**TABLE OF CONTENTS**

INTRODUCTION page 1

PART I: OVERVIEW page 2

Historical and Intellectual Context

Cypherpunk Ethics

The Basic Components of Ethical Theory

Purpose & Structure of the Module

Pedagogical Note

PART II: LESSON A page 6

Assigned Texts

Lesson Steps

Lesson Materials

Lesson Notes

Article Summary and Explanation for Instructors

PART III: LESSON B page 12

Assigned Texts

Lesson Steps

Lesson Materials

Lesson Notes

Article Summary and Explanation for Instructors

PART IV: OTHER LESSON OPTIONS page 17

Other Materials

Online Classes

REFERENCES & RESOURCES page 18

**INTRODUCTION**

This module consists of two lessons. For Lesson A, students learn about cypherpunk ethics by reading three short essays for homework and then discussing them in class. Instructors will lead students in discussing the relationship between privacy, diversity, and the open society and connecting those values to cryptography and system and device security. For Lesson B, students learn about contemporary “security verses security” debates by reading two short Congressional testimonies for homework and then discussing them in class. Instructors will lead students in discussing the relationship individual privacy, national security, and systems/device security while reflecting on the role of cryptography in these ethical debates. The instructor guide provides the necessary background and explanations of the material so that everything the instructor needs to run these modules in a class are contained here, including handouts and PowerPoints. Additional resources can be found referenced throughout the instructor guide with a specific list at the end.

**PART I: OVERVIEW**

*Historical and Intellectual Context*

Over two decades before Edward Snowden blew the whistle on the mass surveillance programs and capabilities of the National Security Agency (NSA), the cypherpunks emerged as a grassroots movement simultaneously criticizing the emerging government mass surveillance made possible by the computer revolution and advocating the widespread use of digital encryption as the best means for individuals to protect their personal privacy from such surveillance. The cypherpunk movement formed at a meeting of cryptography enthusiasts in San Francisco in 1992. The recognized founders of the cypherpunks are Timothy May, a physicist who retired from Intel, John Gilmore, a programmer who retired from Sun Microsystems and later cofounded Electronic Foundation Frontier, and Eric Hughes, who studied cryptography with the famous David Chaum.

As increasingly powerful computers made possible more surveillance and higher capacity data storage, many Americans began to worry that the age of the computer meant the end of privacy. As the US government achieved greater surveillance capabilities, it began to justify mass surveillance and mass databases by appealing to what can be called *the security principle*: the claim that the government has legitimate national security and law enforcement interests in conducting such surveillance and in keeping such databases. In response, many activists asserted what can be called *the privacy principle*: the claim that individuals have a right to privacy and that the government must show compelling, individualized evidence to justify any violation of the right to privacy.

In the decades that followed, this “security versus privacy” debate has persisted. While most parties on both sides of the debate acknowledge that security and privacy are valuable social goods, they disagree about how to balance these values in instances when they seem to conflict. While this debate is often framed as an individual right to privacy pitted against the government’s duty to ensure public safety and criminal justice, the cypherpunks largely reject appeals to an individual right to privacy. Instead, the cypherpunks argue that privacy is a means to preserving an *open* *society*, which means their arguments are not individualistic but grounded in a conception of what kind of society they believe we ought to desire.

More recently, many technologists have attempted to reframe debates about the ethics of encryption as a “security versus security” debate. Unlike the “security versus privacy” framing, which views national security/law enforcement and individual privacy as the two primary values in conflict, the “security versus security” approach argues that the conflict is between national security/law enforcement, on the one hand, and device and systems security, on the other hand. This framing pushes the conversation about the ethics of cryptography beyond the commonplace claim that “in order to have security, we need to give up a little privacy,” showing us that two types of security are implicated in debates about the ethics of cryptography.

*Cypherpunk Ethics*

While the cypherpunk movement is ideologically diverse, there are some shared ideas to be found in the writings of the movement’s founders. First, the cypherpunks argue that the ideal society is an open society, a pluralistic society consisting of diverse religious, ideological, and moral worldviews and governed by mutual toleration (but not necessarily acceptance) among all. Second, they argue that privacy is a necessary condition for an open society because it secures a space where difference and diversity can be expressed and exercised even if the politicians who control the government at any given moment do not like difference and diversity. Third, they argue that technological solutions are preferrable to legislative solutions because laws can be repealed or remain unenforced, while technology is difficult to eliminate once it is publicly available. Finally, they argue that cryptography is the technology that will protect privacy—and by extension, preserve an open society—in the computer age.

The security versus security framing presented by Susan Landau in Lesson B is not, strictly speaking, an example of cypherpunk ethics. However, her academic and public policy work can be viewed as an extension of cypherpunk principles. And given her collaborations with Whitfield Diffie—whose cryptographic research and activist pursuits directly inspired the cypherpunks—her contributions to the ethics of cryptography belong in this discussion.

*The Basic Components of Ethical Theory*

All moral philosophy is built around two concepts: means and ends. The *ends* are the desired outcomes, and the *means* are the ways the outcomes are pursued. Following from these two concepts are the basic questions of ethical theory: *Which means are permissible and why?* and *What ends are desirable and why?* Answers to such questions are normative or prescriptive, in that they take a stance how people *ought* and *ought not* behave.

In the context of computer science and ethics, anyone working on data communications, networking, cybersecurity, or related security areas of computing must ask these two questions. In terms of desirable ends, computer scientists must go beyond the simple “end” of creating a functioning product. Instead, they must as themselves two questions: “What kind of behavior, what kinds of relationships, do I want to promote with the creation and distribution of this product?” and “Why are these behaviors and relationships morally desirable?”

In terms of permissible means, computer scientists must be able to distinguish between morally permissible and morally impermissible means; that is, they must differentiate action that they must never do from actions that they may do.

Cypherpunk ethics are relevant to computer science ethics because they require us to ask fundamental questions about how humans *ought to be*. If computer scientists are creating technologies that affect the overall structure of society, which they do by necessity, then they must ask what kind of society they wish to build and which means are justifiable in building that society. Cypherpunk ethics helps us reflect on these matters.

*Purpose & Structure of the Module*

The purpose of this module on cypherpunk ethics and cryptography is to get students thinking about the ethical dimensions of information technologies and networks. Too often computer scientists focus purely on the functionality of the technologies they create and assess those technologies only in terms of function. For example, if the software or the network “works” as intended, then the product is a success.

The module includes two lessons:

Lesson A requires students to read three short “manifestoes” from the cypherpunk movement as homework (before coming to class) and then provides the instructor with the materials necessary to facilitate an in-class discussion based on the reading. Instructor materials include a PowerPoint slideshow and accompanying notes. This lesson provides the conceptual foundations for understanding cypherpunk ethics, including their use of the concepts “open society” and “privacy.” The full version of this lesson can be completed in a 50- to 75-minute class period.

Lesson B requires students to read two testimonies from Congressional hearings on cryptography and then provides the instructor with the materials necessary to facilitate an in-class discussion based on the reading. Instructor materials include a PowerPoint slideshow and accompanying notes. This lesson provides the conceptual foundations for understanding the difference between the “security versus privacy” and “security versus security” framing of the cryptography debate. The full version of this lesson can be completed in a 50- to 75-minute class period.

The double lesson structure of the module is designed to give instructors flexibility as they incorporate the module into their classes. Lessons A and B can be taught individually or as a pair, depending on the needs and desires of the instructor. Here are a few examples how the lessons can be used individually or in tandem:

* To use the lessons in their fullest forms, instructors would use both Lesson A and B over two class periods. In both class periods, students will come to class having read the assigned essays; in class, the instructor will review the reading using the PowerPoint provided and then either facilitate a discussion as a class or have the students work through questions in breakout groups.
* In one abbreviated form, instructors could use only Lesson A, assigning the cypherpunk readings to students and then discussing them during the following class period.
* In another abbreviated form, instructors could use only Lesson B, assigning the Congressional testimonies to students and then discussing them during the following class period.
* In another abbreviated form, instructors could use both Lesson A and B in a single class period. This approach would require assigning all five short readings for homework and then discussing them all, either in breakout groups or as a class.

*Pedagogical Note*

Some instructors may be new to teaching and discussing ethics in their computer science courses, and for that reason, some instructors may feel underprepared or even uncomfortable with their level of experience in conducting ethical analysis. But it is important to remember that, when teaching ethics, instructors are not expected to have the right answers but are rather expected to pose the right questions. Thus, the best approach for this material is the Socratic method, which emphases asking questions over providing answers. Importantly, because ethical problems are open-ended problems, the questions asked should be open-ended. The lessons in this module are not designed to help students or faculty come to definitive answers about the ethics of cryptography, privacy, and security. Instead, the lessons are designed to provide students with the opportunity to think through their own views and, most importantly, provide reasons for their views.

Instructors should not feel obligated to settle any moral issues in one or two class periods. Instead, instructors should view the modules as an opportunity to initiate and practice ethical reasoning with students. One challenge of the Socratic method is that there are no obvious or objective right answers. Another challenge is the diversity of answers that the instructor will get from students. A third challenge is that the instructor must momentarily set aside their usual position as a content expert and focus instead on being the person with questions rather than answers. (See the resources at the end for a helpful guide to Socratic teaching.)

It should also be noted that, where possible, the reading and discussion questions have been constructed using Bloom’s taxonomy (the revised 2001 terminology is used here). The reading questions consist of “lower order” questions designed to help students *Remember* (Level 1) and *Understand* (Level 2) the ideas in the assigned readings. The discussion questions consist of “higher order” questions designed to help students *Apply* (Level 3), *Analyze* (Level 4), *Evaluate* (Level 5), and *Create* (Level 6). (See the resources at the end for a helpful guide to Bloom’s taxonomy.) These lists of questions are not exhaustive, so instructors are encouraged to add or modify questions as they see fit.

**PART II: LESSON A**

*Assigned Texts*

Gilmore, J. (1991, March 28). Privacy, technology, and the open society. First Conference on Computers, Freedom, and Privacy, Computer Professionals for Social Responsibility, Burlingame, CA. [[Accessible here](https://archive.md/yF4Z3).]

Hughes, E. (1993, March 9). A cypherpunk’s manifesto. [[Accessible here](https://www.activism.net/cypherpunk/manifesto.html).]

May, T. C. (1992, November 22). A crypto anarchist manifesto. [[Accessible here](https://www.activism.net/cypherpunk/crypto-anarchy.html).]

*Lesson Steps*

1. In advice of the designated class period, provide students with the assigned texts and ask them to read them as homework before coming to class. Students may be provided the reading questions in the Lesson A Student Handout to help them identify the most important ideas in the text. Instructors may choose to require students to submit answers to the reading questions. Remember that no student will master the ideas in the text on a first read, so this reading assignment is just a primer. The reading should take students approximately 30 minutes to complete outside class.
2. In class, before discussing the readings, prompt the students to think and discuss the basic components of ethical theory, using the concepts on the handout and/or PowerPoint (though instructors need not use the slides in class). This step helps students begin thinking about right and wrong, good and bad, before jumping into cypherpunk ethics. This step should take approximately 20 minutes.
3. In class, place students into breakout groups of 3 or 4. Ask them to collaborate, working together to respond to the discussion questions. Students do not need to come to a consensus, though they may. They should have remarks prepared when returning to full group discussion. It can help to provide students with a printed copy of the discussion questions. This step should take approximately 10-15 minutes.
4. Once student groups have completed their breakout discussions, ask student groups to share their ideas with the class, providing reasons for their conclusions. Instructors should write all student answers on the board in a table (or similarly record student contributions to keep track of the discussion). In small classes, it is possible to hear from every group. In larger classes, the instructor may take volunteers or call on groups randomly. This step should take approximately 20-30 minutes.

*Lesson Materials*

|  |
| --- |
| **Reading Questions** |
| These questions can be provided to students to help them *Remember* (Level 1) and *Understand* (Level 2) the texts as they do the readings:   1. According to Gilmore, what is the relation between privacy and an open society? 2. Why does Gilmore advocate the use of “physics and mathematics” to preserve privacy rather than “laws”? 3. How does Hughes define “privacy”? 4. Given the way Hughes connects privacy and cryptography, how does he seem to understand the *moral* meaning of cryptography? Identify at least one example. 5. What does May mean when he argues that cryptography might create the conditions for “abhorrent markets”? Why or why not? 6. What does May mean when he says that cryptography creates so much openness that it will “alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation”? |

|  |
| --- |
| **Discussion Questions** |
| These questions are posed to students to help them *Apply* (Level 3), *Analyze* (Level 4), *Evaluate* (Level 5), and *Create* (Level 6) in response to the readings:   1. Is the definition of privacy offered by Gilmore and Hughes satisfactory? Why or why not? If it is not satisfactory, what would be a better definition and why? 2. Gilmore argues that an open society is defined by its level of tolerance for difference, but no society can tolerate *everything*. There must be some line separating what a society will tolerate and what it will not tolerate. What are the limits to toleration? In other words, how to we differentiate things we should tolerate and things we should not tolerate? 3. To what extent is May correct when he says that cryptography creates so much openness that it will “alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation”? Does cryptography actually undermine current social relations? 4. To what extent is the cypherpunk emphasis on technical solutions to moral problems over legislative solutions to moral problems relevant to computer scientists and why? 5. Are the cypherpunks right about the relationship between privacy, tolerance, and an open society? Why or why not? 6. What role, if any, do computer scientists play in promoting the realization of an open society? What are the computer scientist’s ethical obligations in such a role and why? |

*Lesson Notes*

Given the way that each of our three authors present their arguments, it is helpful for students to read them in a specific order: Gilmore, Hughes, May. Gilmore sets the stage by introducing the central terms. Hughes elaborates on the notion of privacy and connects it to cryptography more explicitly. And May pushed the conversation the farthest, acknowledging that the liberty of an open society necessarily entails people being able to do morally undesirable things.

Politically and ethically speaking, this order also moves the students from the most moderate position to the most radical. Gilmore is a staunch civil libertarian, while May is an avowed anarchist. Hughes falls somewhere in the middle. By moving from Gilmore to Hughes to May, instructors can lead student from the most to least palatable arguments (from the perspective of most audiences), thus easing them into the most extreme implications of cypherpunk ethics. Discussing May last also sets up the topic in Lesson B, providing for a smooth transition.

The point of the lesson here is twofold. First, students will have to consider the connections between an open society, privacy, and computer technology. The cypherpunks see encryption as enabling a desirable kind of society, which means that encryption is not, in their view, a value-neutral technology. Second, students will have to consider where to draw the line on diversity and toleration. Certainly not all ideas and activities can be tolerated, even in a very tolerant society. Even if we all agree that toleration is morally desirable, we might strongly disagree about where to draw the line on certain beliefs and actions.

One of the key terms in this module and in the cypherpunk texts is “privacy.” To understand the cypherpunk arguments about privacy it is necessary to recognize the difference between law and ethics. Law consists of the rules created and enforced by governments, while ethics consists of broader value frameworks that can either inspire or critique the law. For the sake of this lesson, discussions of privacy should stay within the moral sphere, leaving the legal sphere aside unless discussing the legal aspects of privacy help to illuminate some moral claim or value. The cypherpunks provide a definition of “privacy” in the readings, though this definition can and should be examined and questioned in class discussion.

Another key term in this module and in the cypherpunk texts is “toleration” or “tolerance.” The notion of toleration is deeply connected to the notions of “pluralism” and “diversity.” A society that is diverse or pluralistic is one that has many different religious, ideological, subcultural, linguistic, and/or racial/ethnic groups and individuals living together. Toleration describes the extent to which these various groups and identities can cohabitate in the same civic space (such as a nation-state) without resorting to violence or coercion to settle any disagreements or conflicts that arise. Being tolerant does not mean that one accepts the views of others, but it means they accept the fact that others disagree and accept the fact that disagreements are not to be handled with harassment, intimidation, or violence. As Gilmore and Hughes suggest, the more toleration there is, the more open the society is.

A third key term in this module and in the cypherpunk texts is “open society.” The term was coined by French philosopher Henri Bergson (1935) in *The Two Sources of Morality and Religion*, and Bergson conceived of an open society primarily in religious terms. His idea is similar to our contemporary notion of religious toleration, a practice in which people of various faiths live together in a single society because they acknowledge that no one individual or group has a monopoly—or more accurately, an unquestionable certainly—on spiritual matters and because they prioritize dialogue over force.

The concept of an open society was made famous, however, by Karl Popper’s (1950) now-classic text *The Open Society and Its Enemies*. Whereas Bergson offered a religious conception of the open society, Popper’s conception was more broadly epistemological, meaning that he was interested in intellectual or ideological pluralism and diversity. In Popper’s view, no individual or group had a monopoly (or unquestionable certainly) on any matters of knowledge, which means that knowledge must be constructed using the scientific method. All truth claims would be treated as hypotheses and subject to testing and verification. So Popper’s understanding of science and his advocacy of an open society went hand-in-hand.

In his introduction to *Rethinking Open Society: New Adversaries and New Opportunities*, Michael Ignatieff provides a short, effective summary of Popper’s open society:

One critical aspect of open society thinking was the connection that Popper drew between the epistemology of a free society and its morality of tolerance. As a philosopher and a historian of science, Popper believed that the key practice that keeps a society free is the scientific method, the constant falsification of theory through systematic reality testing. His attack on totalizing political ideologies derived from this epistemological and also moral conviction that all theory is conditional, provisional, and must give way when falsified by the facts. Few elements of his thinking remain more relevant to a university’s mission than this.

From that epistemology Popper developed an ethic of tolerance. If all theory was conditional upon falsification, no one was in sole or exclusive possession of the truth. If we know we can be wrong, it pays to listen to others, to tolerate, even welcome views that diverge from whatever theory or political or moral values we happen to hold. Since our relationship to facts is or ought to be an individual relationship, dependent upon our free minds alone, we have an obligation to get reality, our conception of it, right for us.

Constitutional liberalism entrenches this epistemology within its very institutions. Power checks power, so no single source can impose an ideology from the top or even sometimes a clear political direction. Parliamentary democracy forces executive authority to justify its measures before the adversarial scrutiny of a parliament. Judges bring the critical epistemology of law to the review of administrative and legal decisions. A free media referees the battle over public choice with a complex epistemology of scrutiny, driven by skepticism, scandal mongering, and profit seeking. Universities play their role in subjecting public claims to peer-reviewed research. These institutions—courts, parliaments, media, universities—together, and without concertation or top-down direction, create the epistemological frame in which a free society struggles its way towards the knowledge it needs, or the closure on debate it must accept, in order to chart its collective course into the future. This is how an open society actually operates, and it is a messy, confusing, and often unsatisfying process that produces recurrent nostalgia for rule by experts or charismatic leaders or both. (Ignatieff & Roch, 2018, p. 6-7)

*Article Summary and Explanation for Instructors*

*John Gilmore*—Gilmore begins by positing a connection between “privacy” and an “open society.” He does not give explicit definitions for either of these terms, but their definitions can be inferred from his argument. For Gilmore, privacy seems to be defined by the ability of the individual to exert control over information about themselves, including his or her name, personal records, financial transactions, and other means of identification. He suggests that the ability to choose anonymity is part of the exercise of privacy. On the other hand, open society seems to be defined by two things: (a) increased levels of toleration for difference and disagreement and (b) increased levels of privacy for individuals. This conception implies that most forms of surveillance and database construction are incompatible with an open society.

In ethical terms, Gilmore’s end is an open society and the means he identifies is privacy. As he writes, “Privacy is a means; what is the real end that we are looking for here? I submit that what we’re looking for *increased tolerance*.” In Gilmore’s view, the more tolerance a society has the more open it is.

Gilmore maintains that privacy is relevant to computer science because “Our computers are extensions of our minds,” arguing that “We should build them so that a thought written in the computer is as private as that thought held in our minds.” He rejects the use of “fake protections,” such as laws, and advocates the use of “real protections,” or cryptography. As Gilmore writes, “I want a guarantee—with physics and mathematics, not with laws—that we can give ourselves things like real privacy of personal communications. Encryption strong enough that even the NSA can’t break it.” Thus, Gilmore makes the classic cypherpunk argument that advocates technological solutions over legislative solutions.

\*\*\*\*\*

*Eric Hughes*—Hughes does more than Gilmore to explicitly define privacy and connect it to cryptography. Hughes is clear that, in his view, secrecy and privacy are two different things. As he writes, “Privacy is not secrecy. A private matter is something one doesn’t want the whole world to know, but a secret matter is something one doesn’t want anybody to know. Privacy is the power to selectively reveal oneself to the world.” In this last sentence, Hughes defines privacy in a way that is similar to Gilmore.

Hughes agrees with Gilmore that “Privacy is necessary for an open society in the electronic age.” However, Hughes does less than Gilmore to define the term “open society.” Instead, he emphasizes the fact that network protocols reveal identities by default, and he therefore concludes that encryption is the only way to ensure privacy. This is why he writes, “When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.” In other words, digital communication systems are antithetical to privacy unless they are equipped with encryption.

It is important to note that Hughes is not content to make a theoretical argument about privacy and the open society. Instead, he states that cypherpunks will create and share cryptographic tools because the way we ensure an open society is to take action—in this case, the action is coding. “Cypherpunks write code,” he observes. “We know that someone has to write software to defend privacy, and since we can’t get privacy unless we all do, we’re going to write it.” He says that governments and corporations have an interest in imposing on privacy, which means they will not build the means to privacy. Thus, cypherpunks must. (To be sure, Hughes writes these words in 1993, before cryptography was a commercially established product to the degree it is today.)

\*\*\*\*\*

*Timothy May*—More than the other cypherpunks, May celebrates what he sees as the anarchistic tendencies of encryption. Whereas Gilmore and Hughes argue that cryptography preserves an open society, May claims that cryptography undermines the power of government to the point where government may have difficulty functioning. Citing the developments in cryptography in the 1980s, May concludes that “These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.”

May anticipates that governments will perceive cryptography as a threat and thus try to prevent cryptography from being widely available. Instead, May notes that governments will appeal to *the security principle*, arguing that the widespread use of encryption will impede law enforcement and national security programs. As he says, “The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration.”

Interestingly, while Gilmore and Hughes say that encryption will preserve society, May is willing to grant that government fears are valid: “Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion.” Thus, May is willing to push—and to celebrate—openness in the anarchistic extreme. Cryptography, in his view, will promote liberty more than any other current technology, and while such liberty will enable some people to do morally reprehensible things, the exercise of liberty is a good that outweighs those morally reprehensible things.

**PART III: LESSON B**

*Assigned Texts*

*The Encryption Tightrope: Balancing Americans’ Security and Privacy*, 114th Congress. (2016, March 1) (testimony of S. Landau before the Senate Judiciary Committee). [[Accessible here](https://docs.house.gov/meetings/JU/JU00/20160301/104573/HHRG-114-JU00-Wstate-LandauS-20160301.pdf).]

*Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*, 114th Congress. (2015, July 8) (testimony of J. B. Comey & S. Q. Yates before the Senate Judiciary Committee). [[Accessible here](https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy).]

*Lesson Steps*

1. In advice of the designated class period, provide students with the assigned texts and ask them to read them as homework before coming to class. Students may be provided the reading questions in the Lesson B Student Handout to help them identify the most important ideas in the text. Instructors may choose to require students to submit answers to the reading questions. Remember that no student will master the ideas in the text on a first read, so this reading assignment is just a primer. The reading should take students approximately 30-45 minutes to complete outside class.
2. In class, before discussing the readings, prompt the students to think and discuss the basic components of ethical theory, using the concepts on the handout and/or PowerPoint (though instructors need not use the slides in class). This step helps students begin thinking about right and wrong, good and bad, before jumping into cypherpunk ethics. This step should take approximately 20 minutes.
3. In class, place students into breakout groups of 3 or 4. Ask them to collaborate, working together to respond to the discussion questions. Students do not need to come to a consensus, though they may. They should have remarks prepared when returning to full group discussion. It can help to provide students with a printed copy of the discussion questions. This step should take approximately 10-15 minutes.
4. Once student groups have completed their breakout discussions, ask student groups to share their ideas with the class, providing reasons for their conclusions. Instructors should write all student answers on the board in a table (or similarly record student contributions to keep track of the discussion). In small classes, it is possible to hear from every group. In larger classes, the instructor may take volunteers or call on groups randomly. This step should take approximately 20-30 minutes.

*Lesson Materials*

|  |
| --- |
| **Reading Questions** |
| These questions can be provided to students to help them *Remember* (Level 1) and *Understand* (Level 2) the texts as they do the readings:   1. What does Comey mean when he claims that the FBI is “going dark”? What seems to be the central moral problem that arises from “going dark” and why? 2. According to Comey, what role does cryptography play in the “going dark” problem? 3. What does Landau mean when she claims that the central issue is not a conflict between security and privacy but a conflict between security and security? What seems to be the central moral problem that arises from this “security versus security story” and why? 4. According to Landau, what role does cryptography play in the “security versus security story”? |

|  |
| --- |
| **Discussion Questions** |
| These questions are posed to students to help them *Apply* (Level 3), *Analyze* (Level 4), *Evaluate* (Level 5), and *Create* (Level 6) in response to the readings:   1. In your view, which framing of the issue—Comey’s “privacy versus security” or Landau’s “security versus security”—is more convincing or insightful? Why? 2. How do computer scientists determine the ethical limitations of their technical contributions to law enforcement and national security agencies? In other words, what principle or principles can computer scientists use to decide when to accept or reject law enforcement and national security requests for technical assistance? 3. Based on what you know, what seems to be the most ethically sound solution to the law enforcement and national security problems the FBI claims to be facing and why? What would computer scientists have to do to help put this solution into practice? |

*Lesson Notes*

The main ethical issue prompted by the debate between Comey and Landau is whether questions about cryptography should be framed as “security versus privacy” or “security versus security.” Importantly, this distinction is important not merely from a technical perspective but also from an ethical perspective because it forces us to answer two questions: “What do we value?” and “How do we rank those values and why?” Comey attempts to frame the issue as a balance between the two values of privacy and security, but when Landau introduces a third value, device and systems security, the debate changes.

If Lesson B is being used as a follow up to Lesson A, then it is helpful to consider how various ideas from both lessons connect to each other. John Gilmore introduces the distinction between “laws of man” (legislation) and the “laws of nature” (cryptography) and states his preference for using the latter to promote an open society where privacy is respected. Timothy May notes that this shift does more than promote and open society; it ultimately means that government agencies will have more difficulty functioning. James Comey agrees with May, but as a leader of a government agency (FBI), Comey expresses concern about the ability of cryptography to circumvent law enforcement procedures. Landau responds to Comey by noting that privacy is not necessarily the central issue. The real question, she says along with the cypherpunks, is “what kind of society do we want to have?” In Landau’s view, we do not want a society with weakly protected and secured digital systems. However, this means that Landau rejects May’s thesis that cryptography will undermine government functions; she simply concludes that law enforcement will have to modify its approach.

An alternative version of this lesson can be arranged in which students read only Landau and the instructor explains Comey’s argument, Landau is reacting to, briefly in class. Comey’s argument is so commonplace and intuitive that most students will understand his position following a short explanation of his thesis. Landau’s argument is more sophisticated and nuanced, therefore requiring deeper engagement.

*Article Summary and Explanation for Instructors*

*James Comey*—Comey presents the official FBI argument about encryption and national security/law enforcement, and as the title suggests, he frames the argument in the classic “security versus privacy” set up. This framing is illustrated by his statement that “We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public.” The problem, according to Comey, is that the FBI is “going dark,” that its agents are unable to gather the evidence necessary for prosecuting and convicting criminals because of encryption.

The apparent dilemma for law enforcement emerged from the technological changes over the past few decades. In the 1970s, most people kept their files in filing cabinets, and even if those cabinets had locks on the drawers, law enforcement could, after obtaining a warrant from an independent judge, either find the keys (perhaps in a desk drawer or on a key ring) or physically break the lock (perhaps with a crowbar). In the twenty-first century, most people keep their documents digitally, on a device of some kind. If a device is encrypted, then there is almost no way to find the key or physically “break” the lock (ex: a brute force attack) without risking the loss of the data.

Recalling John Gilmore’s cypherpunk demand that personal data be protected with “the laws of nature” rather than “the laws of man,” we can better understand Comey’s concern. Assuming an ideal situation in which the FBI or other law enforcement have followed all the legal and moral requirements (the laws of man, which Comey calls “court authorized investigative tools”) for obtaining someone’s data, encryption (the laws of nature) might prevent them from executing the warrant.

Thus, Comey asks: How can law enforcement do its job when individuals can use math to prevent the state from carrying out legitimate law enforcement functions?

Comey goes out of his way to make the point that the FBI is not asking for unconstitutional means of accessing data; instead, the FBI is asking how they can access encrypted data once all the legal and Constitutional requirements for seizing data have been met. Thus, Comey says, “We are not asking to expand the government’s surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.” For Comey, the core question is this: “Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?”

In the end, Timothy May’s anarchistic understanding of encryption becomes relevant, for May understands that encryption entails the very problem Comey is worried about. The difference is that Comey believes US law enforcement to be legitimate, while May remains skeptical about and critical of centralized government power. In other words, May and Comey agree that cryptography will impede law enforcement activities (and other government functions), but they disagree about whether this is a good thing or not.

\*\*\*\*\*

*Susan Landau*—Landau rejects Comey’s argument, starting with his “security versus privacy” framing. As she states, “this is not a simple story of national security versus privacy. It is, in fact, a security versus security story.” The two types of security she refers to are “national security” (which includes law enforcement) and “system and device security,” which are made possible by strong cryptography. She accuses Comey and the FBI of remaining trapped in twentieth century thinking and urges them to rethink law enforcement approaches to encryption.

Her main concern is the FBI’s demand that tech companies like Apple create a modified operating system that can be installed on smart phones of interest so the FBI can conduct brute force attacks without causing the phone to erase all its data. In her ethical analysis, Landau notes that this approach has benefits and drawbacks. “In weighing the FBI request,” she says, “one has to look at the potential gain and weigh it against the potential cost.” The potential gain is to collect data for prosecutions. (This is a generalized interpretation. She is specifically talking about the 2015 San Bernardino shooting.)

Despite this potential gain, Landau takes a “security versus security” approach to identifying the costs, which she documents at length. She notes that the Department of Defense has identified the theft of US intellectual property (she calls it the “cyberexploitation of US companies”) as a serious national security risk. She also notes that many people now use their personal smartphones for work, which means that proprietary data is now on millions of personally owned devices. Only strong encryption, she says, can ensure that all of this proprietary data—on both business owned and personally owned devices—is kept secure.

If the FBI’s proposal is carried out, Landau concludes, the result would be an undermining of our system and device security practices. And once people realize that, for example, Apple can and does install updates that allow law enforcement—and anyone else, for that matter—to attack their devices, people would lose trust in the tech companies and refuse to install updates that patch security flaws. As she asks: “How many people would stop automatic smartphone updates from Apple if they knew that the update could steal their bank account information? How many people would stop using virus scanners on their PCs if they knew that these programs were sometimes used by law enforcement to spy on their users? If this activity were to cause people to back away from using automatic updates for patching and the like, the impact on security is likely to be disastrous.”

Thus, Landau’s argument cleverly pivots always from the “security versus privacy” framing and appeals directly to the people who already believe security is the more important value. As she demonstrates, device and system security are *part of* national security, and those who think national security is the prevailing value in the encryption debate should want to reject the FBI’s proposals.

In the end, Landau explains that the FBI is not actually “going dark” because it is very rare that the FBI’s inability to access data on an encrypted device prevents them from prosecuting and convicting criminals. She observes that the FBI has been successful at collecting necessary evidence using other means, and she argues that the FBI needs better technology staffing and training to deal with law enforcements needs in the twenty-first century.

**PART IV: OTHER LESSON OPTIONS**

*Other Materials*

Instructors who wish to further explore the ethics of cryptography can refer to resources provided by the Markkula Center for Applied Ethics at Santa Clara University. Their “[Ethical Questions About Encryption](https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/ethical-questions-about-encryption/)” provides a list of the ways in which different types of moral theory would ask questions about balancing privacy and security. Likewise, their “[Apple vs. FBI Case Study](https://www.scu.edu/ethics/focus-areas/business-ethics/resources/apple-vs-fbi-case-study/)” poses some questions specifically about the San Bernardino shooter’s phone. Thus, both of these resources would complement Lesson B.

*Online Classes*

*Synchronous*: In synchronous online classes, instructors can implement the modules almost as designed with the right tools. Class discussions and breakout groups can be conducted over Zoom, with the instructor using the groups setting to simulate breakout sessions and using the screenshare setting to simulate a whiteboard where students contributions are displayed.

*Asynchronous*: In asynchronous online classes, instructors can modify the lessons and adapt them to be either homework assignments or discussion board topics. For example, both Lesson A and B could consist of:

* A discussion board for the reading questions
* A short lecture video using the PowerPoint slideshow provided
* A discussion board and/or a group assignment for the discussion questions

**PART REFERENCES AND FURTHER READING**

*References*

Bergson, H. (1935). *The two sources of morality and religion.* (R. Ashley Audra & C. Brereton, Trans.) Garden City, NY: Doubleday & Company.

*Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*, 114th Congress. (2015, July 8) (testimony of J. B. Comey & S. Q. Yates before the Senate Judiciary Committee). https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy

Gilmore, J. (1991, March 28). Privacy, technology, and the open society. First Conference on Computers, Freedom, and Privacy, Computer Professionals for Social Responsibility, Burlingame, CA. https://archive.md/yF4Z3

Hughes, E. (1993, March 9). A cypherpunk’s manifesto. https://www.activism.net/cypherpunk/manifesto.html

Ignatieff, M, & Roch, S. (2018). *Rethinking open society: New adversaries and new opportunities*. Baltimore: Central European University Press.

*The Encryption Tightrope: Balancing Americans’ Security and Privacy*, 114th Congress. (2016, March 1) (testimony of S. Landau before the Senate Judiciary Committee). https://docs.house.gov/meetings/JU/JU00/20160301/104573/HHRG-114-JU00-Wstate-LandauS-20160301.pdf

May, T. C. (1992, November 22). A crypto anarchist manifesto. https://www.activism.net/cypherpunk/crypto-anarchy.html

Popper, K. R. (1950). *The open society and its enemies*. Princeton: Princeton University Press.

Raicu, I. (2016, Jan 1). *Ethical Questions About Encryption*. Markkula Center for Applied Ethics at Santa Clara University. https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/ethical-questions-about-encryption/

Skeet, A,. & Markkula Center Staff. (2016, Dec 2). *Apple vs. FBI case study*. Markkula Center for Applied Ethics at Santa Clara University. https://www.scu.edu/ethics/focus-areas/business-ethics/resources/apple-vs-fbi-case-study/

*Resources*

Anderson, P. (2020). Privacy for the weak, transparency for the powerful: The cypherpunk ethics of Julian Assange. *Ethics and Information Technology*. Published Online.

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the future of the internet*. New York: OR Books.

DeCew, J. (2018) Privacy. In E. N. Zalta (ed.), *Stanford Encyclopedia of Philosophy* (Spring 2018). Stanford University. https://plato.stanford.edu/entries/privacy/

Greenberg, A. (2012). *This machine kills secrets: How WikiLeakers, cypherpunks, and hacktivists aim to free the world’s information*. New York: Dutton.

Landau, S, & Diffie, W. (2007). *Privacy on the line: The politics of wiretapping and encryption, updated and expanded edition*. Cambridge: The MIT Press.

Levy, S. (2001). *Crypto: How the code rebels beat the government—saving privacy in the digital age*. New York: Penguin.

Sloan, R. H., & Warner, R. (2015). The harm in merely knowing: Privacy, complicity, surveillance, and the self. *Journal of Internet Law* *19*(1), 3-14.

*The Socratic Method: What it is and How to Use it in the Classroom*. (n.d.). Stanford: Tomorrow’s Professor Postings. Retrieved Jan 28, 2021, from https://tomprof.stanford.edu/posting/810

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2020). Privacy and information technology. In E. N. Zalta (ed.), *Stanford Encyclopedia of Philosophy* (Summer 2020). Stanford University. https://plato.stanford.edu/entries/it-privacy/

*What is Bloom’s Taxonomy?* (n.d.). Bloom’s Taxonomy. Retrieved Jan 28, 2021, from https://www.bloomstaxonomy.net/