Online privacy: FBI vs. Apple Socratic Seminar

Our Socratic Seminar Rules:

- Respect everyone and their opinion, address each other by your name and politely.
- No sarcasm or put-downs allowed.
- Listen well before speaking and consider others' viewpoints and ideas.
- Don't raise your hand, but wait for a person to finish before speaking yourself.
- If you do not understand something, ask for clarity or explanation.
- Address any disagreement in a courteous way: question the statements and explain your differing view.
- Everyone should have a chance to speak at least once. Invite others to speak.

+ **We will all sit in a circle facing each other.**

Any other you suggest we add??

First Paper Survey…

WARNING FIVE YEAR OLD INFORMATION, still relevant

How Apple tracks your location without consent, and why it matters

A log file on your 3G-enabled iPhone or iPad shows nearly every place you've been
by Jacqui Cheng - **Apr 20, 2011** 12:55pm PDT
http://arstechnica.com/apple/2011/04/how-apple-tracks-your-location-without-your-consent-and-why-it-matters/

It was “discovered that the iPhone or 3G iPad—anything with 3G data access … are logging location data to a file called consolidated.db with latitude and longitude coordinates and a timestamp.”

“Of course, the fact that this data exists somewhere is nothing new. Cell companies have been tracking this triangulation information for their own purposes for years. In the US, however, regular people cannot access that data—law enforcement must obtain a court order before they can get it for an investigation, and your jealous spouse can't get it from the wireless company at all.”

"Anyone with a good jailbreaking tool could get it off the phone too. And of course my forensics tools," iPhone hacker and forensics expert Jonathan Zdziarski told Ars. "In fact even the old SSH worms … could be modified to collect this. It's part of the Core Location cache on the phone.

Q: What other information/data do you think may be stored in your mobile phone that you don’t realize?

Fighting Crime with Mobile Technology

http://source.southuniversity.edu/fighting-crime-with-mobile-technology-137309.aspx

“Mobile technology has become a powerful crime-fighting tool.

“Cell phones contain call history, contacts, text messages, web browser history, email, a Global Positioning System (GPS), and other location information that police and law enforcement agencies find valuable. Evidence from cell phones can help investigators piece together motives and events and provide new leads.

“’Smartphones and cell phones have become a regular part of criminal investigations because they are now owned by most people and provide information about a person’s whereabouts and a person’s contacts,’ says Adam Pincus, a Legal instructor at South University, Online Programs. ‘This helps to jumpstart a criminal investigation.’

“Digital forensics is a branch of science encompassing the recovery and investigation of material found in digital devices, including computers, cell phones, and digital cameras.”
…
“Identity theft, stalking, fraud, …illegal electronic surveillance, and theft of intellectual property are just some of the examples of crimes committed every day on mobile devices.”

Thoughts? Anyone interested in this as a career?

What do you know about the case between Apple and the FBI from earlier this year??

Enable Erase Data option to delete data after 10 failed passcode attempts

http://ioshacker.com/how-to/enable-erase-data-option-delete-data-10-failed-passcode-attempts

“By enabling ‘Erase Data’ option you can make your iPhone, iPad or iPod touch erase all the data stored in it when 10 failed passcode attempts have been made. This means the device will not only get disabled at a certain point but it will also delete your private data to ensure it doesn’t get into the wrong hands.”

Reference – Other gunfire recently, and closer to Seattle!

Oregon standoff spokesman Robert 'LaVoy' Finicum killed, Bundys in custody after shooting near Burns

By Les Zaitz | The Oregonian/OregonLive
on January 26, 2016 at 6:50 PM, updated February 22, 2016 at 2:56 PM
http://www.oregonlive.com/oregon-standoff/2016/01/bundys_in_custody_one_militant.html

Standoff at Malheur National Wildlife Refuge occupation in January earlier this year as well.
“In the meantime, Operation Mutual Defense, a network of militias and patriot sympathizers, issued a call on its website for help at the refuge. The post was written by Gary Hunt, a board member from California who has expressed support for Timothy McVeigh, who bombed a federal building in Oklahoma City and had ties to the patriot movement.”

Confused about Apple and the FBI? What you need to know

By Anita Balakrishnan
Thursday, **18 Feb 2016** | 2:55 PM ET
[http://www.cnbc.com/2016/02/18/confused-about-apple-and-the-fbi-what-you-need-to-know.html]

The FBI is in the midst of investigating a married couple who killed 14 people in a mass shooting in San Bernardino, California, in December.”
…
“Messages on shooter’s… iPhone may, or may not, shed light on their terrorist ties. But the phone is locked by a pass code, and by default, these phones are programmed to erase data after too many unsuccessful unlocking attempts. The FBI didn't want to risk trying to hack the phone and losing all the data in the process.

“A federal magistrate ruled Tuesday that Apple must create this highly specialized software within a certain time frame. But Apple CEO Tim Cook released a letter saying he would challenge the FBI's demands.”

Here's what Apple says:

1. Apple doesn't currently have access to individuals' iPhone data.Encryption — where algorithms scramble communications into a unique code language used to transmit electronic data — protects photos, music, notes, financial information, locations and health data from hackers. **Apple is "deeply committed" to safeguarding customer data, so much so that the company itself doesn't have access to your iPhone's contents.** In other words, Apple argues it doesn't keep "keys" to your phone lock.
2. Apple would have to build a new version of iOS to meet this demand. Apple has complied with subpoenas and search warrants and provided engineers to help the FBI. **But this request requires a new type of tool that Apple doesn't already have: a so-called back door.**
3. There's no way to limit that new version to a single phone. Cook makes an argument that if a less-secure version of the iPhone is built, there is no way to guarantee that the government can limit it to just one phone. "Once created, the technique could be used over and over again, on any number of devices," Cook writes. **"In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks."**

Comments or thoughts??

Here's what the FBI says

1. **The government lawfully seized this phone**.

The phone was known to be used by a mass murderer, was obtained with a search warrant and the phone owners' consent. This is simply a way to execute the original intent of that warrant. The phone is owned by … the San Bernardino County Department of Public Health. The department has supported federal investigators' requests to search the contents of the device.

2. Other digital searches have given hints that the pair were communicating online with terrorists.

Searches of the pair's iCloud account indicates that the shooter was in contact with the victims prior to the shooting, and had posted allegiance … on Facebook. But <the murder> **stopped backing up to the cloud in late October, leaving the final month of the conversations accessible only on the phone itself.**

3. Apple frequently updates their security features.

The needed change should be well within the company's technical capabilities, given that Apple routinely patches or updates iOS to address security features, the government argues. But **they need Apple's help because Apple codes use a proprietary "signature" that cannot be recreated by with government software.**

4. Apple can use another method to unlock the phone if it wants.

The password features are what the government calls "non-encryption" parts of Apple's code. But **the request allows Apple to use a "mutually preferable" technical solution on this device only.** It can even be done at an Apple facility, according to court documents.

Comments or thoughts??

Questions: (first four from the article. May go out of order. Let's discuss)

0. Initial thoughts about this case?

1. How could Apple, and the government, not have a master key already?

2. Isn't it just one phone? Is it possible to unlock just the one phone, but keep the back door from leaking?

3. Is it even legal for Apple to refuse this?

4. What if other governments — or companies — do the same? If the U.S. government demands access to an iPhone, can other governments do the same? Will consumers around the world still trust Apple products if they know Big Brother is watching?

5. "Identity theft, stalking, fraud, …illegal electronic surveillance, and theft of intellectual property are just some of the examples of crimes committed every day on mobile devices." Should law enforcement to be able to use these same devices to prosecute criminals and not hide behind mobile devices security?

6. Do you think this case could change way data is made available to law enforcement?

7. When do you think it IS appropriate for someone's data to be made available if suspected of a crime?

Closing:

- Show of hands: Who do you side with Apple or the FBI?
- Round the group: What is the most important factor in your answer?

OnLine Post Survey…

New Devices Allow Police to Track, Use Your Cell Phone

WRIC Newsroom
Published: January 15, 2015, 6:20 pm
http://wric.com/2015/01/15/new-devices-helps-police-track-use-your-cell-phone/

“Once activated, devices like Stingray or Hailstorm can locate and search the personal information on a number of surrounding cell phones. You can be outside or inside your home, and currently police don’t need to have a search warrant to use it.”

“This technology can also pretend to be your phone, so they can take your number and communicate with people that you’ve communicated with or with people you haven’t and pretend to be you.”

Cops must now get a warrant to use stingrays in Washington state

New statute also forces police to more fully explain cell-site simulators to judges.
by Cyrus Farivar - May 12, 2015 6:49am PDT
http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/

“Washington’s law, which takes effect immediately, is not the first in the United States, but it may impose the most stringent requirements.

“A handful of states, including Virginia, Minnesota, and Utah have similar laws on the books. Washington’s, though, imposes extra requirements that compel police to describe the technology and its impact in detail to judges—presumably despite any nondisclosure agreement that those agencies may have with the FBI and the dominant manufacturer of the devices, Harris Corporation. Both the FBI and Harris have previously refused to respond to Ars’ direct questions.”
…
“The secretive surveillance devices are not only used to determine a phone’s location, but they can also intercept calls and text messages. During the act of locating a phone, stingrays also sweep up information about nearby phones, not just the target phone. Stingrays typically spoof a cell tower and force phones to connect to it, often by making the handset step down to 2G, which does not require encryption.”

Related: Also now pending is the Federal “Cell-Site Simulator Act of 2015” filed late 2015 will require state and local law enforcement agencies to obtain a warrant before they could use stingray surveillance devices.

Online privacy: FBI vs. Apple (Survey):

What is your major take-away from our FBI versus Apple discussion/seminar?

What factual information and concepts did you learn?

Who do you side with Apple or the FBI?

What is the most important factor in your answer?

Do you think this case could change way data is made available to law enforcement?

When do you think it IS appropriate for someone's data to be made available if suspected of a crime?

Your Online Privacy:
What is the most important about the information you put in your cell phone and enter online via a computer and the web?

What kinds of personal information is most important to be kept private?

Who might be interested in the information that you put online and in your cell phone?

What safe guards do you follow to make sure that your online information is kept private, this includes use of your cell phone & mobile devices as well as computers?

How Private do you think the information you enter online is for your…

A. Your cell phone or mobile device (iPod Touch, Tablet, ...)?
1) Anyone could obtain it … 10) I am the only person who can see it.

B. Using the computers with hour student account at Garfield High School?
1) Anyone could obtain my information … 10) I am the only person who sees my information.

C. The computer you use most outside of school?
1) Anyone could obtain my information … 10) I am the only person who sees my information.

What kind of device do you personally use the most? __ Smart Android Phone __ iPhone __ Tablet or iPod device using Wifi __ Don't use any, I am way safe.

What kind of computer do you use outside of school? __ A shared family computer __ My own computer or laptop __ I use public computers at the library, etc.
What Operating System? __ MS Windows __ Apple OSX __ Linux

Name: _____ **Per:** _____

Your Online Privacy (pre-survey):

What is the most important about the information you put in your cell phone and enter online via a computer and the web?

What kinds of personal information is most important to be kept private?

_____

_____

Who might be interested in the information that you put online and in your cell phone?

_____

What safe guards do you follow to make sure that your online information is kept private, this includes use of your cell phone & mobile devices as well as computers?

_____

_____

How Private do you think the information you enter online is for your…

A. Your cell phone or mobile device (iPod Touch, Tablet, ...)?

	1	2	3	4	5	6	7	8	9	10	
Anyone could obtain my information	○	○	○	○	○	○	○	○	○	○	Private, I am the only person who can see it.

B. Using the computers with your student account at Garfield High School?

	1	2	3	4	5	6	7	8	9	10	
Anyone could obtain my information	○	○	○	○	○	○	○	○	○	○	Private, I am the only person who can see it.

C. The computer you use most outside of school?

	1	2	3	4	5	6	7	8	9	10	
Anyone could obtain my information	○	○	○	○	○	○	○	○	○	○	Private, I am the only person who can see it.

Key Standard/Unit: Security and Risk Awareness Issues

From our SPS Computer Programming Course Framework, CIP Code: 110201

Competencies

- **Discuss security principles, privacy issues, vulnerability and threats**
- **Illustrate what fundamental legal issues involved with security management**
- [Secondary: Explain principles of secure password strategies]

I. Primary Focus Standards:

Educational Technology
2.1 Practice Safety: Demonstrate safe, legal and ethical behavior in the use of information and technology.

21st Century Skills
5. A.3 Apply a fundamental understanding of the ethical/legal issues surrounding the access and use of media.
9. B.1 Respect cultural differences and work effectively with people from a range of social and cultural backgrounds.
9. B.2 Respond open-mindedly to different ideas and values.
11. B.1 Act responsibly with the interests of the larger community in mind.

CCSS- Speaking and Listening
SL.11-12.1. Initiate and participate effectively in a range of collaborative discussions (one-on-one, in groups, and teacher-led) with diverse partners on grades 11–12 topics, texts, and issues, building on others' ideas and expressing their own clearly and persuasively
SL.11-12.2. Integrate multiple sources of information presented in diverse formats and media (e.g., visually, quantitatively, orally) in order to make informed decisions and solve problems, evaluating the credibility and accuracy of each source and noting any discrepancies among the data.

CCSS Reading
RI.11-12.7. Integrate and evaluate multiple sources of information presented in different media or formats (e.g., visually, quantitatively) as well as in words in order to address a question or solve a problem.

II. Additional Standards that could be developed further in this exercise

Educational Technology
1.3 Investigate and Think Critically: Research, manage and evaluate information and solve problems using digital tools and resources
1.1 Innovate: Demonstrate creative thinking, construct knowledge and develop innovative products and processes using technology.
1.2 Collaborate: Use digital media and environments to communicate and work collaboratively to support individual learning and contribute to the learning of others.
2.2 Operate Systems: Understand technology systems and use hardware and networks to support learning.

CCSS Reading

RI.11-12.4. Determine the meaning of words and phrases as they are used in a text, including figurative, connotative, and technical meanings; analyze how an author uses and refines the meaning of a key term or terms over the course of a text (e.g., how Madison defines faction in Federalist No. 10).

2.3 Select and Use Applications: Use productivity tools and common applications effectively and constructively.
2.4 Adapt to Change (Technology Fluency): Transfer current knowledge to new and emerging technologies