EPISODE 489

[INTRODUCTION]

[00:00:00] AH: Okay. Well, it's great to speak to you again, Bart. I really enjoyed speaking to you the other month. Thanks for taking the time to speak to me this morning.

[00:00:07] BG: That's a pleasure. Glad to be back.

[00:00:10] AH: I think a good place to start is just tell us a little bit more about your book. What is your book? What is it you set out to do? What is the story that you're trying to tell?

[00:00:19] BG: Well, there are really three books here, three for the price of one. There are certainly three interweaving narratives. There's the question of who is Edward Snowden? What's he really like? What's he stand for? What's his history? Another is what are the things that you reveal? What are the principal features of the NSA that emerge from the Snowden leaks, from the tens of thousands of documents that he leaked? The third is what was my interaction with Snowden?

When I speak to readers, when I speak to audiences, the questions that are the most burning questions, the ones people are most interested in are how did he get in touch with me? What was it like to interact with him on this highly classified leak? How did we communicate securely? How did I know he was genuine? How did I know that the documents weren't genuine? What kind of pressure did I get from the US government? So I turned out to be a character in the book more than I had expected to be because those are the questions I get most often.

[00:01:34] AH: I would like to focus on each one of those main intersecting narratives. But just before we get there, one of the things I love about our podcast is the range of listeners goes from someone on their morning commute to Fort Meade who worked for the NSA to just your person who's interested in intelligence and espionage. So just really briefly, tell us what the global surveillance state is.

[00:02:01] BG: Well, the NSA had a legitimate problem as the decades passed. If you go back to the agency's predecessor back in World War Two, you had a Japanese general staff and a Nazi High Command, who communicated on their own bespoke communication channels. If you broke into those channels, there was nobody else there. You were guaranteed to get a Nazi. We're guaranteed to get member of the Japanese High Command. That way, your precision or targeting was near 100%.

As the years went by, much the same held true in the early years of the Soviet Union and other global adversaries or targets of interest. But as the global telecommunications networks evolved and the Internet came into being, everyone started communicating on the same channels. These networks were so efficient, and so much better than was within the means even of a government-sized entity to build on its own that more and more of the communications came on channels used by everybody. So the NSA had a problem. If you broke into those channels, it was potentially listening in on everybody, which wasn't its mission and wasn't something that we as citizens are going to want the NSA to be doing.

So the global surveillance apparatus evolved in order to be able to intercept any signal anywhere, anytime, and that's a frightening capability. It drives the NSA, for example, in the United States, to gather records of every telephone call made by anyone to anyone else anywhere. That is to say the call record data, who called, who drives the NSA to break into the Google cloud and the Yahoo cloud, where not only their own individual targets are communicating but literally more than a billion other people. So the global surveillance apparatus becomes very good at compromising more and more of the global communications traffic, which is not to say the NSA is pulling in all that traffic, but it's capable of doing so. It's pulling in more and more of it to evaluate whether it's interested. Its surveillance goes from being carefully targeted upon individuals in adversary networks to being bulk collection of high volumes of communications on networks used by everyone, and that's where the civil liberties concerns come in.

[00:04:59] AH: Okay. Just before I go on to each one of the themes, you mentioned the cloud there. For our listeners, would you recommend using the cloud? Or is it something that you personally steer clear of? Or give as your Bart’s wisdom for our listeners.

[00:05:15] BG: Well, somebody smart said the cloud, which is this vague term, and it evokes a sense of everywhere and nowhere at once. So the cloud is just another word for somebody else's computer. If you put something in the cloud, you were handing it over to someone else to take care of it for you, and that someone else does not have interests identical to yours, and that someone else can turn over your data to a government entity if the government entity asks nicely or with a force of law behind it. The cloud can also be attempting place for an agency like the NSA to penetrate.

On the other hand, the cloud has advantages. You don't have to worry about losing something because these cloud companies are very good at keeping backups. They generally have good security against ordinary level hackers and adversaries. There's value in it. I use the cloud mindfully. I put things there that are low value to me. I'm willing to put some of my ordinary working documents there, some ordinary personal ones. But if it came to medical records or confidential sources or even family photographs, I'd rather back them up by myself, and I put some other things in the cloud that are encrypted. I encrypt them on my computer and put them in the cloud as backup. But even if Google, for example, gave access to my account to an acquiring government, all they could get access to would be an encrypted blob that they had no passphrase for.

[00:06:58] AH: Thank you. Let’s zero in on each one of those strands that you pulled out for us at the beginning. So who was Edward Snowden, and what did he stand for or does he stand for?

[00:07:09] BG: He's a complicated guy. I don't like the sort of binary choice that were offered in most of the public accounts, which is a hero or a traitor. I mean, he's clearly not a trader in the literal legal sense of having transferred his allegiance to a foreign power to have decided that he wanted to harm the United States. You have to take seriously his claim that he believed he was doing something good for his own country. They believed he was supporting democracy. The fact that he's in Russia was an accident that was created by the US canceling his passport while he was changing planes in Moscow or while he was approaching Moscow to change planes. He had no intention of living there.

The senior officials I've talked to, who are most knowledgeable, who have access to current intelligence, including, for example, on the record, the deputy director of the NSA, have said they have no evidence and no longer believe that Snowden gave information to Russia. He didn't bring his documents with him, and there's no evidence that he's cooperating with Russia. He is an idealist. He is a zealot. I think I'd have to say he believes in black and white principles that don't always take account of nuance. I don't agree with everything he says or everything did, not by a longshot. We had quite a few arguments over the years and a lot of tension, but he's a guy who chooses his own path. He's an exceptionally intelligent man. He was bored by school and dropped out, earned his GED, meanwhile took college courses and advanced training courses.

So he, as a teenager, became a Microsoft certified systems engineer, which is difficult. He didn't even take the course. He just worked through the seven volumes of Microsoft, the information required to pass the seven separate tests that make you an MCSE. He did the same for a series of other high level credentials over the years. He came in through backdoors and chance opportunities. He rose up inside the CIA and the NSA because he was good at what he did. But he was, I would say, an uneven performer at work because he was impatient with rules and with supervisors who he didn't think were very smart. He took shortcuts, and he came to believe that the fundamental mission of the NSA and the fact that it was a global surveillance operation of the kind I've already described made it a threat to democracy, and that he had to do something about it.

There is a certain personality that's required if you're going to do something about it. I say that lots of people are dissatisfied at work or even have moral qualms about what they're doing, so they might quit. They might go along to get along. They may tell themselves that, "Well, everyone else is doing it. There must be something good here." They transfer to a different assignment. Most people don't tell themselves, "I've got to bring this thing down. I've got to tell the whole world what's going on." That's what I mean by zealot. He has a certain personality that did not permit inaction once he formed conclusions.

[00:11:01] AH: Just on Edward Snowden, I mean, I think it may be interesting just to blend the first part who was Edward Snowden with the third part that your interaction. So how did you first come across him? When is the first time you met him? When did you first hear his name?

[00:11:18] BG: Those are three different times, by the way. I was Snowden's third choice of a journalist, although he was happy to have three. He tried to get in touch with Glenn Greenwald. So Greenwald, as an ideological ally, as someone who was happy to take on the national security state, who saw himself as adversarial, and he thought he needed that because he was worried that a mainstream journalist would bow to government demands not to publish. He was afraid he would take all these risks and provide information to a journalist, and it would go nowhere. So he tried to get hold of Greenwald but he had to make contact by encrypting anonymous channels.

He reached out to me and he said, "Please learn how to use PGP encryption for email," and Greenwald ignored the emails. So he turned then to a filmmaker named Laura Poitras, who had herself been the subject of fairly intrusive surveillance. Every time she crossed a border, her electronics were searched. Her computer, her storage drives were imaged, and the government kept copies and so on. He thought she would understand the risks of a state that did too much of this. Laura wanted to collaborate with me. She convinced Edward Snowden that film can do some things, and print can do others. She got his permission to include me. So the first time I ever got an email from Ed Snowden, I knew that it was coming. I knew from Laura, who called herself Verax. I didn't know his name.

Verax, I looked it up, was Latin for truth teller. He assigned cover names for me and for Laura, so I was Bras Banner for some reason, and we used the most secure communications possible for a civilian to use. Everything was encrypted. Everything was accessed on the Internet through an anonymity network called Tor. So that if I logged on to a burner account, my communications pass through several global anonymous channels before they reached the server. So that even for the NSA, as we learned from the leaks, Tor is a significant barrier to surveillance. So it was an anonymous person at my end talking to an anonymous person at his end over encrypted channels. Gradually, we started a conversation.

[00:14:05] AH: At the time, just briefly give our listeners a sense of your background because you were at the Washington Post for a number of years, and this is one of the reasons why Snowden was initially a bit hesitant because, like you say, he thought that you're too much of a "sort of traditional journalist."

[00:14:24] BG: Yeah. I mean, Greenwald is a very loud advocate for the view that mainstream journalists are completely compromised by their interaction with government, that we are survival servants of power that go along to get along that value access overall. It is a cartoonish picture of what my profession does, and I had, in fact, spent most of my Washington Post career doing accountability journalism that held government to account for its behavior that pissed off the people I wrote about quite often. I mean, for example, I covered the first Persian Gulf War. I contrasted the videos that were released every day of precision bombs going straight down chimneys, exactly where they were aimed with the fact that 90 something percent of the tonnage of bombs dropped on Iraq that were done bombs, and that a large fraction of those had missed their targets. That was not something the air force wanted to hear, and that was fairly typical of the kind of reporting I was doing in those years.

Snowden decided to take a chance. I explained to him how I work and why the mere fact of government opposition to publication would not stop publication. I told him we would listen to arguments and we would withhold some things. He said that was appropriate because he didn't actually want everything that you reveal to the journalist to be revealed to the public. He was handing over a massive quantity of classified documents. He didn't want to put all that out there. If he did, he didn't need the journalists. All they had to do was post it on the web. Snowden knows how to work the Internet. He could have put it up in ways that would be very hard to censor with multiple servers around the world and so forth.

So he was sympathetic to the idea that we would judge for ourselves what to publish, and I think he thought in terms of engineering, as he was trained as an engineer, that if he gave the documents to three different journalists, he had three different shots at getting it out. That if his worst fears about me and The Washington Post proved to be true, then he still had Glenn and Laura. As it actually turned out, Washington Post did took a lot of chances and provided courageous and deep coverage of the leaks. Most of the stories did not depend entirely on the documents. They took the documents as starting points for reporting.

[00:17:17] AH: Just briefly, did you know Laura Poitras previously before she contacted you, or did she just know of your reputation?

[00:17:24] BG: I knew her a little. We had both been fellows at the same time at New York University in a program called the Center in Law and Security. She had come to me several years before the Snowden leaks because she was stopped at the border so often and didn't want her data to be open to anyone who searched it. So she asked me to teach her how to do encryption, which I was a relatively early adopter of that among journalists and had a reputation as paranoid I think and cautious about how I stored my notes. So I taught her how to use encryption and connected her with other experts.

When she was now in correspondence over encrypted channels with a national security source, and she still didn't know his name or didn't know for sure where he worked. She also knew that in my previous book called *Angler*, which was about Vice President Cheney, I had two chapters about secret warrantless surveillance and had learned something about the way the US government does that sort of thing. So she thought, "I know he knows encryption. He's written about this stuff before," and decided that I might be a useful partner.

[00:18:53] AH: I wonder if you can just join the dots for our listeners about Edward Snowden as a whistleblower, in relation to the global surveillance state compared to former eras where you had maybe someone like Mark Felt, very senior, is working with the Watergate reporters from the Washington Post. It seems to me that like in a former era, particular types of people would have access to particular types of information. But, no, someone likes Snowden or Chelsea Manning. Even in possessions, not as senior, they're able to nevertheless get access to a huge amount of information. It seems to me that that's a product of the information age and the kind of times that we live in. So I just wondered if you had any thoughts on Snowden, the types of information that he was able to get, given his position, and if you can tie that into the rise of the surveillance state.

[00:19:59] BG: Right. That's a very perceptive question. It's exactly right. There is a parallel in the information age between the NSA's reach and the asymmetric threat it faces from the inside when you no longer need to be a top ranking official to have access to highly sensitive information. Mark Felt, who was – For those who don't recall, he exposed as Bob Woodward's source, Deep Throat, in Watergate leaks, was a top FBI official, second or third ranking official at the FBI. The information he gave Woodward came largely in the form of clues and hints and

vague injunctions. “Follow the money,” he would say. He didn't hand over documents and didn't provide very many specifics.

The nearest old-fashioned precedent for the Snowden leaks was Daniel Ellsberg. Before Watergate, during the Pentagon Papers story, who turned over – I think it was seven volumes of an official history, classified government history of the Vietnam War. This was many thousands of pages, and he had a photocopy of those volumes laboriously. The photocopier in those days weren't the high volume modern equivalents, sort of flip the page down, push a button, and **[inaudible 00:21:33]**. Wait and then it was like **[inaudible 00:21:36]**. The whole thing took 10 or 15 seconds. Now, you've got one page and you did this 7,000 times. In fact, he made several copies. He made one for our relations committee, one for the New York Times, and another one for The Washington Post. In order to convey those, he had to physically transfer a large box of paper weighing quite a few pounds, and that's how he conveyed that much information.

When it comes to Edward Snowden, he could fit orders of magnitude, more information, onto a micro SD card the size of a finger nail. I'm not saying that's how he did it exactly, but that's what the capacity would be. He was able to access all that not because he was a very senior official at the NSA. He was very far from it. He was, however, cleared for many of the most sensitive compartments in the compartment intelligence system. So we had top secret clearance, which was the least of it. Then he had clearance into the major compartments for communications intelligence, signals intelligence, geospatial intelligence. Even because he had previously been at the CIA, he had clearance for some compartments in human intelligence, the work of spies.

Perhaps most dangerous of all for the NSA, from its point of view, he had the third and highest level clearance as a system administrator, so he actually had root access to most of the NSA systems, meaning that he could change the fundamental workings of the operating system and could not only open documents I think he had official access to. But he could get around the defensive systems and the security compartments that prevented someone without access from obtaining access. He could do something that the vast majority of people at the NSA cannot do, which was he was able to find workarounds that enabled him to copy information from these secure systems to an external storage device, which allowed him to take that information home and to convey it to journalists. Really, it's a hard problem for the NSA to protect yourself against

someone who has these capabilities. But a high level, a third tier system administrator needs those capabilities to do the job.

[00:24:25] AH: I find the possession of a systems administrator really fascinating. I remember speaking to a former FBI counterintelligence official, and he said that one of the main targets that you would have in an embassy would be the cipher clerk because although they may be relatively junior, they set astride communications, and therefore we can get a lot of important information. I guess if you think about it logically, the more senior someone gets, it's not a perfect mechanism because people like Mark Felt or **[inaudible 00:25:01]**. But the more senior someone gets, the more time they've spent. The more wedded they are the institution and its ideas.

I guess there's just been a much longer vetting process that you can bring in a systems administrator. After a number of years, they can be accessing information that someone may have taken a whole career to get access to. So I think that there's an interesting parallel there between the cipher clerk and the old skill human intelligence and the modern kind of information age. So I just wondered, some of our some of our listeners will know a lot about this. But for people that don't know, what is a systems administrator? Why do they have access to so much information? Can you help us understand that a little bit more?

[00:25:47] BG: Well, there's a lot of really interesting stuff in that question. I haven't ever thought of Snowden as sort of super empowered cipher clerk, but the analogy holds to some extent. The big shots come and have an urgent and confidential message to send. The cipher clerk has to turn that into encrypted code that is transferred back and forth, and so necessarily it has to be able to read it and knows who sent it and when. That's all valuable. Snowden had that capability and also the capability which a cipher clerk doesn't of going out and finding information on his own that he was interested in. So he could browse or search, whereas the cipher clerk has to wait for someone to send a message.

What a system administrator does is to take care of the systems and more importantly the networks of systems function properly. These are immensely complicated machines. For example, the global telecommunications network has been described, I think. I think this is indisputable as the most complicated machine ever built by humans, with sort of a near infinite

number of switches and computers and junctions and complicated code that runs it. So inside the NSA, you have people who are cleared for this and not that people who have to be able to write to a certain database, people who should only be able to read from the database. You have systems that are feeding in vast quantities of new information, processing that information, parceling it out for analysts to analyze their output. Everything has to follow its own channels, and everything has to work. You can't tolerate downtime in systems like that. So a system administrator, in order to keep that network running, has to be able to have access to all the elements within it, and that's what makes a system administrator so dangerous as an internal security threat.

[00:28:05] AH: I was just thinking when you were talking there. Just to play with the analogy just a little bit more, it seems like Snowden was a super empowered cipher clerk, who could also just turn up to the archives. If you think of the old and former era, he could also just turn up to, say, the MI5 archives and start looking through their files to see what he came across. But he could do all of that just by sitting at a computer, and he could make it anonymized. So it's a really fascinating kind of position to be in, I think.

[00:28:40] BG: Right. Well, I mean, Snowden upended the NSA business model because the NSA's job is to keep US government secrets secure and to steal other people's secrets. Snowden burst through the security, and he stole the NSA's secrets. He was almost a kind of jujitsu.

[00:29:02] AH: I think that the 20th anniversary of 9/11 is coming up. After 9/11, we have the 9/11 Commission report, the ODNI. We need to stop information being siloed. We need to share it more. Then the Snowden story breaks that you're a big part of. Then it seems to me that the pendulum starts to swing back the other way. So I just wondered if you had thought about how this book and how the story of Snowden fits within the post 9/11 intelligence landscape.

[00:29:36] BG: That's interesting. The 9/11 accentuated a trend that had already been rolling along quite strongly, which was this sort of enormous expansion of the classified universe. As early as the late 1990s, there was a Harvard political scientist named Galison, who estimated that there might now be more data in the classified sphere than in the unclassified. That is to say more than the entirety of the Library of Congress by volume was classified. There were

times Snowden did what he did, some 4.1 million people who had classified clearances. So people in the national security community sometimes complain that they can't keep any secret, that there are leaks of everything, and that's just plainly not true. I mean, the vast, vast majority of this secret world stays secret, stays on the high side, as they call it, the classified channels. So you had this vast expansion of what was classified. In fact, there were, after 9/11, large swaths of data from government websites that were taken offline and classified retrospectively in order, for example, to protect critical infrastructure.

There was also, as you say, a strong trend towards sharing intelligence more widely across agency boundaries. So the result of that was that Snowden not only was able to see NSA secrets but secrets from the CIA and from others of the agencies in the, at that time, I believe 14 intelligence agencies and an operations around government because they were linked by a secret network and a top secret network that did not carry the most sensitive secrets but quite a few sensitive secrets across agency lines. I mean, the very most sensitive secrets were kept offline in air-gapped systems, and Snowden seldom had access to those. But there was a pretty broad universe of information that he was privy to in part because of the post 9/11 relaxation of agency boundaries.

[00:32:02] AH: I think it would be interesting at this point to move on to the types of things that Snowden revealed. Yeah. For our listeners, some of them again will be very up on the story, and other people maybe a bit rusty — they may be coming across it for the first time. What did Snowden do? So all of these documents and journalists involved as intermediaries and getting the story out, like help us understand the contours of what Snowden did.

[00:32:32] BG: Sure. Honestly, even for the best informed people, I would like to challenge what has become conventional wisdom about Snowden, which is that most of what he revealed, according to this account, was nothing to do with civil liberties, nothing to do with US citizens, and was just gratuitous revelation of foreign intelligence capabilities. I've challenged that because I had to make the decisions myself about what would be published. That is to say if I wrote about it, I was making an independent judgment that there was an important public interest served. There were a lot of things I held back. There were a lot of things that had only to do with foreign intelligence gathering or that identified foreign targets or that identified especially

sensitive US government capabilities that I held back and did not publish. Some of those things were not published anywhere and remain secret.

But the conventional view was that only the collection of call data records of Americans by the NSA was a civil liberties issue. That is to say when you doubt a number of the NSA kept a record, working with the FBI, who you dialed and how long you spoke and when this happened and the social networks that you can build with comprehensive data set like that are enormously revealing. There was a sort of reluctant admission by people in the intelligence community that, yes, there is a civil liberties concern about that, even though many of them would defend the collection. Many of them also said that it was unnecessary and not as it turned out especially valuable against terrorism, which was the declared purpose. Even more said, that it should not have been kept secret, and that by getting caught with his pants down on this, the NSA had helped foster an atmosphere of mistrust. But everything else according to this view was gratuitous.

Now, there was also a program, the first one that I revealed, called PRISM by which the NSA obtained content, not just metadata as in the telephone records but the content of communications that were carried and stored by the large Internet companies. So everything in your email account at Google, every document that you stored on Microsoft OneDrive, everything that you – Every photograph, every spreadsheet, travel document, and so forth were vulnerable to interception, using the PRISM program. It was targeted. It was not a bulk surveillance program but it was used on such a large scale that I was able to show that it swept in the communications and the personal data of nine bystanders for every target. So 9 out of 10 of the communications that were intercepted in the very large scale PRISM program were, to put it another way, innocents, people who the NSA had no reason to believe were valid foreign intelligence targets. They simply got swept in.

The name for that in the intelligence world is incidental communications. That you're trying to get one thing and you incidentally pick up others. But incidental doesn't mean accidental, and it doesn't mean unintended even. It certainly doesn't mean unwanted. The NSA didn't take this stuff and say, “Oh, 9 out of 10 of these I don't need,” and throw them away. The NSA kept them and put them into its bulk storage systems and analyze them, just in case they turned up anything interesting later. They also share that information, for example, with the FBI, which

used them routinely in its domestic investigation. So that meant that information that the FBI would not have had access to with a warrant because it couldn't show probable cause for anything, the FBI, incidentally, had in quite large quantities.

But then take some of the foreign operations. These are the ones that critics of Snowden, critics of me, would say had nothing to do with Americans at all and nothing to do with civil liberties issues. It was simply a spy agency doing what spies do, which is to surveil foreign targets, and it's all totally legitimate. But if you look at the way the NSA did it, which is often bulk surveillance techniques, the rules say, and I'm not saying the NSA broke any rules, the rules say if you intercept something overseas, you're allowed to presume that these are foreign communications. But if I were to send an email from here in New York to you in Washington, Andrew, that email would certainly, because of the way the Internet works, cross over international boundaries and be stored in Singapore and South America. Because let's say I use Gmail, Google has a globally distributed network that based on traffic may serve your account from Ireland, even though you're a lot closer to a data center in the United States, and it will store backups overseas. So if the NSA is intercepting things in Ireland, for example, it's going to get your data. It's going to get my data. I am a US person and entitled to constitutional protections, and the NSA is allowed to presume that I'm a foreigner but I'm not.

When the NSA breaks into the Google Cloud, when it collects, on a bulk basis, all address books to pass global junctions of the Internet, when it collects all the location data that it can get of mobile telephones around the world, it is, in fact, collecting American data. That's not to say that it needs to stop doing all those operations. But the debate has barely even begun about how you protect the privacy of your own citizens when you're doing operations like this. What are the boundaries of secret intelligence in a democratic society?

[00:38:58] AH: I think that's a great question, the subject of a future SpyCast? I can almost predict with this podcast, there's going to be people that say, "Well done for challenging the Papa knows best attitude." Then there's going to be people at the other end of the spectrum saying, "What the heck are you thinking of having Barton Gellman on SpyCast? He abetted Snowden to undermine US national security." So I just wondered, I guess it's just an opportunity for you. For the variety of listeners out there, like help understand a little bit more about how you, Barton Gellman, an American journalist, someone that's interested in civil liberties and the

boundaries of secret intelligence and our democratic society. Help them understand where you're coming from a little bit more.

[00:39:53] BG: A less polite way of asking that question might have been who the hell elected you to decide what secrets should be spilt. The US government put a classified stamp on it, and some people would say that should be the end of the matter. It needs to be a secret and the duly elected government has said so. My argument is that that is a way to answer the question and that, in fact, many people who say it would agree in the end that it does not withstand analysis. If the president can prevent the public from knowing anything he wants on an arbitrary basis by putting a stamp on it, the president can avoid accountability for things that the public would strongly disagree with.

For example, the US government committed torture during the war on terror, and that was all highly classified. If the classification boundaries had been respected, we would not know that there were secret prisons overseas that were doing things to human beings that violated not only our moral standards but our laws. If you say that classified boundaries trumped everything, they must be respected no matter what, then you're accepting that torture is permissible, as long as no one knows about it. You're accepting that something that the great majority of Americans would never authorize is authorized to the government. So the whole idea of popular sovereignty is undermined.

The US government, using in classified programs in previous decades has deliberately infected US servicemen with sexually transmitted diseases in order to see what they look like when they progress untreated. The US government deliberately exposed the US servicemen to nuclear radiation to see what's the effect on the human body. There's a long list of things that were quite serious and damaging contrary to law and contrary to common sense that the US government convinced itself it should do and should place a stamp on. If you think classified boundaries to be respected no matter what, then you're accepting those things.

On the other hand, there's a vast, vast volume of information that is classified unnecessarily. I've seen a classified US Navy laundry manual. This is how you wash the clothes before the warship. The procedures are laid out in great detail. This much soap and so forth. It’s classified secret, which means that somebody wielding the stamp was supposed to have decided that

revealing the soap to water ratio in US laundry would do serious damage to national security if it were revealed. I mean, that defies any rational defense, and there are all kinds of reasons and incentives that cause people to stamp things classified when they're – I mean, I've seen copies of my own newspaper stories that were classified. They'd already been published to millions of readers, but it was a violation of law to disclose them if you read them inside a government information system. This kind of thing makes no sense.

So I'm not saying that every classified secret should be revealed, very far from it. If I find out something that is a secret, I always go to the government, to the responsible agency, and have a conversation about it. Sometimes, I already know without asking that I'm not going to publish it because it's just clearly gratuitous and clearly damaging. There are times when I don't realize how sensitive something is or why. A good government official will sometimes tell me something that I don't know in order to explain to me why something I do know should not be published, and those tend to be successful. But there are times when people say, “You shouldn't publish this for a reason that I can't accept.”

For example, when I had the list of US Internet companies that were subject to the prison surveillance program, the Chief Counsel for the intelligence community, the General Counsel for the Director of National Intelligence, Bob Litt, said to me, “You shouldn't publish the names of those companies.” I said, “Why?” He said, “Because when you publish the names of those companies, they're not going to want to cooperate with us anymore.” I said, “First of all, they're obliged by law to cooperate with you. Second of all, if your reason for keeping a secret is that the American people won't like something, and therefore companies sensitive to its customers will not want to do it, that's not a reason for me to hold back. If you believe in the popular sovereignty of the American people, then you can't hold something back from them because they wouldn't like it. Quite the opposite, that's a reason to publish.”

[00:45:00] AH: I wondered if you could tell our listeners as well, what are some of the personal things that are – Or what are some of the things that you do or you would advise when going online? Do you always use Tor? Do you use an encrypted email? Do you always use signal when you're communicating? Help us understand just the basic kind of protocol and procedures that you follow to keep your own communication secure.

[00:45:30] BG: Well, the measures I take are not for everyone. Everyone has to consider their own threat model, which is what are they trying to protect, who might reasonably be expected if you're trying to penetrate that protection, and what are the stakes. Is it life and death? Is it embarrassment? Is it just ordinary keep out of my business privacy? Because I had the Snowden documents, I've been an interesting target for foreign intelligence agencies and for sophisticated hackers. So I kept that material and my notes about that material offline, on air-gapped systems. I communicated about them only on encrypted anonymous channels and so forth. I've got them in cold storage now in a place that would be not easy to find. If they are found, they're encrypted. The encryption keys are kept somewhere different from where the documents themselves are.

For my ordinary day-to-day communications, I much prefer to use encrypted channels just for ordinary privacy. So I communicate with friends and certainly with ordinary journalistic sources using something like Signal, which didn't exist during the Snowden leaks but is very good encryption and just as easy to use as a text message. Signal.org, I strongly recommend it. I keep my personal files, my tax returns, my family photos on an encrypted computer so that if someone were to lift the computer, steal it from me, they wouldn't be able to get access to that stuff. I'm mindful about what I put in the cloud and what I put in the cloud. Backup is an important part of security because you can lose something to a fire or to a system error. So keeping a multiple set of backups on the hard drives, as well as some stuff in the cloud, is important.

I use Tor when I am browsing or communicating about something that I consider highly private. It might be that a friend or family member has a medical condition that I want to know more about, and I don't want to advertise to the great gods of Google that I'm interested in this or that disease. I don't want to be on database like that. I use DuckDuckGo as my search engine rather than Google, because DuckDuckGo is not building a profile of me and storing data about what I searched for and where and when and so forth. These are all just ordinary sorts of precautions that anyone can take.

I use a VPN for security to avoid being hacked primarily and to avoid telling my Internet service provider every spot that I visit on the Internet. I'm trying to think what else would be useful to mention. For security, the most important single thing you can do is to update your software.

When you get a notice from Apple or Microsoft that your operating system needs updating or from Adobe or from whatever other software company, update it right away. Don't sit around waiting. Just about every update includes security improvements, and many of them are because there were security threats detected in actual use in the real world, and they close those holes. If you don't update, those holes are still over for you.

In fact, this gigantic Russian hack of thousands of government and corporate computers relied on the fact that the initial entry points were using Microsoft systems that were not updated. The updates have been published and were widely available, but system administrators have not got around to updating them. So turn on automatic updates and do that habitually, and you're already ahead of the game security wise.

[00:49:40] AH: Okay. Are you still on the radar of intelligence agencies, either domestic or foreign? Or maybe that's not something you want to talk about. I know that in a previous event, we spoke about this a little bit. But, yeah, help us understand what it's like to be you. How do you not end up like in the movies, just on your closet scraping through everything, looking for secret buts, and so forth?

[00:50:08] BG: Well, during the height of this story, I had definitive knowledge that I was targeted for surveillance. I mean, I watched my iPad hacked in front of my eyes. It rebooted itself into root and started replacing the operating system and installing spyware that I could see scrolling across my screen because they had made a mistake on their end. It did things that should not have been visible to me in a way that was visible. Google notified me that there were attempts to compromise my account in my machine from a state-sponsored actor. I heard the same from US government sources and so on. I mean, I talk about these in detail in the book, and it's a very interesting sort of spy versus spy story. So I was always changing equipment and improving my security measures. It got to the point where I was carrying my computer with me everywhere, not because I was carrying around the secret data, but because if I left it alone, someone could implant a device that would defeat my security, that would steal my passwords and so forth. The computer technical people call that the evil maid attack. Imagine that you leave your computer in your hotel room and you walk out for 20 minutes, the evil maid comes in and does something, and you're compromised.

I became quite paranoid, and it was hard just to live an ordinary life. It was inconvenient and embarrassing for my friends and family. It was a huge tax on my time. I mean, if you have to type five or six long passphrases and get the equipment out of the safe before you can start work every morning, that's what I had to do at the time. I've relaxed my measures considerably, now that the Snowden documents are in cold storage, and they have aged out of intense interest. I think, at this point, eight-year-old documents, many of which have been revealed, don't have the same appeal that they did at the time.

[00:52:25] AH: I mean, I guess the final question would just be some of the people that listen to this are also going to say, “Well, why didn't Snowden go through the proper channels internally and those kinds of things?” So I just wondered if you had any thoughts on Snowden as a whistleblower versus Snowden as someone that tried to change the system from within.

[00:52:47] BG: Yeah. I don't actually love the term whistleblower because there are whistleblower laws that define the subject that whistleblowing as a waste, fraud, and abuse. So there's a relatively narrow category of facts that are considered legally justifiable to blow the whistle on, whereas you can't blow the whistle on an agency using internal processes by saying, “Good God. Man, a whole big swath of what you're doing is illegal. It should be.” Sometimes, the scandal is what's legal. Sometimes, people have evolved behaviors and operations and beliefs inside a closed system without subjecting those beliefs and behaviors and operations to the perspective of an outsider who would say, “What the heck do you think you're doing here?”

I think it's inarguable that NSA, because of what it considered an inevitable incursion into the digital commons that we all use, did not fully consider the civil liberties implications. Although it followed the rules in all cases, as far as I know and I give credit for that, the rules were not adequate and needed to be rethought. There's controversy over whether the Whistleblower Protection Act would have covered Snowden as a contractor. I think it probably would not, this controversy of whether he raised alarms inside the system. He certainly didn't go through all the procedures. But I don't know anyone who would say that we could have had the public debate we had. That debate, according to lots of senior people, Jim Comey said it to me on the record from my book. So did James Clapper and others. This was a valuable public debate about what the norms should be in intelligence collection. I don't see anyone who could tell me how that

debate could have happened if Snowden had simply gone through internal procedures, challenged fundamental aspects of what the NSA was doing and squashed.

[00:55:01] AH: Okay. Well, I could speak to you for hours, Bart. But thanks so much for your time.

[END]