

PSCI / PPOL 4302
Data and Policy
SPRING 2019

Instructor: Vito D’Orazio

Time and Location: T, Th 2:30-3:45am, CB3 1.312

Contact: dorazio@utdallas.edu 972-883-6212

Office Hours: Wednesday 9:00-11:00am, GR 3.108D

Teaching Assistant: Austin Kingsolver

Contact: akingsolver@utdallas.edu

Office Hours: Tuesday 4:00-6:00, GR 3.314

Course Goals and Overview

Data is collected on all of us, nearly all the time, by many types of actors—government and corporate, domestic and international. Much of this data is just a by-product of our everyday lives, sometimes referred to as our *digital breadcrumbs*. What does this data look like? Who owns it? What are the policies that determine how business and government may acquire and use our data? How does data in the hands of government threaten our privacy? What is our right to privacy to begin with? How does data in the hands of government promote security? How much data are we willing to let the government have? This is the first part of the course, with an emphasis on the individual.

In most places, the stability of the government is not as secure as in the United States. Threats to stability, for example by way of rebellion and protest, are often present or on the horizon. In many places, including the US, terrorist threats are a primary security concern. Destabilization and terrorism often go hand-in-hand. How do governments around the world use data to combat these threats and promote stability? How do governments around the world use data to repress dissent? Many people around the world have legitimate grievances against their government. What is the role of data in making those grievances known? What is its role in electoral processes? This is the second part of the course, with an emphasis on the state and domestic politics.

We have heard of things like cyberwarfare and cyberattacks—but what are these things? Are they really any different from conventional warfare? What incentives do states have to engage in cyberwarfare? In what sense do the actions states take to promote their cybersecurity encourage others to do the same? A century ago, the machine gun proved to be an incredibly valuable defensive weapon. Are cyberattacks an incredibly valuable offensive weapon? What can states do to defend themselves against cyber threats? This is the third part of the course, with an emphasis on international relations.

This course has three major goals: (1) to understand how and why governments and citizens use data to achieve policy objectives; (2) to think critically about the balance between liberty and security; (3) to familiarize students with modern technologies and government programs associated with data collection and use.

These three learning objectives will be assessed throughout the course's homework assignments and the three quizzes. Each of these are writing assignments, and the goal for each student is to demonstrate an analysis and synthesis of course materials.

Course Requirements

You are required to complete a reading assignment before every class, with exceptions noted below. There will be eleven graded homework assignments and three quizzes.

Final Grade Composition

Eleven Homeworks	30% (3% each, 1 bonus)
Three Quizzes	60%
Attendance & Participation	10%

Attendance and participation (10%)

These are the easiest points you can get. Show up, be attentive, and participate to get full credit.

Short homework assignments (30%)

There will be eleven short homework assignments to be submitted through eLearning by midnight **the day before class**. For each assignment (unless otherwise noted): summarize the reading (1-3 sentences), raise two thoughtful questions, and discuss your reaction to the reading (1-2 paragraphs). For example, by midnight of January 24, complete the readings and submit the homework through eLearning.

Note that there are eleven homework assignments, but that you cannot receive more than 30 points toward your final grade. Thus, if you complete all eleven assignments and your scores sum to 31, 32, or 33, you still only receive 30 points toward your final grade.

Quizzes (20% each)

Each quiz is an open book exam. You will be provided with two essay questions, will pick one, and write a *one page* essay on it. Essays should include in-text citations of course readings. If you cite readings that are not required, include their citation in a reference list at the end of your essay. The reference list will not count towards your one page limit. A perfect essay has a clearly stated thesis that is supported with facts and examples using the vocabulary of the class. It demonstrates both analysis and synthesis of course materials. The structure and organization make sense, and include an introduction, conclusion (which may be very short), a thesis, and topic sentences. The writing is clear, precise, and deliberate—grammar and spelling do not need to be perfect, but the writing must be get the point across in an understandable way. The vocabulary that we use in class is incorporated into the arguments. All parts of the question are answered. Finally, to get above a 90, the answer

must be creative. Hypotheticals, counterfactuals, and new applications are some ways to be creative in a response.

Grade Scale

A+	≥ 97%	B	= 83-86%	C-	70-72%
A	= 93-96%	B-	= 80-82%	D	65-69%
A-	= 90-92%	C+	= 77-79%	F	≤ 64%
B+	= 87-89%	C	= 73-76%		

See <http://catalog.utdallas.edu/now/undergraduate/policies/academic> for additional information about university grading policies.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus: <http://go.utdallas.edu/syllabus-policies>.

Required Texts

- Moore, A. and Lloyd, D. (2008). *V for Vendetta*. Vertigo. ISBN: 978-1401208417
- Schneier, B. (2018). *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. Norton. ISBN: 978-0393608885
- Buchanan, B. (2017). *The Cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press. ISBN: 978-0190665012
- Additional readings are available through the library and will be made available online. Students are not required to print materials.

Course Outline

Part I: The Individual and Data

Day 1: Introductions and Syllabus **January 15**

- V for Vendetta: Book 1

Day 2: Extreme Surveillance **January 17**

- V for Vendetta: Books 2 and 3

Day 3: The Right to Privacy I **January 22**

- Warren, S. D. and Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, pages 193–220

- Day 4: The Right to Privacy II** **January 24**
- House, W. (2012). Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. *White House, Washington, DC*, pages 1–62
 - Homework 1
- Day 5: Trends in Connectivity I** **January 29**
- Schneier: Introduction, Ch 1, 2
- Day 6: Trends in Connectivity II** **January 31**
- Schneier: Ch 3, 4, 5
 - Homework 2
- Day 7: Policy Solutions I** **February 5**
- Schneier: Ch 6, 7, 8, 9
- Day 8: Policy Solutions II** **February 7**
- Schneier: Ch 10, 11, 12, Conclusion
 - Homework 3
- Day 9: Section 702 I** **February 12**
- Lawfare Podcast: Episode 230: Matt Olson on the Future of 702
- Day 10: Section 702 II** **February 14**
- Lawfare Podcast: Jim Baker and Carl Ghattas on Section 702
 - Homework 4
- Day 11: Sovereignty and Surveillance** **February 19**
- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., and Walker, R. B. (2014). After snowden: Rethinking the impact of surveillance. *International political sociology*, 8(2):121–144
- Day 12: Quiz 1** **February 21**
- Quiz I covering Part I of the course

Part II: The State and Domestic Data

Day 13: The Zapatista Effect February 26

- Cleaver Jr, H. M. (1998). The zapatista effect: The internet and the rise of an alternative political fabric. *Journal of International Affairs*, pages 621–640

Day 14: Social Media and Protest Mobilization February 28

- Breuer, A., Landman, T., and Farquhar, D. (2015). Social media and protest mobilization: Evidence from the tunisian revolution. *Democratization*, 22(4):764–792
- Homework 5

Day 15: Democracy and Cyberspace March 5

- Diamond, L. (2010). Liberation technology. *Journal of Democracy*, 21(3):69–83

Day 16: Authoritarianism and Cyberspace March 7

- Deibert, R. (2015). Cyberspace under siege. *Journal of Democracy*, 26(3):64–78
- Homework 6

Day 17: Twitter: Iran March 12

- Morozov, E. (2009). Iran: Downside to the” twitter revolution”. *Dissent*, 56(4):10–14

Day 18: China March 14

- King, G., Pan, J., and Roberts, M. E. (2017). How the chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, 111(3):484–501
- Homework 7

Day 19: Internet Blackouts I March 26

- Gohdes, A. R. (2015). Pulling the plug: Network disruptions and violence in civil conflict. *Journal of Peace Research*, 52(3):352–367

Day 20: Internet Blackouts II March 28

- Freyburg, T. and Garbe, L. (2018). Blocking the bottleneck: Internet shutdowns and ownership at election times in sub-saharan africa. *International Journal of Communication*, 12:3896–3916
- Homework 8

Day 21: Quiz 2 **April 2**

- Quiz 2 covering Part II of the course

Part III: State-to-State Data and Cyberwar**Day 22: Cyber Power** **April 4**

- Nye Jr, J. S. (2010). Cyber power. Technical report, Harvard Univ Cambridge MA Belfer Center for Science and International Affairs

Day 23: Security Dilemma and Cyber Offense **April 9**

- Buchanan: Introduction, Ch 1, 2

Day 24: Cyber Defense and Threats **April 11**

- Buchanan: Ch 3, 4
- Homework 9

Day 25: Mitigation and Information **April 16**

- Buchanan: Ch 5, 6

Day 26: Limitations and Solutions **April 18**

- Buchanan: Ch 7, 8, Conclusion
- Homework 10

Day 27: Stuxnet **April 23**

- Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3):365–404

Day 28: Myth of Cyberwar **April 25**

- Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, 38(2):41–73
- ~~Homework 11~~

Day 29: Managing the Cyber Space **April 30**

- Nye, J. S. (2014). The regime complex for managing global cyber activities
- News segment presentations (replacing Homework 11)

Day 30: Quiz 3

May 2

- Quiz 3 covering Part III of the course