MIT CENTER FOR CIVIC MEDIA

LOGIN

SASHA COSTANZA-CHOCK

Associate Professor of Civic Media and Co-Principal Investigator

Twittter: @schock

Sasha Costanza-Chock is a researcher and mediamaker who works on social movement media, co-design, media justice, and communication rights. He is currently Associate Professor of Civic Media at MIT's Comparative Media Studies program (http://cmsw.mit.edu), and is a Faculty Associate at the Berkman Center for Internet & Society at Harvard University. He sits on the board of Allied Media Projects (http://alliedmedia.org), and is a cofounder of Research Action Design (http://rad.cat). For more info see http://schock.cc.

schock.cc
Comparative Media Studies
Research Action Design (RAD)

THE GOVERNMENT IS PROFILING YOU: WILLIAM BINNEY (FORMER NSA)

Submitted by schock on November 26, 2012 - 11:34pm

CORRECTIONS via Deborah Hurley: The organizers of the event were Deborah Hurley and Ron Rivest. The event was co-sponsored by MIT Cryptography and Information Security Group and the Computers, Freedom and Privacy Conference (cfp.org). I invited Bill Binney to give his talk and invited Carol Rose, ACLU of Massachusetts, to serve as discussant to Bill's talk. The talk was subsequently posted at: http://techtv.mit.edu/genres/49-technology/videos/21783-the-government-i.... Following the recent revelations, I learned (yesterday) that someone had posted it here: http://www.youtube.com/watch?v=qB3KR8fWNh0. Although the MIT techtv version was fine initially, it does seem to have developed some audio/video problems.

--
On Monday, November 19th, former NSA official William Binney gave a talk hosted by MIT's CIS Group, entitled The government is profiling you. The talk was cosponsored by the ACLU and attended by about 65 people. Binney talked about the history of social network analysis as used by government, military, and intelligence agencies, the NSA electronic surveillance systems he helped to build, the expansion of US surveillance systems to include warrantless domestic monitoring of US citizens; his own whistleblowing efforts around the Stellar Wind program and the resultant intimidation he and his family faced, and the need for people to organize, speak up, and hold Congress, the Executive, the military, the NSA, and other organs of the State accountable. Binney was joined by Carol Rose from the ACLU, who described the current state of law, key cases, and key policy initatives. I liveblogged the talk via a public etherpad, and bear full responsibility for all errors or omissions. - @schock.

The Government is Profiling You: William Binney

[A short description of the talk, from CSAIL's site:]

“While spreading an atmosphere of fear after 9/11, our government has violated our laws, prevented the Congress and courts from doing their Constitutional duty, created a surveillance state and concentrated power in the executive, all in the name of keeping us safe. In an effort to reverse these ongoing unconstitutional activities, William Binney revealed the National Security Agency's massive domestic spying program, Stellar Wind, which intercepts domestic communications without protections for US citizens. Binney disclosed that NSA sought and received access to telecommunications companies' domestic and international billing records.”

“He told the public that, since 9/11, the agency has intercepted between 15 and 20 trillion communications. Binney also revealed that the NSA concealed Stellar Wind under the patriotic-sounding "Terrorist Surveillance Program," in order to give cover to the warrantless surveillance program's violations of Americans' constitutional rights.”

Key link: http://www.whistleblower.org/program-areas/homeland-security-a-human-rig...

This story was covered in Wired magazine:
http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/
http://www.wired.com/threatlevel/2012/04/shady-companies-nsa/

Introduction

[we're waiting for the talk to start / introduction.] The person who does the intro describes how Binney suffered an FBI raid on his house, at gunpoint, after he began his whistleblowing activities. Some years later, he received a letter from the DoJ telling him he was guilty of no crime.

Binney begins by outlining what he'll describe during the talk: a surveillance state that's currently being created. This all started in the early 1990s. Dr John Taggert, research chief of NSA, pulled together a central group to do dev in NSA. It required bringing all the talents together in one place to share the effort. Otherwise, everyone would be sitting in their own bins, not solving the problems that needed solution.

This was the SIGINT automation research center. John [Taggert] brought researchers and physicists, while Bill [Binney] brought crypto experts, analysts, and programmers. They brought all the researchers together in one place,

and assigned people to one component or another. People could then work together and incrementally improve, using rapid prototyping and spiral development.

In the mid 1990s, the biggest problem was the ballooning WWW. They decided they should focus on that, although their charter was foreign intelligence. They thought they should figure out how to monitor, diagnose, and select out of the flow of information that which they needed to analyze. So, they would throw out all domestic communication – it would never be collected.

They had the problem of how to look at terabytes a minute of data. They wanted to look at 20TB /minute. They thought the best way was to look at relationships between people. IP, username, ISPs, phone numbers, all would be attributes they could use to build relationships or social networks.

Social Network Analysis: Old Tricks

Binney asks us if we know how social network analysis was conducted by the U.S. Government during the civil war? He states that they simply watched people visiting other people. That's how they uncovered the spy network in Washington.

In WWI they did formal network analysis.

Now it's called social networking. It's nothing new really, just the scale: Binney's team wanted to do the entire world. This didn't pose a problem to them, b/c they would keep everything simple. Index flat files, knowledge DB graph and throw most away. It worked fairly well, for the arguments they had. It was clear they could scale to any number.

“We had no problem getting all the bad guys with that approach.”

Questionable Constitutionality

However, Binney notes that they realized they were picking up Americans. It was easily understandable via the phone numbers and IpV4. So, they developed a plan to managed the information collection that they thought would be constitutionally acceptable. They proposed to do this on a mass scale, worldwide.

Binney says that this process has never gone to court. The EFF lawsuit is dealing with that, and he signed an affidavit to support their suit, because he feels the collection of all this info is unconstitutional.

However, at the time, they got no feedback from DoJ: just a visit from the FBI to tell them to keep quiet.

Later, they learned that NSA had approached the phone companies to request all the billing data for all customers. This was 8 months before September 11th. Management had made this plan even before 9/11. When 9/11 occurred, it was the perfect excuse to get the data from the Telcos: protect the USA from terrorism.

Binney claims “That was a false premise: we could identify these people from the beginning. But it was a great pretext. They used a program we had setup to do foreign intelligence, and turned it around.”

The company that began was ATT. They forwarded roughly 320 million records of US citizens every day. Binney's estimate, and also Mark Klein's disclosure of the ATT evidence [re: signal splitting and "secret rooms" for NSA surveillance] insert device, gave a sense of how much data was involved.

Binney's estimate now is 20 trillion US citizen transactions, with other US citizens. “When you do that, assemble that much info, you're assembling power,” he says.

The NSA kept claiming that volume, velocity, and variety were problems. Binney says these are positive aspects, not problems; the question is how to take advantage of it. Binney used graphing techniques. He shows a slide “New Domain Access and Relationship Mapping.”

Relationship Mapping

He describes the key points of the slide: “Validating the data is crucial. Then you move to event recognition, check against your graph to see if you want that data or not. You also need privacy protection: determine whether to encrypt. Then you build an activity graph, and take other graphs from other domains: banking, phones, travel, twitter, whatever else you can gather. With a consolidated graph across all those domains, you analyze.“

One goal they had in the 1990s was to detect social security fraud. Their attempt was subject to an investigation. Binney thinks the data process they were using to do this wasn't unconstitutional.

In target development and discovery, you needed to figure out the network of possibles (suspects), separate from 'knowns,' and eliminate the vast bulk of traffic. This is what big data initiatives are looking for: automating target development.

He shows another slide: timeline analysis, email and phone. The slide shows communications activity over time across multiple platforms (email, phone, etc). Binney feels this also needs to be automated: what transaction combinations in this group need to trigger a warning?

For example: if you're trying to smuggle drugs from Colombia into the USA, the buyer and seller have to communicate to plan the transaction. “We have to find these communications and assess them.” Everyone in the USA is profiled. The info is gathered, and all they have to do is point to the target.

Someone from the audience asks “are those real phone numbers on the screen? Those are US phone numbers”

The image is of analysis of 9/11, Binney says. This is the danger. If you become a target, like Petraeus, now you're in the DB. The problem is, the FBI has access to this data. Mueller testified to that in March 2011 to the Senate judiciary committee.

In response to the Q: how would you prevent a future terrorist attack? Mueller said: we have a DB where one query can get all past emails and future emails as they come in. Then he says that “This is what Bluffdale is all about: storage for all that data.”

Q&A part I

Question: When you form the graph, you prune it, partly through relationship analysis?

A: You do frequency analysis.

Q: So does this pruning happen at the listening post? At the ATT station? If I broke into one of those rooms, I would have access?

A: Yes.

Binney provides another example about Canadian communications monitoring.

“Ready to be turned on for the imperial presidency”

Binney feels that “Unfortunately, the state of our surveillance state is: all set, to be turned on for the imperial presidency to do whatever it wants to do.”

“The real kicker for me, after they came after us, pointed guns at us, was they also falsified evidence. They also did this to Tom Drake. They falsified the classification of materials.”

Question: to what extent can we assume the left hand always doesn't know what the right hand is doing?

Binney: That's always our government. Forrest Gump had it right. Stupid is as stupid does. That described our government. The problem is, incompetence at this scale is dangerous. You could end up on a kill list, without knowing what the criterion is to get on or off?

Q: Could you speculate as to whether any foreign agencies have compromised the DB?

A: Mueller did.

Q: Are there intelligence sharing agreements that would give them access?

A: Yes. It's called the 5 eyes group. The English speaking countries. They're much closer than others.

Q; What about other nation states?

A: They're all depending on NSA. There's nothing comparable.

Q: What about the data center in Utah?

A: The Bluffdale facility. Probably about 5 zetabytes of capacity in the facility. If you eliminate all the video, and analogue audio, and just pick up the material you want, that's enough to store 100 years of the world's communication data. 10 to the 21st bytes.

Q: What if we send things disguised as video?

A: We were talking about this earlier. In my mind: no online cipher is safe. If they don't have the key, they'll come get it from you. Assuming they didn't plant. The safest thing is do all the encryption offline. Then send it. Then decrypt offline.

Q: steganography?

A: That's not safe.

Q: In the 1980s, NSA was doing trigger keywords.

A: Sometimes they attribute more capability than exists. I knew a lot of problems with that - it wasn't useful in an operational sense. Too many mistakes.

Q: A lot of times we hear 'patterns will tell us who the bad guys are.' You're saying, they have all the data and can turn the spotlight on anyone. Is there a system that will tell us predictively who the bad guys are?

A: We had no problem making those decisions. They claimed this as an excuse. They actually wanted to spy on the entire United States.

Q: If you're doing crypto offline, will anything highlight you as a suspicious person? The fact that you're using encryption?

A: Generally the FBI says "If you're encrypting, you're suspicious." I don't know how many tics it takes to get on the hit list. Kennedy got on he no fly list! If he had problems, imagine the problems any of us would have!

Q: If the data about Americans was being encrypted... first of all, is collecting it legal? Do you imagine that this data is still being encrypted? We've seen cases where privacy is NOT protected b/c we can still find patterns. Curious about your philosophy.

A: That was in place til 9/11. After that: they removed the protections on US citizens. Secondly: I designed the encryption to resist mass attack. It had 3 levels of encryption; whatever key they attempted to apply, if they got something that looked partial, it would be an error - by design. I was designing it so NSA couldn't break into it.

Q: Graph structure still makes clear where someone lives, or whatever. They live in NYC.

A: All that material was encrypted. All the attributes that were identifying would be encrypted.

Q: There have been attacks. For example, the FB graph, anonymous, just on graph structure you can recover people's IDs. That's the issue.

A: well you'd have to have some way to break it down to subsets to do that assessment. You have to do the same thing with the phone network. On billions of combinations.

Q: Are you saying it's not linkable?

A: uniquely encrypted. Your name, unique, constant over time. To build probable cause over time, to justify getting a warrant. The procedure we wanted to set up.

Q: From the point of view of statistics, even that, creating the graph...

A: you'd need a graph to compare it to.

Q: If you're the NSA equivalent in Britain, you have a graph like that.

A; They're even worse than we are.

Q: You said you "had no problem IDing the bad guys." How do you tell the bad guys from a bunch of kids pretending to be bad guys?

A: In the billions of people you're graphing, if they showed up as suspects, we'd look at them. To develop new targets. Not the rest of the innocent people doing absolutely nothing.

Q: Going back to crypto being unsafe: the algorithms are unsound? Or the popular implementations?

A: the implementation. If you take it offline, and use your own key, that should be secure. I have no idea how long it would take to get into them.

Q: You're saying I shouldn't use OpenSSL?

A: Is it on the web? The safest way to encrypt is offline. So it can't be penetrated.

Carol Rose (from ACLU) takes the mic

“I'm pleased so many of you are here today. The time will come, in your career, to decide how to use the incredible skills you're developing at MIT. We have to distinguish between privacy and secrecy. Privacy is your ability to control information about you. Secrecy is what the state is doing. In a democracy, it's the job of the people to watch the government, but the government is watching the people.”

“The law hasn't caught up with technology. Tech is not inherently good or bad, but it's being deployed in problematic ways. So how do we develop public policy around the right to control info about ourselves? The courts are saying "you can't bring that case to court." They're taking what was a rule of evidence: exclude a state secret from the trial. Now, they're saying the whole case is kicked out. You can't even get into court to find out whether it's constitutional. They other problem is standing: they're saying you have no standing to bring that case.”

“Amnesty International Vs. Clappert, clients of ACLU who want to know whether they're being subjected to warrantless wiretapping when talking to clients overseas. They may be talking to journalists, clients whose rights have been violated. The Gov is saying: you can't prove we're wiretapping you. So, you have no standing to bring the case. It's catch 22. It's not Orwell: it's Kafka. You can't get into court, to vindicate your rights.”

“I'm not a conspiracy theorist, but it's real. Howard Zinn is now in a terror DB. All these innocent people are being swept up in the DB, and local cops get access. We have fusion centers everywhere with no check and balance. In MA we have two. How do we put in some legal protections, so that we have the benefit of the technology, but enjoy the freedoms of this country?”

“For one, we need people like Binney, Tom Drake, Martin Klein (?) ATT guy, who are technologists, who spoke up about it. They understood what was happening, and saw that it didn't have to happen. We need you to do this. There will come a time in your life when you'll have to decide what to do. If you're not sure: call ACLU. We'll give you free legal advice.“

“We also need help from technologists. For example, when the Charlie Card came in, we said, shouldn't there be a way to have it anonymous? We met with the MBTA, they said "technologically that's not possible!" I had my guy from MIT, I pulled him out like in that Woody Allen movie. He said "no, that's nonsense!" So we need help with that: techs who can work with us and help us. We really do want to work with you and the MIT community.”

“The last thing: when you leave here tonight, talk to five other people about what you've learned. I don't think it's too late. How can we use technology to create more liberty, a greater breathing space? I think we can be both safe, and free.”

Q&A II

Shava Nerad, former ED of TOR Project: My dad was an activist with SCLC and Dr. King, that's how I came into this. When it was possible to request his records from the FBI, from 1963, he got a large paper box. The FBI knew who he had lunch with every summer. This isn't new, it's just electronic. It's been going on for a century, at least. One of the things that being ED of Tor did, my family has leadership positions in government, military, and activist circles. I got to talk to a lot of poeple on the agency side of things. After Patriot act, the people who wanted to respect civil rights and civil liberties, they would be trampled for every promotion in their work and left behind. And there would be no people with those attitudes at the high levels of any of those agencies. It happens in every branch of DHS, in Bush administration. Understanding that even people who deeply believe in these rights are forced into compromising their integrity.

Binneyl: They're being threatened and intimidated.

SN: people in these agencies aren't all jerks. They literally can't complain. They're prevented from talking about that.

Binney: Stellar Wind knowledge was limited to 4 people, to begin with. Nancy Pelosi, two Senators. Chief and ranking members of House and Senate intel committees. So, people have no way of validating these things, or monitoring them. They subverted our entire constitutional process.

SN: during the Bush administration, many people held on by their fingernails. Career diplomats gritting their teeth for 8 years, trying to swallow their bile.

Binney: it doesnt get any better with any party, it seems.

SN: Many of you may be thinking you never want to work for the government. But we may need to infiltrate. My son was working on Tor project, he looked at the problem from all sides and said 'if people of our viewpoint say 'none of our children will go into the military,' that's bad.

Carol: Whatever platform you're working on, you can make that a force for good. That moment may come when you know there's a tradeoff, a decision of conscience.

Q: It's always been my understanding that the outside of NSA community runs 10 to 20 years behind the NSA in encryption tech. Is that gap getting bigger or smaller? You said they can hold 100 years of data. Historically, we'd say

'we can go back tomorrow and break it.'

B: I can only give you my guess. I think the gap is closing. We're catching up. That's my impression. More in terms of capability.

Q: Everyone has been very careful to focus on the problems with extending these systems to US Citizens. But in the real world, don't they cause serious problems wherever they're implemented? For example, now we have a kill list, and drone strikes, ordered in secret by the executive with no due process. If you generate a kill list through these relationship mapping systems, and there's a false positive, and there's no checks? Not to mention that they're implemented through illegal drone strikes that kill civilians. The real world application of such systems always leads us to 'collateral damage' of one kind or another.

B: The drone program is terrible. It's very sloppy.

Carol: ACLU is litigating around the secrecy of the kill list: who's on it, how do you get on it or off it? We're also looking at the militarization of local police forces and their surveillance techniques.

Q: I feel bad for the thousands of people who are good guys, inside the government. The point is that, compared to other countries, such as the Soviety UNion, where I was born... it's too early to lose hope.

Q: over the weekend, they're talking about the Petreaus and Allen thing. Perhaps other public figures, particularly those in Congress, might wonder when the machinery will be targeted at them. Maybe they'll rein it in.

Bill: Pelosi said 'impeachment of Bush is off the table,' partly because she couldn't impeach him without impeaching herself.

Q: Clarification: we've been talking about the FISA amendment act. The problem there is that internal/external communications are being monitored. But it seems like a red herring, if all communications are being captured.

Bill: the problem is secrecy. We have no way of knowing what they're doing!

Q: Is there a boundary that prevents this warrantless tapping from entering the courtroom?

Bill: The tap they have on me, they entered it in an affadavit, and said I told them about that convesation.

Q: Where do you see this in 5-10 years, given the fusion centers and whatnot?

Bill: I've said in a number of forums that it's going towards a totalitarian state. We'll have an imperial president, and a dictator. Everyone in Congress is violating the constitution by supporting this activity. We have to throw it in their face. Put them on the record in public.

Carol: there was no environmental movement before 1970. We need to have a privacy movement. We should have control over the info about us. We should have checks and balances. The ACLU is conservative. We can take action. Send emails. Talk to people. Create a movement. Until we change the situation on the ground, we can't just go to the courts. We need a groundswell. I love the Petraeus thing, it's great - it's an opportunity to make some change. Every time there's an opportunity, we have to be educated, articulate, ready to speak about it.

Bill: As citizens of this country: what kind of country do you want? That's what's at stake here.

Q: I was wondering: how much of a threat are private surveillance systems, political surveillance, credit card surveillance, commercial systems.

Bill: credit cards, financial transactions, the standard used to be: if the transaction was more than 10k it went on the list. For 911, they transferred 60k for Atta's flight training. But they dont' analyze things properly, or pay attention. This is now coming back to financial transactions of US citizens. If you fall out of grace with the administration, that problem occurs.

Carol: In the EU system, you own information about yourself. Here, your ISP owns the info. Your banker owns your info. The only exception is video, which is an exception because it was done to a Supreme Court justice. In Europe, you own info about yourself, and the state needs permission. Here, you don't! The NSA just gets it. Now, county prosecutors can go without a warrant and get information about you. We need to change that 3rd party doctrine. I think it can make a big difference.

Q: I was thinking something much more mundane. An entity like Walmart, say, knowing the political proclivities of potential job applicants.
Is any of that stuff being done?

ACLU: companies do a lot of surveillance. Target has their own fusion centers where they monitor cameras from all their stores. They datamine customer information to figure out when women are pregnant and send them targeted

ads.

Moderator: Google and Target are corporations. If you don't like them, you can shop elsewhere. But we own our government.

Bill: Plus, the government can come point a gun at you.

Q: The word unconstitutional gets used a lot. But the Constitution is old, and vague. Could you speak about that?

Bill: It's not vague at all. Email is mail. Papers.

Q: That has to be determined by legal precedent.

Carol: I just read Amnesty vs. Clappert (?). The solicitor general says 'may it please the court,' and sotomayor says "who woul dhave standing then?" He couldnt' even get a word out. Sotomayor also wrote an opinion about tracking devices on cars; privacy advocates kept saying 'we could put this on your car, your honor!' We seem to be able to win more when we do that. The 4th amendment has been weakened, but the GPS Jones case gives us a little more daylight.

Q: You say "the data only on bad people" was used. What are the requirements for being bad? If I email my friend saying "the party will be the bomb?"

A: After 911, that system of acquisition was done away with. Now: everything is stored.

Q: Do you hold any hope for Sotomayor's line?

Carol: Gramsci says you need pessimism of the intellect, and optimisim of the heart. It's hard to be optimistic, but on some issues, like prviacy and speech, there's a bit more wiggle room.

Q: Could we say something about cell phone tracking? Most of us do carry cell phones.

Bill: I think there's still enough radiation to be detected by the towers. As you move around, that's still possible.

Carol: We have a legislative initiative, Ed Markey is helping us try to put restrictions on cell phone tracking, as well as license plate scanners. It's important for a lot of people to know they don't have to make a choice

Q: How much discretion to telephone companies have in refusing to comply with government requests?

Bill: The CEO of Qwest refused. It causes serious problems for them.

END

surveillance
nsa
wiretap
constitution