarly publishing and cutting-edge art production together when we discovered the work of Phillip David Stearns.

A Brooklyn-based artist, Stearns has worked at the crossroads of technology and creativity, developing, among others, a project entitled *Glitch Textiles*, which explored the intersection of digital art and textile design.

A search for an original visual translation of the hidden digital world inhabited by hackers led us to *Fragmented Memory:* a work of art in which data, software and—stunningly—jacquard woven cotton merge into "hypothetical forms of portraiture," to cite the artist.

"Since 2012," Stearns said, "if anything, I've been seduced by the aesthetics of the algorithm." With the author Alana Maurushat being a self-described ethical hacker and the artist developing a series of "Ethical Hacking workshops for non-technical people," *Fragmented Memory* seemed to us the only possible cover image for this volume.

Law, Technology and Media

Edited by Michael Geist

The *Law, Technology and Media* series explores emerging technology law issues with an emphasis on a Canadian perspective. It is the first University of Ottawa Press series to be fully published under an open access licence.

Previous titles in this collection

Derek McKee, Finn Makela, and Teresa Scassa (eds.), *Law and the "Sharing Economy": Regulating Online Market Platforms*, 2018.

Karim Benyekhlef, Jane Bailey, Jacquelyn Burkell, and Fabien Gélinas (eds.), *eAccess to Justice*, 2016.

Jane Bailey, and Valerie Steeves (eds.), *eGirls, eCitizens*, 2015.

Michael Geist (ed.), *Law, Privacy and Surveillance In Canada in the Post-Snowden Era*, 2015.

Michael Geist (ed.), *The Copyright Pentalogy: How the Supreme Court of Canada Shook the Foundations of Canadian Copyright Law*, 2013.

www.press.uottawa.ca

How will governments and courts protect civil liberties in this new era of hacktivism? *Ethical Hacking* discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto "we open governments" on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred.

Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public.

How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that *Ethical Hacking* presents a fundamental discussion of key societal questions.

"Many ethical hacking incidents are closely tied to the protection of human rights and the promotion of an open, transparent democracy."

Alana Maurushat is Professor of Cybersecurity and Behaviour at Western Syndney University. She is also on the Board of Directors for the cybercrime investigation firm IFW Global.

University of Ottawa **Press**
Law, Technology and Media
press.uOttawa.ca