DANIEL MORGAN GRADUATE SCHOOL
of
NATIONAL SECURITY

presents

"Expectation of Privacy in the Digital Age"

Terry Roberts
Former Deputy Director,
Naval Intelligence

I come at privacy and national security issues from a little bit of a different perspective than people may think. Under my personal privacy hat, I am really in-the-box. I do not do Facebook or LinkedIn; I am a bit paranoid about it, because my personal privacy is very important to me. Of course, on the professional side, I have been out there for a long time. As I go to the next phase of my company, I have to have people who are going to manage the company's online face with LinkedIn, Facebook, Twitter, and all of that. Personally, I never share photos, except within a family group-share. I never share pictures of children; I have a whole speech that I give on social media security to executives and middle managers of companies. I am really in-the-box on the privacy side.

On the national security side: I know about the authorities that the national security community has, and the oversight regarding those authorities. I believe that we need to have a continuous discussion out in the open about them. I want law enforcement and the Intelligence Community, including the Department of Defense and Homeland Security, to have the ability to protect us. Many people talk about privacy and national security as though it is a balance, but I do not think it is a balance at all. I do not think that you can walk a balanced line.

I would like to walk you through a logic train of events in order to frame the discussion, then introduce some of the current statutes and precedents that we are operating under, and then delve into some specific areas. From this discussion I want you to understand that we have been talking about privacy and national security in black and white, and that is not helpful. We are saying both "I want my privacy," and "we have to have a strong national security capability," but those two things juxtaposed at a really high level is not bringing us down to a level of how we work day-in-day-out in specific circumstances. It is also important to look at what is realistic today; we are living in a dramatically different world than I lived in as a little girl.

We can start with some of the recent cases, which I will frame according to this discussion. The Anthem breach was the first time we lost personal health profiles at scale. Think of what you have in your health records: they would all be gone. With the Sony breach it was more about intellectual property: first their unreleased movies, and then executive-level communications. The one that really let the cat out of the bag, from the industry side, was the Panama Papers. With regard to law firms, there is a trust that they

---

This article is derived from remarks delivered at the Daniel Morgan Graduate School as part of the 2016 National Security Lecture Series on July 7, 2016.

have with their clients. Whether you appreciate who was outed or not, those are some of the most private business discussions; there could be mergers and acquisitions, business secrets, and financial secrets, among other things.

On the national security side, we have not done any better. Starting with WikiLeaks and Private Manning, then moving on to Edward Snowden and the files that were stolen from NSA, it is still not over. The OPM breach was a personal loss for myself, three times over: my background investigation from Navy, from National Reconnaissance Office, and from DHS. Fingerprints, and everything were lost. They went right to the Chinese, who want to use them against us. Then, there is the recent case of Apple and the FBI, which is slightly different: it concerns the appropriate relationship across commercial industry and government when it comes to a national security issue. So, what are some of the common threads across all of these things? It is that the precedents we are currently relying on for a lot of these circumstances are from the Nineteenth and Twentieth centuries. Very little of new precedent of any import has been created in this space and in this center.

One precedent in particular is illustrative of the privacy issue, because it is important to understand how we in the United States define "right to privacy." It comes from *Katz v. United States* from 1967. I like the way that it defines us in this space: "reasonable expectation of privacy is an element of privacy law that determines in which places and in which activities a person has a legal right to privacy." I may value my privacy, but I only have a "right to privacy" in certain circumstances. There are three aspects of this definition of reasonable expectation of privacy: one, the individual must have a subjective expectation of privacy. The individual has to believe that they have the right to privacy in communication, interaction, or discussion. Two, subjective expectation of privacy must be one that society is prepared to recognize as reasonable. Three, if either element is missing—the personal expectation, or societal expectation—then you do not have a reasonable expectation of privacy. The bottom line is that we need to establish a reasonable expectation of privacy in the digital age.

One of the examples that I give is from the old days when you had a switchboard operator either in a government headquarters, or in a big company. All of the calls came into the switchboard operator. So the switchboard operator knew who was calling, who they wanted to get connected to, and often they heard the beginning or ending of the conversation. While you had an expectation of privacy, there was a third party involved in every one of your discussions. Another analogy is a party line, in which two or three families shared the same phone line. They could pick up on your call at any moment, so you could ask yourself whether those conversations were private or not. It is similar to normal mail service. On the outside of a letter you know who it is going to, you know who it is coming from, and you know the date of the postmark. You have the externals of that communication.

Regarding work emails on company or government IT: do you have an expectation of privacy? If your boss owns your infrastructure, such as phones, devices, laptops, they own all the communications that are on them. Do you think that with social media postings within your established connections you have an expectation of privacy that your information will remain within that circle? No, because your friends can share things. If you are just searching and shopping online, is there an expectation of privacy? No, because we all get advertisements because they have been tracking our cookies. They know all of the websites that we have gone to and the purchases we have made, and they have a profile of us. Blogging is definitely not private, because you are putting information out there on purpose. On personal cellphone conversations where you own the device: do you have an expectation of privacy? Keep in mind the legal definition of a reasonable expectation of privacy: in the digital age, do we have a reasonable expectation of privacy in which both we as individuals as well as society believe?

Part of the reason why I think we want to define this better is because once we have a definition then we can put the right statutes, technologies, and protocols in place, to achieve that level of privacy for personal calls on our phones. By not carefully defining this in the eaches, then we are not moving to the belief stage. It is like the old saying: "if you are protecting everything, you are protecting nothing." If our expectation is that everyone has a right to privacy, but we are not doing anything about that, then we really do not have it. That is where we are now—we are fighting so much for it, that we do not have it almost anywhere.

Communications that impact a potential crime or terrorist act, such as a letter or communication from you that went to a known terrorist, are what the FISA law deals with. Law enforcement agencies can look at the externals of the communication, but not its content. They use this information to look for connections to known bad actors. If probable cause is found, they can then seek a court order to look at the content of the communication.

With regard to legal or financial transactions with a CPA or attorney, do you have an expectation of privacy? For that, I would say yes. When it comes to personal medical information, such as a personal consultation with your doctor, we have had a lot of breeches. This is because we have not consistently set up the technologies that allow us to put those files in an encrypted level of access, and then link it to a member number or a name. We really have not consistently come up with real rules, protocols, and basic approaches that you can put in place to protect medical information.

We should not treat all information the same way. We need to stop trying to protect everything online, because it is impossible. It cannot be done with any kind of certainty. Most of us who work in the field today know that the criminals are already in. If you have no protections in place in either your home infrastructure or office infrastructure, if you don't have cyber security protocols in place, or simply have old software or operating systems, then low-level crime and fraud actors can break into your system. If you have some level of cyber security programs in place, then it takes a more sophisticated actor to get in. But if you are a lucrative target, like a bank or a law firm, where it is worth them having some level of capability to get in, the assumption that we are making today is that they are already in.

Consequently, the real question becomes: what do you really need to protect? The analogy I like to use is your home. Right now, if you have an old operating system, then your doors and windows are open and your jewels and bonds are in your underwear drawer. If you have up-to-date software and regular patching and employee training, you automatically get rid of a lot of the low-level access. This has a lot to do with privacy. If you treasure your personal financial information, what you are working on, or what you are sharing and developing at work, and if you have an expectation of privacy because of all the reasons we discussed, then that is going to make a difference.

One of my friends started the Insider Threat Center at Carnegie Mellon University twelve years ago. Today, they have had over 1000 cases throughout the government and private industry. They have been able to model the behaviors of cyber criminals and can tell you how to easily put a program in place to secure information and technology. They can suggest the top five things to track without spending much money. These things are just business process things, such as alerting security before someone is fired, and taking them off the system so they do not have access before they are told; little things like that can make a huge difference.

We are not talking about getting rid of all cyber breaches and espionage, but, I think that we can get rid of eighty or ninety percent if we all buy in. If we stop trying to protect everything and stop thinking that everything we do online is not exposed, and is private, and try to protect all of it. That is when we start going into that death spiral.

Returning to national security versus privacy; again, let's go back to Apple. The intelligence community has Title 50 authorities: espionage, collection, and other things. And there is a regular and extreme oversight that includes intelligence oversight. Even when I was a junior officer I would have to go through an intelligence oversight inspection every year. You cannot detect, find, and disrupt the bad guys without these capabilities because they have no rules. So we need rules of law, and we need them to be realistic in the fact that if we know that a bad guy is communicating with an unknown entity, potentially innocent, that whomever they are communicating with means we need to look further. Do we want to know who known bad guys are communicating with? If we do, then it is about having the right frameworks in place. We have had a lot of the right frameworks, but they need to be tweaked, because this whole arena is moving at the speed of technology. I do not like seeing policies or statute that are technology-centric as opposed to function-centric. The Office of Management and Budget has a policy about multi-factor authentication, and fourth-factor authentication. Why would you drill down into inner agency wide policy as a guide, rather than state-of-the-art technology that will be released in an annual update? If proceed in this manner, you just cannot keep up with what is going on.

Law enforcement has authorities under the U.S. Code, to include showing probable cause for a warrant, regular oversight, and court system checks and balances. Currently, their authorities are based on the Federal Wire Tap Act of 1968. Think about that. Then, there is the Electronic Communications Privacy Act of 1986. The first was to address interception of oral and wire communications, and the second one to extend coverage to the response to the need of regulating interception of computer, and other digital and electronic communications. That last law has been updated twice. Additionally, these laws are very rarely taken to court. And that is my bottom line: we have old statutes, we have a desire to maintain privacy in critical areas, so we have to define what those areas are. I think we are already there.

We want our medical information to remain private, and we want our financial and legal transactions to remain private. We want phone calls on our devices, or emails on our infrastructure to remain private, unless there is probable cause for a reason to delve into the content. But we do not have expectation of privacy anywhere else, because it is not reasonable in the digital age. It is not supportable. Can society as a whole look at those instances and say: "Yes, we can deliver privacy in that area."?