Frontline: Spying on the Homefront

* December 2003: FBI Ellen Knowlton – to all casinos “We want all your records.”
	+ Hotel directors resisted
	+ Lots of intimidation (from: ACLU)
	+ Knowlton:
		- Asking for records for single purpose of making comparisons
		- Not asking for records that would be incorporated into FBI files
		- As many records as they could obtain
	+ Before this, requests for targeted individuals happened, this was first time they received requests for everyone, all records
	+ Knowlton:
		- If they’re not a terrorist, has nothing to worry about
* Terror attacks on 9/11 brought a new strategy
	+ New Paradigm of Prevention
		- Innocent people caught in the dragnet
* NSA – warrantless eavesdropping in US
	+ NYT story dropped Dec 16, 2005
		- Congress erupted in protest
	+ Cardinal rule during cold war was “Hands off Americans”
	+ Bush changed this with secret order
		- Said program was “narrowly targeted”
		- Assured American people he “had authority to do this”
	+ Watergate was NSA controversy that’s happened before
		- NSA had been spying on Americans for decades
		- Operation Shamrock
			* Obtain access to telegrams leaving US for foreign countries
			* Look through telegrams for telegrams of interest
			* Gained access simply by asking communications carriers
			* Very few rules restricting agencies at this time
			* Violated section 605 of communications act of 1934 and 4th amendment
			* Congress passes FISA law
				+ Foreign Intelligence Surveillance Act
				+ Secret court on 6th floor of Justice department
				+ No wiretaps in US without warrant
				+ FISA court exclusive authority for obtaining warrants
			* Want cops to be aggressive and ambitious, but also want an authority to reign them in and keep them in check
	+ Bush: “Of course we use FISAs. But FISAs is for long-term monitoring. What is needed in order to protect the American people is the ability to move quickly, to detect.”
	+ NSA needed to tap into comms more broadly than president indicated
		- Foreign agents disguise selves as civilians
		- How does NSA figure out who is foreign agent?
	+ Blanket eavesdropping = Electronic Driftnet
	+ Hayden said they were going for specific comms, denying the driftnet
		- “in this program…”
			* But not other programs, hehe
		- Alberto Gonzales denied driftnet as well, calling president allowing a narrow program
		- Every denial attached to words “this program”
			* “…the program which I am testifying about today”
			* Gonzales avoids answering when asked about OTHER programs
* NSA capabilities
	+ Calls sucked up by millions
	+ Not just calls, but data mining
		- No individualized suspicion
		- Collecting all data, data gives rise to individuals based on connections found
* Mark Klein, internet tech for AT&T
	+ 2002 email, someone from NSA was going to visit for business
		- Background checks for security clearance for field engineer
		- Working on new room being built
		- Workmen treated room as hush-hush
		- Only guy with NSA clearance had access
	+ Maintain internet service for millions of customers, domestic and internal
	+ Klein’s room connected to NSA room via a splitter
		- Intercept internet stream
		- Copy the data
	+ Found 3 docs
		- Detailed designs for secret room
		- Could do anything they wanted with computing power in that room
		- Narus STA 6400
			* Heavy duty processing power to analyze data
			* Narus = latin – to know
			* Analyze all the internet traffic flowing through the room
			* Packets
				+ First layer: addresses
				+ Deeper layers: payload
			* Rep from company that sells Narus hardware unable to answer basic questions, even hypotheticals
		- Klein realized the room was a spy operation
	+ Decided to blow the whistle
	+ Went to Electronic Frontier Foundation, Cindy Cohn
		- Scott Marcus estimated eavesdropping rooms at 15-20 sites in US, JUST at AT&T
	+ 2006, EFF files suit against AT&T for selling customer phone and internet traffic data to government
		- AT&T urged dismissal citing state secrecy
* Bush put the single program back under FISA
	+ Not the others
	+ At the time, Narus box was still peering at internet traffic
* Vegas
	+ Cabs
		- Digital still pictures taken upon entry
		- Audio and video being recorded entire time
		- If an event, 20 prior and during event captured and downloaded
	+ Only time someone isn’t on video in vegas: private hotel room, or restroom
	+ After 9/11, government agencies moved aggressively to tap into all those data streams
	+ Alan Feldman, MGM Mirage
		- Wanting all data on everyone is unprecedented in the industry
	+ Patriot Act gave FBI board authority to engage in fishing expeditions
		- Expanded reach for national security letters, which didn’t require a warrant
		- Expanded to not just target an individual, but an entire database
		- Phone, internet, credit histories, and others
	+ If Feldman received a national security letter, could not tell anyone if they did
		- With warrants, they could talk about it, but not with NSLs
	+ CDs of data sent from Vegas to DC to compare against terrorist lists
		- Made a few hits
			* Could be as little as a similar name
	+ For years, casinos used software to ferret out criminals from potential employees
		- Unmask obscured relationships
		- To determine if someone applying as a dealer was a known theif
		- Idea was to protect company assets before crime took place
		- FBI used this software to analyze data obtained in Vegas
	+ Acxiom, LexusNexus, ChoicePoint
		- Data collection agencies, create dociers on individuals
		- Gvt pushed agencies to use these private databases
		- FBI doc shows they pushed to use ChoicePoint, for example
	+ FBI workaround
		- Ping private sector database
		- As long as its one query at a time, doesn’t break the law
	+ Robert Muller called by congress for using NSL’s to secretly collect private records of US citizens
		- 150,000 requests over last 3 years along (at time of recording)
		- Muller “acknowledged problem and dangers” (ha, sure)
	+ Government accounting office found 199 datamining ops in over 150 agencies
	+ DARPA
		- TIA – Total Information Awareness
			* Required access to enormous volumes of personal data
		- 2003, congress supposedly cut off funding for TIA
			* Possibly moved over to the NSA after this cut
* Tech guys seem to know ubiquitous surveillance is happening, will continue to happen, and thinks normies are naïve for thinking we even CAN have a public conversation on the topic
* Balance of security vs rights…
* Dec 2003
	+ Sheriff Bill Young – decided to carry on with New Years Eve celebrations in Vegas
		- Threat was too vague
	+ Stephen Sprouse and Kristin Douglas caught up in the driftnet
	+ FBI says it held data from Vegas for more than 2 years
		- Claims to have destroyed it all
* Does prevention collide with the constitution
* Peter Swire – WH privacy council
	+ Check everybody
	+ General warrants was part of the reason for American revolution
* John Yoo, Justice Dept sr. attorney
	+ Can have warrantless searches, but must be reasonable
	+ Does it apply during wartime operations?
		- No
		- Do we want to make it more difficult for gvt to stop terrorist attacks?
	+ Michael Woods, FBI national security atty
		- Tradition of law, sphere of privacy the gvt can’t come into
		- But, sphere is getting smaller and smaller
* People in America think this doesn’t affect them, that it only applies to terrorists
	+ Naïve
	+ Innocent americans WILL be affected
* FBI found NO terrorists in Vegas once they went through all the data collected
* Original intelligence warning about vegas, it was a mistake
	+ Someone got it wrong
	+ Led to massive data collection, breach of privacy