COMM567: The Political Economy of Privacy and Cybersecurity

Fall 2016:
Mondays 2:00 – 4:50 in ANN 305
Instructor: Jonathan Aronson (Aronson@usc.edu)
April 22, 2016

This graduate seminar considers the challenges of maintaining and protecting privacy while improving cyber-security in the United States and globally.

Students in this course will learn:

1. An understanding of the technical challenges involving privacy and cyber security and the options for improving it (students do not have to master engineering materials)
2. An understanding of the range of cyber threats, ranging from deliberate attacks for military or political advantage through the many forms of cyber crime
3. An understanding of the fundamental problems of designing prudent national policies that are politically feasible
4. An understanding of the possibilities and limitations regarding the creation of cooperative international arrangements, involving governments and civil society, to reduce risks to cyber security
5. The interdependence of cyber security, privacy, and the regulation of information markets by national rules and global rules
6. Evaluations of illustrative remedies proposed for cyber security risks

Requirements:
Students will be evaluated on three dimensions:

1. Class participation (including attendance): 10% of the total grade
2. Team presentations: All students will be assigned to a team. Each team will be responsible for:
    a. A team project evaluating a specific policy proposal. The team will do a presentation of the analysis to the class. The presentation must be supplied to the commenting team 3 days in advance of the session.
    b. Each team will be required to present a critical analysis of another team's policy analysis. In the intelligence world this is a team commissioned to challenge the findings of the primary team in charge of a piece of intelligence analysis
    c. These two presentations will create a group grade that is worth 30% of each team member's grade
    d. The list of topic subjects for papers is attached. These may be refined. The wording, these are the core ideas. I will create teams at the end of week two.

3. Individual paper: Each student will write an individual paper on the subject of his/her team's policy topic. This paper will count for 60% of the final grade.

Please note: The class lectures and readings will provide analytic and empirical materials to introduce you to the topics covered by the team assignments. **Your papers should draw on these materials**.

Readings and Course Materials that cannot be directly downloaded will be distributed

Texts that Would Be Useful (available by download or through Amazon)

- National Research Council (NRC), Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010). Note: This book can be downloaded as a PDF from the National Academy of Sciences website (http://www.nap.edu/catalog.php?record_id=12997)

- Peter Cowhey and Jonathan Aronson, *Transforming Global Information and Communications Markets*, MIT Press, 2012 paperback edition

- Peter Cowhey and Jonathan Aronson: *Digital DNA: The Information and Production Disruption and Its Consequence for Global Governance* (forthcoming)

- P.W. Singer and Allan Friedman, *Cyber Security and Cyber War* (Oxford University Press)

Academic Conduct

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in *SCampus* in Section 11, *Behavior Violating University Standards* https://scampus.usc.edu/1100-behavior-violating-university-standards-and-appropriate-sanctions/. Other forms of academic dishonesty are equally unacceptable. See additional information in *SCampus* and university policies on scientific misconduct, http://policy.usc.edu/scientific-misconduct/.

Discrimination, sexual assault, and harassment are not tolerated by the university. You are encouraged to report any incidents to the *Office of Equity and Diversity* http://equity.usc.edu/ or to the *Department of Public Safety* http://capsnet.usc.edu/department/department-public-safety/online-forms/contact-us. This is important for the safety whole USC community. Another member of the university community – such as a friend, classmate, advisor, or faculty member – can help initiate the report, or can initiate the report on behalf of another person. *The Center for Women and Men* http://www.usc.edu/student-affairs/cwm/ provides 24/7 confidential support, and the sexual assault resource center webpage sarc@usc.edu describes reporting options and other resources.

Support Systems

A number of USC's schools provide support for students who need help with scholarly writing. Check with your advisor or program staff to find out more. Students whose primary language is not English should check with the *American Language Institute* http://dornsife.usc.edu/ali, which sponsors courses and workshops specifically for international graduate students. *The Office of Disability Services and Programs* http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.htmlprovides certification for students with disabilities and helps arrange the relevant accommodations. If an officially declared emergency makes travel to campus infeasible, *USC Emergency Information* *http://emergency.usc.edu/*will provide safety and other updates, including ways in which instruction will be continued by means of blackboard, teleconferencing, and other technology.

COURSE OUTLINE

NOTE: THE SCHEDULE OF CLASSES MAY SHIFT AS GUEST SPEAKERS ARE FINALIZED

Week 1: (8/22)

- **The Dimensions of Public Policy Analysis & the Problems of Privacy and Cyber Security**

- What is Public Policy
- What is a Policy Regime
- The Six Steps of Policy Analysis

READINGS: FOR WEEKS ONE AND TWO

- Is there a serious problem?
  Ross Anderson et al, Measuring the Costs of Cybercrime,
  http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

- Shahar Argaman and Gabi Siboni, Commercial and Industrial Cyber Theft in Israel, *Military and Strategic Affairs*, March 2014
  http://www.inss.org.il/uploadImages/systemFiles/MASA%20-%206.1.pdf

Can the market/civil society solve the problem itself? Incentive Alignment among Stakeholders:

- Tyler Moore, Introducing the Economics of Cybersecurity: Principles and Policy Options, National Research Council, Proceedings of a Workshop (hereafter NRC Workshop)
  http://www.nap.edu/openbook.php?record_id=12997&page=3

Do we have a plausible theory of how government could better solve the problem?

- William D. Nordhaus. The architecture of climate economics: Designing a global agreement on global warming *Bulletin of the Atomic Scientists January/February 2011 67: 9-18, doi:10.1177/0096340210392964* http://bos.sagepub.com/content/67/1/9.full

Do social benefits outweigh the social costs?

- Jules Polonetsky and Omer Tene, Privacy and Big Data – Making Ends Meet, 66 *Stanford Law Review Online* 25, September 3, 2013.
  http://www.stanfordlawreview.org/online/privacy-and-big-data/privacy-and-big-data

- Baruch Fischhoff, The realities of risk-cost-benefit analysis, *Science,* 30 October 2015
  http://www.sciencemag.org/content/350/6260/aaa6516.full.html

Effective implementation of the solution (political economy and administrative feasibility)?

- Samuel J. Rascoff, "Presidential Intelligence" *Harvard Law Review*, Vol. 129, No. 3, January 2016, http://harvardlawreview.org/2016/01/presidential-intelligence/

- Martin Hirt and Paul Willmott, "Strategic principles for competing in the digital age," *McKinsey Quarterly*, May 2014. Available at: http://www.mckinsey.com/insights/strategy/strategic_principles_for_competing_in_the_digital_age?cid=other-eml-ttn-mip-mck-oth-1412.

- Background: Dara Cohen, et al "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates", http://papers.ssrn.com/abstract=926516

Organizational/Societal Reaction to the Policy

- The Graying Thieves Who Nearly Got Away With a Record Heist in London - The New York Times, Dec. 12, 2015: http://www.nytimes.com/2015/12/13/world/europe/london-hatton-garden-heist.html?ref=world

Examples of Major U.S. Policy Strategies:

- "Assuring a Trusted and Resilient Information and Communications Infrastructure" *Cyberspace Policy Review.* White House. Assigned Pages: Executive Summary and pp. 1-12. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

- PCAST review for White House: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf

- Example of industry response: http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf

- How Government Gathers Information-The Notice of Inquiry: https://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities

Background supplemental readings

- General background to cybersecurity policy: Singer and Friedman, pp. 12-110
- Background: Canada's proposed cyber infrastructure solution: https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf
- Background: EU cyber security cooperation strategy report, 2013: http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline

Week 2: (8/29)

- **Introduction to the IPE of Cyber Security and its relationship with Privacy**

Historic context: 1987-1998 (pre-Internet), 1999-2005 (build out), 2005-2016 (profit driven)

No Class on September 5: Labor Day

Week 3: (9/12)

- **The Technical Challenges and Economic drivers for Cybercrime and Security**

- Understanding the co-evolution of technology and semi-organized crime
- Marketplaces and business models (advertising vs theft vs extortion)
- Chokepoints: Anti-malware, blacklisting, site takedown, registrars, payments

READINGS FOR WEEK 3:

- Scott Berinato, Who's Stealing Your Passwords? Global Hackers Create a New Online Crime Economy, *CIO Magazine,* Oct 2007. (Read whole series) http://www.cio.com/article/135500/Who_s_Stealing_Your_Passwords_Global_Hackers_Create_a_New_Online_Crime_Economy ,
- Thomas et al. Framing Dependencies Introduced by Underground Commoditization, http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_thomas.pdf, WEIS 2015.

- Paganini, Cyber Criminal Ecosystems in the Deep Web, Infosec Institute White paper, 2016.http://resources.infosecinstitute.com/cyber-criminal-ecosystems-in-the-deep-web/,

- Levchenko et al. Click Trajectories: End-to-end Analysis of the Spam Value Chain. IEEE Security and Privacy, 2011. http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf ,

- Miller, The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales, Workshop on the Economics of Information Security, 2007 (http://weis2007.econinfosec.org/papers/29.pdf)

- Gallagher, Cyberwar's Grey Market, *Slate*, January 2013 http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html,

- Background reading: Singer and Friedman, pp. 12-110

Week 4: (9/19)

- **Cyber War and Cybercrime**
  - Cyber War Capabilities
  - Restructuring National Security Capabilities—Thinking about Implementation
  - Deterrence Policy—Strategic Bargaining and Learning
  - Zero day exploits

READINGS FOR WEEK 4:

- Joseph Nye, Nuclear Lessons for Cyber Security, https://citizenlab.org/cybernorms2012/nuclearlessons.pdf

- Eric Gartzke, Bringing War on the Internet Back Down to Earth, Working Paper 2012: http://pages.ucsd.edu/~egartzke/papers/cyberwar_12062012.pdf

- William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affair*s vol. 89, no. 5 (2010), http://handle.dtic.mil/100.2/ADA527707

- Background: Paul Rosenzweig, The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059443.pdf

Zero day vulnerabilities and state procurement

- Miller, The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales, Workshop on the Economics of Information Security, 2007 (http://weis2007.econinfosec.org/papers/29.pdf)

- Gallagher, Cyberwar's Grey Market, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html, Slate, January 2013

- Background: Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/, Forbes, March 2012

Additional background readings:

- Background: Thomas Rid, "Think Again: Cyberwar," *Foreign Policy* (March/April 2012), http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full

- Background: Martin C. Libicki, Cyberdeterrence and Cyberwar (Santa Monica, CA: RAND, 2009), http://www.rand.org/pubs/monographs/MG877.html
- Background: Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," Wired Threat Level Blog (11 July 2011), Http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1
- Background: William A. Owens, Kenneth W. Dam and Herbert S. Lin, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (National Academies Press, 2009), http://www.nap.edu/catalog.php?record_id=12651

Week 5: (9/26)

- **China (and India), Cybersecurity and Espionage**

READINGS FOR WEEK 5:

- IGCC, China and Cybersecurity: Political, Economic and Strategic Dimensions, Proceedings of a Workshop, April 2012 http://igcc.ucsd.edu/assets/001/503568.pdf

- Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," The Brookings Institution (February 2012) http://www.brookings.edu/papers/2012/0223_cybersecurity_china_us_singer_lieberthal.aspx

- G. Ciboni, Cyber Security--Buildup of India's National Force, *CyFy Journal* 2014, http://www.inss.org.il/uploadImages/systemFiles/Cyber%20security--%20Buildup%20of%20India's%20National%20Force.pdf
-
- Espionage: http://www.chinausfocus.com/peace-security/cyber-espionage-reducing-tensions-between-china-and-the-united-states/
    - Background (full report highlighted in the required reading): East-West Institute on cyber détente between the US and China: http://www.ewi.info/system/files/detente.pdf
    - Background: Mandiant APT 1 report on Chinese espionage: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Week 6: (10/3)

- **Three Emerging Policy Issues: The Cloud, Privacy, and Cyber Security**
  - The Rise of the Cloud and Its Implications for Privacy and Cyber Security
  - Data Privacy
  - Cybersecurity SWIFT and Cards

READINGS FOR WEEK 6:

- Peter Cowhey and Jonathan Aronson: *Digital DNA: The Information and Production Disruption and Its Consequence for Global Governance* (forthcoming). Chapters 6-8.

Week 7: (10/10)

- **The Dimensions of Public Policy & the Problem of Critical Infrastructure Protection**
  - What is Public Policy – the public and private dimensions
  - Policy as a Hypothesis – Building the Capacity for Learning
  - Policy as Incentive Alignment Among Stakeholders
  - Political Constraints on Policy
  - Implementation Blues
  - How does the private market for cybersecurity work?

READINGS FOR WEEK 7:

- Background: Singer and Friedman: 205-246

- Background: Report of the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC) Working Group 4

- Background: National Research Council, Cybersecurity of Freight Information Systems, http://www.trb.org/main/blurbs/152722.aspx

- Background: Kenneth Cukier, Viktor Mayer-Schonberger, and Lewis Branscomb, Ensuring (and Insuring) Critical Information Infrastructure Protection, Kennedy School of Government, RWP05-055, October 2005 http:\\papers.ssrn.com/sol3/papers.cfm?abstract_id=832628

Examples of Major Policy Strategies:

- "Assuring a Trusted and Resilient Information and Communications Infrastructure" *Cyberspace Policy Review.* White House. Assigned Pages: Executive Summary and pp. 1-12. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

- PCAST review for White House: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf
- Example of industry response: http://www.itic.org/dotAsset/3ed86a62-b229-4d43-a12b-766012da4b1f.pdf
- Background: Executive Office of the President, Seizing Opportunities, Preserving Values, May 2014 (available on EOP web site)
- Background: Canada's proposed cyber infrastructure solution: https://citizenlab.org/cybernorms2012/cybersecurityfindings.pdf
- Background: EU cyber security cooperation strategy report, 2013: http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline

Incentive Alignment among Stakeholders: Economic Stakes and the Micro-economic Incentives

- Tyler Moore, Introducing the Economics of Cybersecurity: Principles and Policy Options, National Research Council, Proceedings of a Workshop (hereafter NRC Workshop) http://www.nap.edu/openbook.php?record_id=12997&page=3
- Background: Peter Cowhey and Michael Kleeman, "Unlocking the Benefits of Cloud Computing for Emerging Economies—A policy Overview," October 2012. Available at: http://irps.ucsd.edu/assets/001/503998.pdf

Legal and Organizational Dimensions:

- Lior Jacob Strahilevitz, "Towards a Positive Theory of Privacy Law," 125 *Harvard Law Review* 2010 (2013).
- On the organization of ISACs, see the series in Dark Reading: http://www.darkreading.com/analytics/efforts-to-team-up-and-fight-off-hackers-intensify/d/d-id/1319368?itc=edit_in_body_cross
- Background: Jorg Monar, "The Rejection of the EU-US Swift Interim Agreement by the European Parliament: A historic Vote and its Implications," *European Foreign Affairs Review*, 15, 2010, pp. 143-51
- Background: Goldsmith, Jack. "The Cyberthreat, Government Network Operations, and the Fourth Amendment," *Brookings Paper.* December 2010. http://www.brookings.edu/papers/2010/1208_4th_amendment_goldsmith.aspx
- Background: Peter P. Swire, The System of Foreign Intelligence Surveillance Law, George Washington Law Review, Vol. 72, 2004 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616
- Background: http://www.nytimes.com/2013/06/14/technology/secret-court-ruling-put-tech-companies-in-data-bind.html?pagewanted%3Dall&_r=0

The Politics and the Feasibility of Improving Policy Designs:

- William D. Nordhaus. The architecture of climate economics: Designing a global agreement on global warming *Bulletin of the Atomic Scientists January/February 2011 67: 9-18, doi:10.1177/0096340210392964* http://bos.sagepub.com/content/67/1/9.full

- Background: Dara Cohen, et al "Crisis Bureaucracy: Homeland Security and the Political Design of Legal Mandates", http://papers.ssrn.com/abstract=926516

Learning Challenges:

- CIA, Biases in Perception of Cause and Effect, Chapter 11 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art14.html
- Background: CFIUS Annual Report to Congress, 2013: http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2013%20CFIUS%20Annual%20Report%20PUBLIC.pdf

Week 8: (10/17)

- **Public and Private Policing of Transnational Cybercrime**
  - Public vs. Private Capabilities
  - Establishing norms in the absence of state agency

READINGS FOR WEEK 8:

- Center for Democracy and Technology, Security Proposals to ITU Could Create More Problems, Not Solutions. https://citizenlab.org/cybernorms2012/CDT2012.pdf
- UN Cybercrime document http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Lamacchia et al, Rustock and Coreflood: a call to arms for strategic offensive action, http://www.scmagazine.com/rustock-and-coreflood-a-call-to-arms-for-strategic-offensive-action/article/203204/ SC Magazine, May 2011.
- Higgins, Botnet Takedowns Can Incur Collateral Damage, http://www.darkreading.com/advanced-threats/167901091/security/news/232900383/botnet-takedowns-can-incur-collateral-damage.html , DarkReading, April 2012.
- McCoy et al. Priceless: the role of Payments in Abuse-advertised Goods, http://www.cs.gmu.edu/~mccoy/papers/CCS12Priceless.pdf, CCS 2012.
- Background on "self-defense" option: http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/
- Guidelines for corporate self-defense: Irving Lachow, Active Cyber Defense, Center for a New American Security, 2013
- Background: Valpy FitzGerald, Global Financial Information, Compliance Incentives and Terrorist Funding, European journal of Political Economy, Vol. 20, 2004.

Week 9: (10/24)

- **International Regimes:**
  - Their functions, their design, and their limitations
  - Their Links to Domestic Policy Regimes
  - How Can Policy Designs Go Wrong?
  - When Do Experts Make a Difference?

READINGS FOR WEEK 9:

Design and Functions:

- Barbara Koremenos, Charles Lipson and Duncan Snidal, The Rational Design of International Institutions. *International Organization* 55, 4, Autumn 2001, pp. 761–799 © 2001 by The IO Foundation and the Massachusetts Institute of Technology http://www.jstor.org/stable/pdfplus/3078615.pdf

Examples of International Coordination on Cyber Security:

- Knake, Robert K. "Internet Governance in an Age of Cyber Insecurity" Council on Foreign Relations. Council Special Report No. 56. September 2010. http://www.cfr.org/terrorism-and-technology/internet-governance-age-cyber-insecurity/p22832
- Background: OECD Privacy Principles, http://oecdprivacy.org/ (This link also takes you to other privacy principles)
- K&L Gates, EU-US Privacy Shield Released, March 4, 2016 http://www.jdsupra.com/legalnews/eu-us-privacy-shield-released-87863/
- NIST, Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, December 2015. http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf
- Peterson Institute of International Economics, EU-US Mutual Recognition Agreements, http://www.piie.com/publications/chapters_preview/392/07iie3624.pdf

- Vilnius IGF Forum, International Cyber Security: Background Paper. "Legal Aspects of Internet Governance: International Cooperation on Cyber-security" http://meetings.abanet.org/webupload/commupload/CL320061/relatedresources/IGF_Vilnius_Workshop_123_Background_Paper_Final.pdf
- Espionage and transparency: http://www.chinausfocus.com/peace-security/cyber-espionage-reducing-tensions-between-china-and-the-united-states/
  - Background (full report highlighted in the required reading): East-West Institute on cyber détente between the US and China: http://www.ewi.info/system/files/detente.pdf

Background: CSCAP Regional Forum Cyber Security Strategy, "Ensuring a safer cyber security environment"
http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%2020%20--%20Ensuring%20a%20Safer%20Cyber%20Security%20Environmenet.pdf

Week 10: (10/31)

- **Privacy, Personal Data Online and Cross-Border Data Flows**

READINGS FOR WEEK 10:

- *Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Mar. 2012, http://ftc.gov/os/2012/03/120326privacyreport.pdf*
- Jonathan R. Mayer and John C. Mitchell, Third-Party Web Tracking: Policy and Technology, in proc. IEEE Security & Privacy ("Oakland") 2012, https://www.stanford.edu/~jmayer/papers/trackingsurvey12.pdf
- OECD Privacy Principles, http://oecdprivacy.org/ (This link also takes you to other privacy principles)
- US surveillance programmes and their impact on EU citizens' fundamental rights: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

- Daniel Castro, The False Promise of Data Nationalism (Information Technology and Innovation Foundation, December 2013) (downloadable from web site)
- Background: Sally Annereau, Monday 22 April 2013, guardian.co.uk, http://www.guardian.co.uk/media-network/media-network-blog/2013/apr/22/data-protection-right-to-forgotten
- Background: Washington Post, NSA Secrets (available from Amazon)
- Background: APEC Privacy Principles: *http://www.apec.org/Groups/Committee-on-Trade-andInvestment/~/media/Files/Groups /ECSG/05_ecsg_privacyframewk.ashx*
- Background: Monika Kuschewsky, "OECD Privacy Guidelines—What has really changed*?*" *Privacy Laws & Business International Repor*t, December 2013, pp. 15–17. Available at: http://www.cov.com/files/Publication/650e4cae-0ed0-4122-b243-29921e8d0513/Presentation/PublicationAttachment/770065fe-b381-4ad9-9077-31f04c2368dc/OECD_Privacy_Guidelines_what_has_really_changed.pdf

- Background: Popular case studies:
  - Angwin, The Web's New Gold Mine: Your Secrets, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html *Wall Street Journal*, July, 2010.
  - Steel and Angwin, On the Web's Cutting Edge, Anonymity in Name Only, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html ,*Wall Street Journal*, August 2010.
  - Angwin, 'Scrapers' Dig Deep for Data on the Web, http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html , *Wall Street Journal*, October 2010.

Week 11: (11/7)

- **Privacy, Cyber Security and International Governance: The Rise of Multi Stakeholder Organizations**

READINGS FOR WEEK 11:

- Peter Cowhey and Jonathan Aronson: *Digital DNA: The Information and Production Disruption and Its Consequence for Global Governance* (forthcoming). Chapters 4, 5, 9.

Week 12: (11/14)

- **Privacy Policies**

READINGS FOR WEEK 12:

Privacy policy for commercial purposes

- Joseph W. Jerome, Buying and Selling Privacy: Big Data's Different Burdens and Benefits, Stanford Law Review online, September 3, 2013: http://www.stanfordlawreview.org/online/privacy-and-big-data/buying-and-selling-privacy
- Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, Mar. 2012, http://ftc.gov/os/2012/03/120326privacyreport.pdf
- Background: Jonathan R. Mayer and John C. Mitchell, Third-Party Web Tracking: Policy and Technology, in proc. IEEE Security & Privacy ("Oakland") 2012, https://www.stanford.edu/~jmayer/papers/trackingsurvey12.pdf
- Background: Alan Charles Raul, The Privacy, Data Protection and Cybersecurity Law Review, November 2014 (a review of comparative national privacy policies) http://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/singapore/fileattachment/singapore.pdf
- Background: OECD Digital Economy Paper 2013, Exploring the Economics of Personal Data
- Background: Ariel Porat and Lior Jacob Strahilevitz, Personalizing Default Rules and Disclosure with Big Data, University of Michigan Law Review, Vol. 112, 2014
- Background Resource: Journal of Privacy and Confidentiality
- Background: Popular case studies:
    - Angwin, The Web's New Gold Mine: Your Secrets, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html Wall Street Journal, July, 2010.
    - Steel and Angwin, On the Web's Cutting Edge, Anonymity in Name Only, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html ,Wall Street Journal, August 2010.

- Angwin, 'Scrapers' Dig Deep for Data on the Web, http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html , Wall Street Journal, October 2010.

Government surveillance and privacy

- IC vs LE: 215 & FISA (role of FBI vs NSA)

- 4th amendment and digital evidence, CALEA, Pen register vs wiretap, MLATs and Globalization

- Wikipedia survey page on Intelligence community surveillance disclosures https://en.wikipedia.org/wiki/Global_surveillance_disclosure

- Landau, Making Sense from Snowden: https://www.computer.org/cms/ComputingNow/pdfs/MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf IEEE Security and Privacy, 2013.
- US surveillance programmes and their impact on EU citizens' fundamental rights: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf
- Peter P. Swire, The System of Foreign Intelligence Surveillance Law, George Washington Law Review, Vol. 72, 2004 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616
- CALEA, https://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act
- Cell site simulators, https://en.wikipedia.org/wiki/Stingray_phone_tracker
- Legal issues around the DoJ/iPhone case
  - https://www.washingtonpost.com/news/volokh-conspiracy/wp/category/going-dark-debate/
    (read "Preliminary thoughts on the apple Iphone order" parts 1, 2 and 3)
- Legal issues around the DoJ/Microsoft [Irealand] case
  - https://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview
  - http://www.brookings.edu/blogs/techtank/posts/2015/09/21-lowering-temperature-microsoft-case
  - http://www.theguardian.com/technology/2015/sep/09/microsoft-court-case-hotmail-ireland-search-warrant
- Background: Goldsmith, Jack. "The Cyberthreat, Government Network Operations, and the Fourth Amendment," *Brookings Paper.* December 2010. http://www.brookings.edu/papers/2010/1208_4th_amendment_goldsmith.aspx

Week 13: (11/21) and WEEK 14: (11/28)
Team Project Presentations and Critiques

In these topics remember that policy can emerge from government authorities or by agreement among private stakeholders on how to govern particular activities. In most cases you will have to discuss how global interdependence in cyber space influences the policy options and design.

1. *The explosion of the Internet of Things in the consumer space poses numerous challenges for cyber security. Unlike information technology giants, like Apple, a large percentage of the offerings in this market will be from small to medium sized firms. Analyze the nature of the cyber risks, consider the implications of the market dynamics for this space, and develop recommendations of policies to mitigate risks.*

2. *A feature of information technology revolution is the growing share of value added in traditional goods (ranging from cars to farming) created by networked software and sensor systems. This also opens the way to new forms of cyber risks, whether for security or privacy. Take one "vertical" (e.g., autos or medical equipment) and analyze policy strategies that are emerging. What explains the choice of strategies? How adequate are they? What changes in the policy mix would be feasible and effective?*

3. *Cyber warfare is emerging although usually in small and slightly hidden ways. Analyze the vulnerability of one area of critical infrastructure in a country. Examine the feasibility of improving security against a stealth cyber-attack. Your analysis should include an analysis of what options for reprisals against the suspected attacker should be given priority (if any). Be sure to consider the attribution problem.*

4. *The line between espionage, economic espionage and pure theft has become particularly blurred in the Internet era. Moreover, it may not be clear at the time an incident is discovered which of these underlying motivations is the driver. Consider the tools available to a state for addressing these issues and the tradeoffs in different approaches for addressing information theft from state, state-sponsored or state-tolerated actors.*

5. *Two economic tools for managing behavior are liability and insurance. Each provide a mechanism for making risk explicit and valuing that risk to incent efficient actions by organizations. However, neither liability or insurance have yet been significant forces in improving cybersecurity. Explore why this is and what kinds of change in capability or policy would need to take place for them to exert due influence.*

6. *The state interest in obtaining digital forensic evidence lives at the intersection of technology issues, policy issues and the forces of globalization. Recent examples such as the Microsoft Ireland case, or the DoJ/Apple case, highlight the complex landscape around corporate global brand interest, individual consumer privacy interest and state interests in criminal enforcement capability. Select one or more examples in this space and try to identify what kinds of compromises could partially satisfy the interests of these stakeholders.*

7. *Zero-day exploits represent cyber attack capabilities that, by definition, cannot be stopped and thus carry significant value for potential attackers. Historically, the development and sale of such capabilities is legal in the United States although this has been complicated by the US involvement in the cyber provisions of the Wassenaar Arrangement. Explore the policy implications around regulating the development or sale of zero-day exploits, the range of stakeholder interests, and why Wassenarr was not considered a success. Identify what reasonable goals might be and what kinds of policies might achieve those goals in the light of these findings.*

8. *Arms control agreements and laws of war have been used for over one hundred years to attempt to reduce the chances of war and/or limit the range of damage of war. Create a proposal for two or three measures to address the risks of cyber war or terrorism. Analyze the feasibility of the proposals and the benefits and costs entailed by the measures.*

9. *Today's Internet services sell to a global market and are provided "in the cloud" by computers in data centers distributed internationally. While this broad distribution makes sense technically, it does not eliminate issues of national interest. For example, the recent revelations of surveillance with and against US service providers has undermined international trust in these entities and may impact their ability to sell services abroad. Conversely, the issue of jurisdiction complicates the offering of distributed services (e.g., what is the relationship between where data is stored and who may lawfully request access to the data)? Examine at least one such issue in depth, explore the tensions between stakeholders and what kinds of solutions (either from the private sector, individual governments or from international cooperation) might feasibly address these tensions*