* **Why did Snowden leak the information?**
* **Do you believe that he regrets his actions?**
* **What is your opinion regarding the ethics of his actions?**
* **Do you consider him a hero or a villain?  Explain.**

Notes:

Edward Snowden: How Your Cell Phone Spies On You

<https://www.youtube.com/watch?v=VFns39RXPrU>

Phone always signaling: IMEI and IMSI

* Unique identifiers
* IMEI burned into phone
* IMSI burned into SIM card
* Heard by cell towers
  + Who they “hear” louder is closer
  + Makes notes of
    - Handset
    - Phone number
    - Time
    - = identity
  + Compares notes of other nodes in network
    - Where is this phone in the world right now
    - Network figures this out to direct calls to the intended phone

Data collected use to be “ephemeral”, or it would disappear, before collection started

* Now, this data is permanent

Every access point also has a globally unique identifier

Google Street cars keep track of where the wifi networks are, including personal wifi networks

When you shut your phone off, is it really off???

Operational Security:

* What are the realistic threats you’re trying to mitigate
* What would the loss be if compromised

Andrew Bunihwuam

* Introspection Engine

Average person primary threat:

* Bulk data collection

Problem:

* Don’t know what devices are actually doing
* Can’t see data collection

Apple and Google don’t let people shut down connections made by apps

* They basically don’t allow full user-controlled security
* They don’t trust the user to use it properly
* They ARE right that it’s a security risk, from a certain perspective

Problem:

* Inequality of Available Information
  + They can see everything about you
  + You can’t see everything about them
    - You paid for the device
    - They own more of it than you do

By design, governmental and corporate realized it was in their interest to conceal data collection activities to increase breadth and depth of sensing networks

Surveillance use to be government only operating satellite data collection

* Is now bulk and widespread “dragnet”

User agreement contracts, TOS, give them the ability to say “You agreed to this” when we really agreed to access the app, not to be surveilled, but legally, we gave permission

“Third Party Doctrine”

* Legal principle derived from Smith vs Maryland
  + Smith harassing lady, making phonecalls to her “creeper”
  + She calls the cops, sees a car driving past her house, gets license plate number
  + Gives plates to cops
  + Cops look up number
  + They find the house, they ask phone company for number, they find the guy
  + Arrest the guy
  + Went to court
  + Cops got the records without a warrant, expedience, just wanted to get the guy off the jail for being a creeper
  + Ruled the records were not actually HIS records, they were the company’s records, so no warrant was required
  + No 4th Ammendment protections
* Government used this ONE case as precedent for widespread data collection
* Still relying on this single precedent to this day

It’s not just data, it’s people’s lives. People are being exploited. People are being manipulated, not data.

* Companies and governments still denying

John Pearbarlow

* Freedom of Press foundation
* “You can’t awaken someone who’s pretending to be asleep”

Edward Snowden on German TV: US Media Blackout

https://vimeo.com/85736856

Buzzfeed:

* Interviewed gov officials, gave them anonymity
* Gov officials wanted to murder Snowden
* “Bullet in head,” “poison him on way home from grocery store,” “die in the shower”

Political class didn’t protect public’s right, but the rights of the security state

Thousdands of violations by NSA and other agencies every year

Obama wanted to preserve authorities we didn’t need

These programs have no value, never stopped an attack in the US, marginal other value

NSA operates under President’s executive authority alone

Everything you do leaves a trace

* Gov decides it’s a good idea to collect it ALL
* Used to need a warrant
* Now they apply totality of their powers in advance, prior to an investigation

**WHY?**

Breaking point: Seeing director of national intelligence James Clapper directly lie under oath to congress

* No saving int community that believes it can lie to public and legislators who regulate its actions
* Seeing that meant no going back
* Realization no one else was going to do this
* Public had a right to know what the government was doing “in its name” and against the public
* NSA employees and elected reps were banned from knowing and discussing these things
* Only review they had was FISA court
  + Rubber stamp authority
* When you realize the power you have:
  + Can wire tap the president
  + Wire tap a judge
  + NSA only discovers abuses through self-reporting

5 eyes

* Artifact of post-ww2 era
* Anglophone countries of major powers coop to share costs of int gathering infrastructure
* UK – GCHQ
* CANADA CSEC
* US NSA
* NZ DSD
* AUS signals intelligence directorate
* Supra-national intelligence organization
  + Doesn’t answer to laws of their own countries
* Brits cant surveil brits, but NSA can, and they exchange data
* 5 eyes won’t “spie” on eachother’s citizens
  + Spying is defined differently
  + GCHQ is gathering enormous data on UK citizens
  + NSA doing same to US
  + Agreements are NOT legally binding
  + Can be deviated from or broken at any time
  + Can spy on citizens and share that information
* “nudge and wink” dynamic
* Surveillance and abuse doesn’t occur when data is viewed, but when it’s gathered
* German and US services “in bed” together
  + Share tools, infrastructure, and reporting

Ex Key Score

* Front end search engine
* All records collected worldwide all day
  + Any email
  + Any website traffic
  + Any device someone sits at
  + One stop shop for access to NSA info
  + Can tag individuals using it
  + Fingerprint:
    - Network activity unique to a target
    - Anywhere a person goes and tries to hide, the NSA can find them
    - Anyone NSA shares this software with can do this
  + NSA gets German data, whether provided or not
    - Every country in the world has data of their citizens in the NSA
    - All data, calls, emails, purchases, location info, etc, in hands of NSA
  + Filtering of Ingest:
    - When NSA puts secret server or hacks router, “if I see what I think is a german talking to another german, I’ll drop it”
      * But how do we know
    - When they say there’s no spying, they don’t mean data isn’t being gathered, they mean they’re not intentionally searching for citizens
      * Fingers crossed behind the back promise
  + If the NSA isn’t collecting data on german citizen in Germany, they are intercepting that data after it leaves the country
    - Anywhere comms crosses, it gets ingested and added to database
    - Same deal worldwide
  + Spies on companies as well, “probably”
  + US is engaged in economic spying, “no question”
    - For National interests, not national security
* Capabilities provided because of weak security standards in internet and networks, int services CAN create services that see EVERYTHING

We know Angela Merkel was monitored by NSA

* How reasonable is it to assume she was the only german official monitored
* Would suggest unreasonable that they’d only watch merkel and not her aids, heads of ministries, etc…

How did Snowden get into such a sensitive position with the access he had?

* Highlights dangers of privatizing government functions
* Served as a private contractor
* For profit companies doing gvt work like targeted espionage, surveillance, etc..
* Anyone who has the skills and qualifications will be empowered by gvt to do so with very little oversight
* Had a deep information education in computers and electronic technology
* Wanted to join special forces in may 2004
  + Not actually intended for direct combat
  + Intended as a force multiplier
  + Inserted behind enemy lines
  + Teach and enable local population to resist and support US forces
* Broke his legs and was discharged during training
* In 2007, was in CIA op in swizerland
  + Wanted to do everything he could to prosecute the public good in the most effective way
  + Use his tech skills in most difficult positions he could
* How did he become a whistleblower
  + No matter how deeply embedded in and faithful to gvt, no matter how strongly they believe in causes, people can learn/discover line between appropriate gvt behavior and actual wrong doing
  + Became clear to him that line had been crossed
* Contracting culture of national security community in us
  + Driven by number of interests
    - Limiting direct gvt employees
    - Keeping lobbying groups in congress from very well funded businesses
  + Gvt policies are being influenced by private corps who have interested divorced from public good
    - Boozallen hamilton
      * Private individuals have access to millions and millions of records
      * Can walk out the door with those records with no oversight
* Chief of task force investigating snowden found no evidence of help, deal, or contact to accomplish his mission.
  + Snowden not a spy or foreign agent
  + Not a traitor
    - Gave info to American public, journalists reporting American issues
  + Snowden will NEVER be fully safe until these systems have changed
* Applied to long list of European countries for asylum
  + All of whom felt that doing the right thing was less important than supporting US political concerns

Foreign countries creating national internets to protect data

* Not going to stop the NSA
* Solution is not walled garden
  + Though does raise level of sophistication of collection
* Securing the data is the problem

Obama asked Putin to extradict snowden multiple times

* Will snowden have to spend the rest of his life in Russia?
* Leaks caused no harm, did public good
* NYT wrote comment in favor of snowden
  + Didn’t do much to help

Obama said Snowden charged with 3 felonies

* Thinks he should return, speak to a lawyer, make his case
* Crimes he’s charged with are crimes that don’t allow Snowden to make his case or defend himself
* Espionage act never intended to prosecute journalistic sources
* Intended for people selling docs in secret to foreign governments
* Illustrative the president would choose to say someone should face the music when he knows the music is a show trial

Frontline: United States of Secrets – Part 2

<https://www.youtube.com/watch?v=rs2iN0oVdt4>

Snowden fled to Hong Kong

* Met Glenn Greenwald and Laura Poitras, also Ewen Macaskill from the Guardian
* Order directing Verizon Business Services to hand records over to the NSA
  + Contradicted what James Clapper said before congress just months earlier
  + Clapper’s testimony convinced Snowden to become a whistleblower
* Guardian gave WH 4 hours to respond to their plan to release the report
  + John Delong – NSA Director of Compliance – WH reached out to JD an hour before the story broke
  + Jenine Gibson took return call from WH
    - Tried to persuade her not to publish
    - She asked if WH had any major national security objections
    - WH just stalled
    - Guardian published story
* At Washinton Post Barton Gellman writing another story
  + PRISM – NSA program
    - 9 ISP cooperating with NSA
    - GVT asked him not to publish names of companies
      * If published, companies would be less inclined to cooperate
    - Post then published story
    - PRISM was not about metadata, but about content
      * Photos, videos, words in emails, sounds of voice in skype calls, files stored in cloud services, etc…
* Obama takes one question regarding reports about NSA collection programs
  + Lies to press conference, essentially says metadata is collected
    - Supposedly not against US citizens
    - “No names, no content”
    - Lies – Documents proved it
    - Had no idea what was coming
* Snowden decides to reveal identity using video he recorded a few days earlier
  + NSA targets comms of everyone, ingests them by default, collects them, filters them, analyses them, stores them
  + People should care because even if they’re not doing anything wrong, they’re being watched and recorded
  + These things need to be determined by the public, not the government.
* Knew the minute he revealed his identity, he had to go into hiding
  + A journalist put up on twitter pictures of the hotel room showing the light fittings, identified location
    - Snowden leaves hotel room
  + Left it to the journalists to decide which documents to publish
  + Evaded US press and authorities for two weeks
  + June 23rd, set off for South America via Russia
    - Only got stuck in Russia because US prevented him from leaving
      * US gvt revoked his passport
    - Russia grants Snowden asylum
* President appointed a panel to review NSA programs
  + Go wherever you want, can see any classified program, etc… except realize I won’t accept any block between me and my constitutional oath of defending the united states (paraphrased by another)
* Silicon Valley was angry and confused about access being given to NSA
* Tim Wu, author: The Master Switch
  + Big tech couldn’t believe it
* Big tech denying involvement in PRISM
  + Perceived a threat to their business model
  + Issued heated statements taking issue with the idea they’d hand over free access to the NSA
* PRISM was only part of NSA
  + MUSCULAR extracted data from fiber cables overseas
    - Backdoor access
    - Unrestricted data collection
    - Could hack into company’s servers and collect data in bulk
  + NSA decided it was okay under EO 1233 with backing of justice dpt and WH to break into private data links connecting data centers of google and yahoo around the world, collecting large fraction of world’s internet traffic, including Americans
  + Stewart Baker, Asst Sec., Homeland Security – Overseas, the ability to do that in bulk is “critical” in finding comms of people trying to hide. If you can look for certain patterns and dive into those comms, you find people unknown to you that were very dangerous
* Leaked files showed NSA operatives bragging about what they were doing
* Google criticized for not encrypting data traveling between data centers
  + They’re now trying to encrypt it all
* NSA believes Snowden is causing damage and harm to US companies and US interests
  + Should have been no surprise the NSA was snooping into this data
* Patriot Act in 2001
* AT&T secret room in 2002, San Francisco, Mark Klein noticed and figured out what they were doing
  + Discovered gvt was copying ALL internet traffic
  + Afraid to speak out for several years, but went public after reading a NYT front page story about NSA spying in 2005
  + No one ever acknowledged it, but no one denied it
  + Robert Dietz, NSA General Counsel 98-06
    - Wouldn’t talk about it
    - Legal program
    - Doesn’t think it was warrantless wireless tapping
    - Far as he was aware, it was still classified
  + Edward Whitacher, AT&T Chairman and CEO
    - Refused to admit to providing customer info to law enforcement agencies
    - “We follow the law”
    - “We don’t violate the law, we follow the law”
  + Telephone companies happy to cooperate
  + ISP’s were uncomfortable, did not like it
  + Nick Merrill, CEO, Calyx
    - Received phone call from FBI that they had letter for him
    - FBI hand delivered letter to him
    - Asked for significant array of information from his company
    - Didn’t appear to be signed by a judge, was not a court order
    - Demanded information from him, said he could never tell anyone about the request
    - National Security Letter
      * Patriot act allowed any security agency to issue these letters and with a gag order
    - Thought it wasn’t legal nor constitutional
    - Disobeyed letter
      * Contacted lawyer and ALCU
    - FBI issued 65000 letters that year
    - Merrill was first to challenge on constitutional grounds
    - Until 2013, no company questioned the constitutionality of these letters
    - Google finally challenged 19 NSL’s
    - By this time, FBI withdrew Merrill’s letter
      * Merrill still cannot talk about exactly what was requested
      * If we knew what was requested, we’d be shocked
  + Big ISP’s had different priorities
    - Trying to find out as much as possible about users
    - NSA was watching
  + Google kept everything people searched for
    - Searches maps nicely to desire of advertisers
    - Gmail mined email content
    - Used data to advertise, $$$
    - Tried to assure they were just scanning the emails
      * No different than a wire tap
    - Andrew Maclaughlin received a call
      * Liz Figueroa,CA senator
        + Meeting with larry and sergei
        + “Sentor, how would you feel if a robot went into your home and read your diary, your records, everything, etc… but before it left your house, it imploded, that’s not violating privacy”
        + “Yes it is!”
        + The robot knows a lot more than just whether you’re sad
        + Figueroa backed off, believing data to be destroyed
        + It wasn’t destroyed
        + Google didn’t want bill to attack their business model
        + Entirety of big tech in CA went against the bill
    - Gvt: If you let them listen, why can’t we listen
  + FBI loves facebook
    - People are willing to tell others everything about themselves on FB
    - Execs at Google became worried due to people posting on FB
    - Google wants to boost data collection to compete
    - Buys a leading data company
    - Became most powerful company in internet ad world
    - Refined data collection from web browsing
  + Cookies
    - Unique ID set by any website you interact with
    - Could be dozens or hundreds of servers per site
    - For NSA, commercial tracking in an opportunity
      * Studied their methods
      * Cookies rarely encrypted
      * NSA could just snatch it
* Google PREFID
  + Special cookie
    - NSA piggybacking off google’s PREFID cookies
    - Used them to track browsing behavior and inject malware into users’ computers
    - Google pushed back
  + Hit piece against Soltani alleged he received funds from a pro-privacy group
    - Article revealed privacy risks associated with advertising
* Dec 17, 2013
  + SV execs went to WH
  + Called in to advise president about fixing health care website
  + Execs refused to go along with that, focused on NSA and how unhappy they were
    - What president has authorized and what NSA is doing is doing huge damage to their global markets
    - Making lots of money, all that goes away if people no longer trust
  + PRISMA supposedly played important role in preventing terrorist attacks
  + But bulk data collection was going too far
  + Tech infrastructure could be abused after another tragedy
  + Had to be sure it couldn’t be used against us
* NSA was racing to build quantum computer to defeat all kinds of encryption
* Moscow, Dec 2013
  + Snowden agrees to meet Bart Gellman
  + Went to hotel, received phone call, given place to meet, met snowden there, led to a secure place to talk
  + Interviewed Snowden for 14 hours over next two days
  + “Found a guy who was almost ZEN-LIKE in his serenity and his comfort with what he had done that he had consciously decided he was willing to take huge risks to provoke a public debate, and he provoked a public debate that no one could possibly have foreseen.”
  + Obama – “You cannot have 100% security, and then have 100% privacy”
* Security state knows so much about us, we know so little about them
* We can’t hold gvt accountable because we don’t know what it’s doing

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What happened to the 2010’s “war” against the government to fight for our privacy and expose its breach of our constitutional rights?

CITIZENFOUR

* SIGINT system
  + Selected?

Bitcoin.comNews

https://news.bitcoin.com/us-federal-court-rules-nsa-mass-surveillance-illegal-edward-snowden/

US Federal Court Rules NSA Mass Surveillance Illegal, Credits Edward Snowden, Sep 03 2020

* US Court of Appeals for the Ninth Circuit
  + 59 page ruling
  + US v Moalin
  + 7 years after appeal filed in Nov 2013
  + 4 Somali immigrants convicted on terrorism financing charges
  + 3 judge panel
  + NSA metadata program “officially” ended in 2015
    - Tracked 5 billion phone records a day
  + Gvt may have violated 4th amendment
  + Jennifer Granick, ACLU, said it was the only case “the government could point to to say that the phone records dragnet ‘works.’ And now we know all that illegal mass surveillance wasn’t relevant even in this single instance,” elaborating: “Government lawyers argued the phone dragnet was critical and lawful. Actually, it was illegal. And it wasn’t critical. It wasn’t even necessary to show probable cause, never mind guilt.”
* Anatoly Kucherena argued US should drop all possible prosecutions against Snowden instead of just pardoning him as he had not committed any crimes.

Business Insider

<https://www.businessinsider.com/nsa-phone-snooping-illegal-court-finds-2020-9>

The NSA phone-spying program exposed by Edward Snowden didn’t stop a single terrorist attack, federal judge finds

* Bulk metadata collection program discontinued in 2015 when Congress passed the USA Freedom Act
  + Bulk phone records could still be kept by private phone companies
  + Could only be obtained by investigators with a judge’s permission
* NSA reportedly stopped pursuing phone metadata entirely by 2018

The Guardian

<https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware>

Interview: Edward Snowden: ‘The people are still powerless, but now they’re aware’, Jun 4 2018

* 5 years later, snowden has no regrets
* Results:
  + US and UK governments faced court challenges to surveillance laws
  + Legislation has been passed in both countries
  + Internet companies have made encryption common place
* Snowden: “People say nothing has changed: that there is still mass surveillance. That is not how you measure change. Look back before 2013 and look at what has happened since. Everything changed.”
  + “The government and corporate sector preyed on our ignorance. But now we know. People are aware now. People are still powerless to stop it but we are trying. The revelations made the fight more even.
  + “If I had wanted to be safe, I would not have left Hawaii”
* US and UK intel agencies say it was an act of betrayal that caused damage on a scale the public does not realize.
* Jeremy Fleming, dir GCHQ: “What Edward Snowden did five years ago was illegal and compromised our ability to do that, causing real and unnecessary damage to the security of the UK and our allies. He should be accountable for that.” (speaking to the GCHQ’s mission to keep the UK safe)
* Agencies were forced to develop and install new and better capabilities faster than planned as a result of the leaks
* Another change: transparency from the intel agencies, at least the GCHQ
  + Fleming repsonds: “It is important that we continue to be as open as we can be, and I am committed to the journey we gbegan over a decade ago to greater transparency” implying change occurred before Snowden
* Dir of NSA Richard Ledgett, when retiring, said US should have made the bulk phone data collection public
* Former Dir of GCHQ Sir David Omand: “A sounder and more transparent legal framework is now in place for necessary intelligence gather. That would hav3e happened eventually, of course, but his actions certainly hastened the process.”
* Big tech pushed back, but why the rise of the “smart speaker” an always-on microphone in people’s homes?

AP News

<https://apnews.com/general-news-2f5ed45a59d0439fad6b9641f30b65a8>

For banks, data on your spending habits could be a gold mine, Dec 2019

* Banks sitting on info that could predict **or sway** where the public spends
* Social Media only try to infer what we buy, but banks KNOW
* Through partnerships with banks, Cardlytics says it gets insights on $2.8 trillion of annual customer spending worldwide
* Augeo is a similar rival company
* AmEx has in-house program
* One positive use of this tech: HSBC can use information that you’ve charged a flight or hotel to avoid declining your card use as fraudulent when meals overseas are charged
* Abeer Bhatia, exec with Chase’s CC business, says commissions barely cover costs, more important to incentivize rewards-conscious consumers to use its cards
* Americans have **demonstrated they value freebies and discounts more than intangible privacy concerns**
* Banks many times don’t seek explicit consent, instead include these programs by reference in general agreements for cards and online banking
* “It’s totally long, and people don’t read that” Saisattha Noomnual, grad student in Chicago
* By federal law, banks only have to let you withdraw (opt out) from marketing
* Banks insist they don’t share data because names are replaced with anon ID numbers, but such data can be “de-anonymized”
* Fast food -> health insurers -> uh oh
* Large bar tabs -> auto insurers -> uh oh
* Targeted offers could lead to unhealthly habits like fast food
* “Consumers aren’t aware of the subtle nudges apps are giving them to buy, buy, buy,” Mierzwinski said. “They are basically digging deep into your psyche and figuring out how to manipulate you.”

NPR

<https://www.npr.org/2021/06/02/1002590964/your-amazon-echo-will-share-your-wi-fi-network-with-neighbors-unless-you-opt-out?utm_source=pocket_mylist>

Your Amazon Echo Will Share Your Wireless Network With Neighbors, Unless You Opt Out

* Amazon building wireless network using your bandwidth
* Amazon Sidewalk
  + Extends the range of low-bandwidth devices to help them stay online
  + Pools neighbors’ bandwidth to help connectivity for devices that are out of range
  + Includes:
    - Ring Floodlight Came and Spotlight models
    - Echo devices
    - Ring Doorbell Pro devices
  + If you and neighbor both have devices, but theirs is too far from their router, it can use your bandwidth
  + Max rate 80kbps
  + Total monthly cap of 500mb
  + Amazon says it’s “secure”
  + Security experts:
    - “I feel like the bigger motivation here is to create a private surveillance network. I suspect they’re seeing this as a real opportunity for kind of bridging all these different Ring devices in particular,” says Jen King, privacy and data policy fellow at Stanford Institute for Human-Centered AI
    - Ashkan Solatani “In addition to caputuring everyone’s shopping habits and internet activity (amazon.com and AWS, respectively)… now they are also effectively becoming a global ISP with a flick of a switch, all without even having to lay a single foot of fiber”
  + Amazon adds devices to shared network unless owners opt-out
  + Why is this not an opt-in?
  + Company says it’s in the customers best interest