IGA-236: Internet Security: Technology, Policy, and Law
Harvard Kennedy School
Spring 2017

Mondays and Wednesdays
2:45–4:00 PM
Room: Littauer 130

Instructor:

Bruce Schneier
bruce_schneier@hks.harvard.edu
Office: 1 Brattle, Suite 470, Room 479
Office Hours: TBD, or by appointment

Course Assistants:

Kirsten Rulf
Kirsten_rulf@hks17.harvard.edu

Andrew McClure
Andrew_McClure@hks17.harvard.edu

Faculty Assistant:

Karin Vander Schaaf
karin_vander_schaaf@harvard.edu
(617) 496-5584
Office: Belfer 322

1. Course Description

In our information-age society, Internet security has become a paramount concern and an increasingly broad area of public policy. From cybercrime to national security, from corporate data collection to government surveillance, from cell phones to driverless cars, issues of Internet security are everywhere. These issues are complex and multifaceted, touching on such things as personal freedom and autonomy, public safety, corporate behavior and profitability, international relations, and war. This course seeks to explore the complex interplay of public policy issues in computer and Internet security.

In the first half of the course, we will survey the nature of Internet security threats, explore the human factors surrounding security, and seek to understand the basics of Internet security technologies. In the second half, we will take our newfound expertise and use it to examine a series of computer- and Internet-security policy issues, both current and near-future. Examples include government demands for encryption backdoors, software liabilities, hate speech and radical speech, digital copyright, surveillance reform, and computer-crime law. While these issues will primarily be US-focused, we will also discuss relevant issues in the EU and China, as well as international tensions and norms.

Cyberspace is fundamentally technological, and an area where public policy requires a firm understanding of the underlying technologies. Cybersecurity is no exception. This class assumes no computer science background and will make these technologies comprehensible to the layperson.
2. Course Objectives

This course aims to give students the tools necessary to understand legal and policy issues in cyberspace. While it is impossible to become a cybersecurity expert in a single semester, students will leave the course as intelligent laypeople, adept at discussing computer- and Internet-security policy issues and able to spot political agendas disguised as technical arguments. Students will understand how technology and policy interrelate, when it’s time to turn to technical experts, and how to use technical expertise to form effective policy.

This course is designed for policymakers, rather than for implementers of pre-existing policy. As such, we will not discuss how to implement Internet security policies within government organizations. We will discuss how to effectively determine which policies are the correct ones to mandate: for government, for private industry, and for individuals. This course is less about learning a body of answers, and more about learning a way of thinking about the topics in general. As a result of the class, you will be more sophisticated when you approach new Internet-security policy issues. Specifically, you will be able to weigh pros and cons, examine consequences of policies, and craft and recommend policies of your own.

3. Prerequisites

This course is open to graduate students from any Harvard school or department, and to qualified undergraduates with the permission of the instructor, and to MIT and Tufts Fletcher cross-registered students; diversity of backgrounds enriches the course. Training in natural or engineering sciences is not a requirement. Auditors will be admitted as space allows.

4. Course Requirements

Students will be encouraged to participate in class discussions, and to hone their analytical, research, and writing skills through the assignments.

The Kennedy School is a professional school, training professionals. As such, students are expected to: 1) attend all classes; 2) be on time; 3) refrain from using their laptops and cell phones in class (except when useful for discussion), 4) submit assignments on time; 5) be respectful of each other and of the instructor; 6) be prepared to be cold-called; and 7) do their best to prepare professional products for their assignments.

Grades will be calculated as follows:

- Class Participation: Every student is expected to be prepared for and attend every class, and to participate in the discussions. (25%)
- Policy Papers and Briefs: Over the course of the semester, students will write five short (500–800 word) policy memos. Each will recommend a policy action regarding an issue that will be discussed in class, and will be due before that class session. (7% each memo, 35% total)
- Final: Students will choose from a short list of cybersecurity policy issues that were not discussed in the class, and will write a 2000–3000-word analysis and policy recommendation regarding the issue. (40%)

Assignments must be posted to the class page before midnight of the day they are due. Late assignments will be marked down one grade for each day they are late, unless the professor grants an exception due to special circumstances.
Class participation will be graded on quality, not frequency. Good contributions have some of the following characteristics: (1) clear, sound, rigorous, insightful analysis; (2) comments that thoughtfully challenge conventional or politically safe positions; (3) realistic recommendations for action; (4) so-called “stupid questions” that no one else is willing to ask but that open up productive paths of inquiry; (5) constructive critique of others’ contributions; and (6) impact on the thinking of others.

Recently, the HKS faculty has addressed the issue of grade inflation. The Academic Council, with the support of the Dean, has issued recommendations on grading policy, including the following suggested curve: A (10-15%), A- (20-25%), B+ (30-40%), B (20-25%), and B- or below (5-10%).

5. Readings

Students are expected to have read the required readings before class – many of the classes will be discussions of issues raised in the readings. Recommended readings represent additional resources that may be useful for students especially interested in a particular topic, but reading them is not required for class.

Readings will be largely book chapters, or articles and essays from the popular press; it will only occasionally be academic or legal. Two books are assigned, and are available at Harvard Coop. The HKS Library will also have a copy of each book on reserve for students who do not wish to buy them.


Bruce Schneier, *Data and Goliath*, W.W. Norton, 2014 (referred to as “Schneier” on the reading list).

All other readings will be available on the Canvas Course Page.

6. Citation Practices and Academic Integrity

Everyone taking this course is working toward a position of public service and trust. Consequently, academic integrity and a solid ethical grounding are vital. It must be shown in this course.

The subject matter of this course is designed to spark discussion, and you are encouraged to talk about everything, including assignments, with your classmates. However, individual work must be done by the individual who takes credit for the work, and ideas imported from elsewhere must give credit to the source of the idea.

Students must be familiar with and must observe Kennedy School and Harvard University rules regarding the citation of sources. Including material from others in the assignments without appropriate quotation marks and citations is regarded, as a matter of School and University policy, as a serious violation of academic and professional standards and can lead to a failing grade in the course, failure to graduate, and even expulsion from the University.

7. Class Schedule

Note: the set of topics is subject to change, as the topic of cybersecurity and the policy debates around that topic change rapidly. Events may well dictate a different topic; if so we will adapt. Consult the Canvas Course Page for the most current syllabus.

Week 1. Introduction: The Security Mindset
   1/23: Thinking About Security
   1/25: Debating a Security Policy Issue: FBI and iPhone Access
Weeks 2—3. Internet Security Technologies
   1/30: Introduction to Internet Security
   2/1: Cryptography
   2/6: Access Control, Attribution, and Anonymity
   2/8: Computer and Network Security

Week 4—5. Threats and Attackers
   2/13: Threat Models and Trust Models
   2/15: Confidentiality, Integrity, and Availability; Review (Schneier will attend via Skype)
   2/20: NO CLASS—PRESIDENT’S DAY
   2/22: Taxonomy of Attackers

Week 6. Human Factors in Security
   2/27: Security Economics
   3/1: Psychology of Security, Security Usability

Weeks 7—9. Policy Issues I
   3/6: DMCA and copyright law—guest lecturer Cory Doctorow via Skype
   3/8: Regulation and the IoT—guest lecturer Melissa Hathaway
   3/13 and 3/15: NO CLASS—SPRING BREAK
   3/20: Topic TBD (Schneier may attend via Skype)
   3/22: Software liabilities and cybersecurity insurance
   3/27: National security and surveillance—guest lecturer Joel Brenner

Week 9: Technical Interlude
   3/29: Data, privacy, and surveillance

Weeks 10—13. Policy Issues II
   4/3: NSA surveillance oversight—guest lecturer John DeLong
   4/5: Surveillance reform—guest lecturer Ben Wizner
   4/10: Commercial surveillance policy
   4/12: Cyberwar
   4/17: FBI and “going dark”—guest lecturer Susan Landau
   4/19: Special topics in government surveillance
   4/24: FAA Section 702 reauthorization and reform

Week 13. Conclusion
   4/26: Final questions, overarching issues, and lessons from the class

8. Detailed Syllabus and Reading List

Yes, there are lots of readings. But most of them are short essays and news articles. Optional readings are not required, but are there for those who wish to delve more deeply into particular topics.

Readings are subject to change without notice. Consult the Canvas course page for the most current readings.

1/23: Thinking About Security

Security is a mindset, and thinking about security requires a different way of thinking. It’s not enough to think like a designer, you have to learn to think like a hacker. In this introductory session, we will explore that way of thinking through a series of security scenarios, most of which having nothing to do with computers, and all of which will foreshadow the technical and policy issues to follow.
Readings: none

1/25: Debating a Security Policy Issue: FBI and iPhone Access

In 2015, the FBI tried to demand that Apple create software that would decrypt an iPhone belonging to dead terrorist Syed Rizwan Farook. This ignited a policy debate about the role of encryption to secure data and communications, and whether technology companies should build in “back door” access mechanisms for the FBI. To start our course off, we will briefly discuss this with the knowledge and opinions we bring to the class.

Required Readings:


1/30: Introduction to Internet Security

It is impossible to discuss any topics related to Internet-security policy without understanding the details of Internet security. In the first of a series of sessions, we will delve into the general technical issues of how security works on the Internet. This will necessarily require us to understand how the Internet works.

Required Readings:

- Singer and Friedman, pp. 12–66 (Part I).

Optional Readings:

2/1: Cryptography

Cryptography is a cornerstone of anything related to Internet security. In this class we'll talk about how cryptography works in both classical pencil-and-paper systems and modern computer systems. Along the way, we will discuss symmetric and public-key encryption, authentication codes, and digital signatures. It is possible to understand how cryptography works without a lot of math, but a little bit helps.

Required Readings:


Optional Readings:


2/6: Access Control, Anonymity, and Attribution

One of the core issues in computer and Internet security is access control. Who has access? How does she get it? How does she prove to the system that she is who she says she is, and should be allowed the claimed access? These are complicated questions, and we will explore them in this session. We will also discuss anonymity and attack attribution, two things that have significant policy implications.

Required Readings:


Bruce Schneier, “Hacker or spy? In today’s cyberattacks, finding the culprit is a troubling puzzle,” Christian Science Monitor, Mar 2015.
http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0304/Hacker-or-spy-In-today-s-cyberattacks-finding-the-culprit-is-a-troubling-puzzle


Optional Readings: none

2/8: Computer and Network Security

Computer networks, especially a ubiquitous global network like the Internet, brings its own security challenges. We will explore this from the inside out: applications software, operating systems, computers,
local networks, and then the Internet. We’ll also talk about software bugs, vulnerabilities, and exploits. And, along the way we will discuss a variety of common network-security technologies: anti-virus programs, firewalls, intrusion detection systems, and so on.

Required Readings:


Optional Readings: none

---

**2/13: Threat Models and Trust Models**

In security, we spend a lot of time trying to model the humans involved in a system. Threat modeling examines who wants to attack the system and their characteristics. Criminals, terrorists, foreign governments, secret police, noisy neighbors and so on have different skills, resources, motivations, risk aversions, and so on. Trust modeling tries to map out who and what needs to be trusted in order for a system to operate. Both are essential for determining if a particular security system is up for the job.

Required Readings:


Optional Readings:


---

**2/15: Confidentiality, Integrity, and Availability: Review**

“Security” is a complex and multi-faceted word, and means different things in different contexts. In this session, we will discuss the traditional “CIA triad,” and see how different security properties are important in different situations and contexts. We will end by reviewing what we’ve learned so far.

Required Readings:


Optional Readings: none

2/22: Taxonomy of Attackers

Building on the previous session, we will examine different types of attackers in detail and their implications for security design. For example, building a system to withstand armed conflict is not the same as building a system that can withstand organized crime. Knowing the attackers is critical to understanding the defense.

Required Readings:

- Singer and Friedman, pp. 67–114.

Optional Readings:


2/27: Security Economics

Internet security is fundamentally about technology, but economic considerations provide a backdrop for understanding what and how different technologies are deployed. Knowing who reaps the benefits and who bears the costs can explain the difference between a successful security technology and a failure.

Required Readings:

Optional Readings:


https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion

http://www.slate.com/articles/technology/future_tense/2014/06/target_breach_cyberinsurance_is_a_mess.html

http://geer.tinho.net/geer.blackhat.6viii14.txt or https://www.youtube.com/watch?v=nT-TGVYO8pl


3/1: Psychology of Security, Security Usability

People have an a natural intuition about security, born out of hundreds of thousands of years of living in risky environments. In this session we will discuss how people think about security and where our cognitive biases fail. We will also discuss another important aspect of security: designing systems so that people actually use them, and use them well.

Required Readings:


https://www.youtube.com/watch?v=lc7scxvKQo


http://discovery.ucl.ac.uk/20247/2/CACM%20FINAL.pdf

http://discovery.ucl.ac.uk/1424472/


Optional Readings:
3/6: DMCA and copyright law—guest lecturer Cory Doctorow

Copyright law is complex and Byzantine, and has completely changed in reaction to the Internet. The Digital Millennium Copyright Act (1996) attempted to modernize copyright, but has also effectively criminalized reverse-engineering. We will discuss how the law is used, and the current battles to repeal it. Our guest for this session is Cory Doctorow, author and longtime copyright activist, currently working on these issues at the Electronic Frontier Foundation.

Required Readings:

http://archive.wired.com/wired/archive/2.03/economy.ideas.html

http://moritzlaw.osu.edu/students/groups/oslj/files/2012/03/63.2.green_.pdf

https://www.engadget.com/2013/04/29/the-itunes-influence-part-one/

https://www.wired.com/2008/10/ten-years-later/


Optional Readings:

http://homepages.law.asu.edu/~dkarjala/OpposingCopyrightExtension/commentary/LessigCreativeCommonsFlaLRev2003.htm


3/8: Regulation and the IoT—guest lecturer Melissa Hathaway

The Internet of Things will bring the Internet into every corner of our life: both sensors that measure our world, and actuators that physically affect this. In this session, we will discuss the security implications of this next phase of computerization, at both the personal and national level. Melissa Hathaway will be our guest speaker. She has done extensive work on this issue in the private sector. Previously, she has had high-profile cybersecurity positions in both the Bush and Obama administrations.

Required Readings:


J.M. Porup, “‘Internet of Things’ security is hilariously broken and getting worse,” Ars Technica, Jan 2016.


Optional Readings:

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

3/20: Topic TBD

I will be amazed if a new policy doesn’t come up during the semester. We’ll use this session to discuss any emerging issues, and return to the previous issues that still have open questions.

Required Readings: TBD
Optional Readings: TBD

3/22: Software liabilities and cybersecurity insurance

One of the proposed remedies for insecure software—and poor quality software in general—is to hold the software vendors liable for the effects of their software. We will discuss the different aspects of this remedy. How viable is it to let a court determine liabilities? What will this do to the software market? What about free and open source software? And if we already live in a world of product liability, do we need a separate liability regime for software? Finally, how does insurance play a role in all this?

Required Readings:


Optional Readings:


3/27: National security and surveillance—guest lecturer Joel Brenner

The role of surveillance in national security will be a repeated theme in this course. To start things off, we will generally look at how surveillance is used for national security purposes. History is important, and we will trace the NSA and other organizations from World War II to the surveillance reforms of the 1970s to
the 9/11 terrorist attacks to today. To assist us in this journey, we will be joined by Joel Brenner. Brenner was the first Inspector General of the NSA, and has been the head of US counterintelligence under the Director of National Intelligence.

Required Readings:

Schneier, pp. 1–87 (Part I).


Optional Readings:


3/29: Data, privacy, and surveillance

Continuing our discussion of data and surveillance, we will talk generally about the technology and business of data collection, analysis and use. This class will largely focus on the technologies we encounter everyday: our smart phones, our computers, our credit cards. Everyone is under pervasive surveillance: not because we asked for it, but because it is a side-effect of our networked technologies.

Required Readings:

Schneier, pp. 90–151 (Part II).

Optional Readings:


**4/3: NSA surveillance oversight—guest lecturer John DeLong**

There are two different kinds of oversight: are you doing things right, and are you doing the right things. The former is compliance, and concerns itself with whether individuals are correctly following the procedures laid out for them. The second is more general, are the procedures the legal, ethical, efficacious, and right ones to follow? For the NSA: the former would be policed by the agency’s internal compliance office, and the latter should be determined by Congress, the President, and the people. Our guest for this session is John DeLong, former Director of Compliance at the NSA.

Required Readings:


Optional Readings: none

---

**4/5: Surveillance reform—guest lecturer Ben Wizner**

While many agree that surveillance needs to be curtailed, the details are far from simple. In this session, we will discuss various possibilities for surveillance reform for both the intelligence community and law enforcement. Our guest for this lecture, Ben Wizner, is the director of the ACLU’s Speech, Privacy, and Technology Project, and attorney to Edward Snowden.

Required Readings:

- Schneier, pp. 155–238 (part III).

Optional Readings:
4/10: Commercial surveillance policy

In the US today, commercial surveillance is largely unregulated. There are exceptions, but in the main the Internet companies you interact with can spy on your every move. And while there is no appetite in Congress to change this, we can both look to Europe to see a different regime. In this session we will talk about potential limits to corporate data collection and use.

Required Readings:

Bruce Schneier, “Data is a toxic asset, why not throw it out?” CNN, Mar 2016.
https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asset.html


https://www.justsecurity.org/28752/keystrokes-solve-crime-press-enter/

http://idlewords.com/talks/internet_with_a_human_face.htm

http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html


Optional Readings:


http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html


“Big Data and Privacy: A Technical Perspective,” President’s Council of Advisors on Science and Technology, May 2014.
https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

https://www.schneier.com/blog/archives/2013/10/the_trajectory.html

---

4/12: Cyberwar

“Cyberwar” has been used to describe everything from the Russian hacks against the DNC to the cyber operations associated with the War in Iraq. In this session, we will explore the various aspects of cyberwar, as well as the military organizations that have emerged to fight in this new battlefield. We may be joined by a former DoD expert in this.

Required Readings:

Singer and Friedman, pp. 114–165.


John Arquilla, Cyber War is Already Upon Us, Foreign Policy, Mar/Apr 2012.
http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

Seymour Hersh, “The Online Threat: Should we be worried about a Cyberwar?” The New Yorker, Nov 2010.


Optional Readings:


https://ccdcoe.org/tallinn-manual.html

https://www.privacyassociation.org/privacy_perspectives/post/the_chinese_hacking_indictments _and_why_economic_espionage_is_different

http://www.lawfareblog.com/2014/05/the-u-s-corporate-theft-principle/


4/17: FBI and “going dark”—guest lecturer Susan Landau

We return to Farook’s iPhone, and the more general question of law-enforcement access to encrypted data and communications. We will discuss whether the ubiquitous use of encryption on computers and phones means that the FBI is “going dark.” Is the solution “back doors” into these devices, or does the FBI have alternative tools at its disposal? We will discuss “lawful hacking” as one such alternative tool. Our guest lecturer for this session is Susan Landau. Landau is a mathematician and engineer who has been working on this issue for decades.

Required Readings:


Optional Readings:


4/19: Special topics in government surveillance

We return to the NSA and government surveillance. Is what they're doing both lawful and necessary for national security, or have they exceeded their legal mandate? We'll look at different proposals to reform the NSA, as well as the role of whistleblowers in the intelligence community.

Required Readings:

Singer and Friedman, pp. 166–246.

Optional Readings: none

4/24: FAA Section 702 reauthorization and reform

The FISA Amendments Act—including Section 702—is up for reauthorization in 2017. In this penultimate session, we'll discuss the section and the issues that will be debated in Congress this year. Alternatively, we will use this session to explore an Internet security issue that has emerged since the class began.

Required Readings:


https://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights

Elizabeth Goitein, Oversight and Reauthorization of the FISA Amendments Act, Senate Committee on the Judiciary, May 2016.
https://www.brennancenter.org/analysis/oversight-and-reauthorization-fisa-amendment-act

Matthew G. Olsen, Oversight and Reauthorization of the FISA Amendments Act, Senate Committee on the Judiciary, May 2016.
https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Olsen%20Testimony.pdf


Optional Readings:


4/26: Final questions, overarching issues, and lessons from the class

In our final class, we'll sum up what we learned and discuss the final exam.
Readings: none

9. Detailed Assignments

All assignments are due at the start of class on the day they are due. Students are to submit assignments two weeks: in Canvas, and by bringing a paper copy to class.

Due 2/6: Brief One

Tell us about your professional background, and recommend the one Internet-security problem the government (US or another government) should work towards solving first. The problem could be important, urgent, solvable or any combination of the three. Length: 500-800 words.

Due 2/27: Brief Two

Explain an Internet-related security problem whose economic considerations prevent it from being solved efficiently. Recommend a policy action to overcome that limitation. Length: 500-800 words.