

# Filling the Blanks in Snowden's 'Citizenfour'

**Exclusive:** To grasp the full story of *Citizenfour*, the documentary on Edward Snowden's decision to expose NSA spying, you must go back four decades to see how the reality slowly dawned on Americans that their privacy and freedoms were at risk, writes James DiEugenio.

By James DiEugenio

In 1974, at about the time President Richard Nixon was resigning due to the Watergate scandal, director Francis Coppola released his haunting, compelling film about electronic surveillance, *The Conversation*. Centered within the lives of surveillance technicians and the powerful corporate officers who employed them, Coppola depicted a nightmare world: one fraught with the invisible threat of electronic spying at almost any place, at any time including in public parks and inside private hotel rooms.

The film had a remarkable double twist at the end. The protagonist, played by Gene Hackman, has found out that, unbeknownst to him, the people who hired him used his work to stage a killing. In turn, they find out about his dangerous knowledge. The long last scene depicts Hackman literally dismantling his apartment, trying to find the microphone his murderous employers have placed in his room.

Coppola has said he never realized his film would play out against the backdrop of the Watergate scandal, which also had electronic surveillance at its center, this time politically, with the Republicans spying on the Democratic campaign headquarters for the 1972 presidential race.

In the wake of the Watergate imbroglio, some of the people on the Watergate Committee, such as Sen. Howard Baker, were not satisfied with the congressional investigation led by Sen. Sam Ervin. Baker felt that the role of the CIA in the two-year long ordeal had been glossed over.

This, plus the exposure of CIA counter-intelligence chief James Angleton's domestic operations, gave birth to the Church Committee, headed by Sen. Frank Church, D-Idaho. It was the first full-scale inquiry into the crimes of the FBI and CIA.

As a result of the publicity given to that committee (back then such events were actually covered in the U.S. news media, not mocked and ignored), some reforms in the monitoring of the intelligence agencies were enacted. After these reforms were put in place, the Senate decided that there should also be some limits and

controls placed upon electronic surveillance over alleged threats from domestic enemy operatives inside the United States.

### **The Birth of FISA**

Therefore, a handful of senators, including Ted Kennedy, banded together in 1977 to pass the Foreign Intelligence Surveillance Act. The act allowed for surveillance of up to one year without a warrant over foreign targets. If one was not foreign, but an American citizen, a warrant had to be granted within 72 hours.

There was an eponymous special class of courts known as the FISA courts set up to deal with these cases. To review and issue the warrants, 11 judges are chosen by the Supreme Court for a period of seven years. When deciding to grant a warrant, the court usually consists of three judges.

The idea was that no American should be spied upon unless the government showed some kind of "probable cause" that the American citizen was an agent of a foreign power or terrorist organization. In other words, the judges were to provide some safeguard against unwarranted and unjustified spying by the government, albeit with their deliberations in secret and without an adversarial proceeding.

Frank Church had seen the awesome power of the FBI, CIA and NSA up close. He had seen what people like longtime FBI Director J. Edgar Hoover had done to Martin Luther King Jr., trying to coerce the civil rights leader over his personal life. Church had been exposed to MH CHAOS, the CIA's domestic spying on radicals and the alternative press in the 1960s and 1970s. He had seen the documents on COINTELPRO, the FBI's program to infiltrate and then undermine leftist, activist groups like the Black Panthers.

And Church had been one of the first outsiders to get an in-depth look at just what the technological capabilities of the National Security Agency were. Even back in 1975, Church was very much impressed and, at the same time, he was quite fearful. He made the following memorable quote in regards to the powers of the NSA:

"If a dictator ever took over, the NSA could enable it to impose a total tyranny, and there would be no way to fight back. That capability could at any time be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide.

"I don't want to see this country ever go across the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this

agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.”

### **Spying on Dissent**

Those comments were probably made because Church found out about Project Minaret, an early and limited attempt at domestic surveillance which targeted the communications of famous personages who criticized the Vietnam War, e.g., himself and King.

Project Minaret lasted from 1967 to 1973 and ended up targeting about 1,650 American citizens. These names were on Watch Lists made up by the executive intelligence agencies. There was no judicial oversight and no warrants were obtained.

With this in mind, Church, Ted Kennedy and others were seeking to balance the threat of domestic infiltration by foreign powers with some semblance of legal strictures to protect our fundamental freedoms, so that Coppola’s Kafkaesque vision did not become an American reality.

This imperfect balance was maintained for about two decades, from the creation of the FISA courts in 1978 to the start of the new millennium. Very few people had ever even heard of FISA courts or understood what they did. Then came George W. Bush and the Al-Qaeda attacks of Sept. 11, 2001. As the saying went, “everything changed.”

The vast expansion of the NSA’s spying began within a few months of those attacks. But the American public did not know about it until December 2005. In fact, President Bush appears to have lied about the program in public when he made two speeches in April 2004 in which he said any wiretaps his administration employed necessitated a court order.

He then added, “When we’re talking about chasing down terrorists, we’re talking about getting a court order before we do so.” He made the same claim at least three other times.

Then on Dec. 15, 2005, the *New York Times* published a story that revealed President Bush had allowed the NSA to “eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without court-approved warrants.” One source for the story said, “This is really a sea change. It’s almost a mainstay of this country that the NSA only does foreign searches.”

The story was written by James Risen and Eric Lichtblau. And it was revealed that the *Times* had sat on it for more than a year. Why? Because the White House

pressured the newspaper not to print it. [See Consortiumnews.com's "Spying and the Public's Right to Know."]

### **Scaring the Times**

Bush and his aides had used all kinds of intimidation tactics to keep the story out of print. From saying the paper would be held responsible for any upcoming successful terrorist attack to threatening another Pentagon Papers-style lawsuit.

A key reason that the *Times* changed its mind and published the story in December 2005 was that Risen was including the information in his book, *State of War*, scheduled for release in January 2006. The *Times* editors judged that the potential embarrassment from continuing to sit on such a newsworthy story outweighed the risks of offending the Bush administration.

The hidden controversy about the story reveals that a number of people inside the NSA and the Intelligence Community were disturbed by what Bush had authorized them to do. And although Risen and Lichtblau used anonymous sources, the government apparently suspects that one major source for them was Justice Department lawyer Thomas Tamm and another was Jeffrey Alexander Sterling, a CIA operations officer.

Sterling is now under indictment for violation of the Espionage Act. Tamm's house was raided by the FBI in 2007. Charges were not filed against Tamm, although the investigation continued until 2011.

It turned out that the release of the *Times* story and the subsequent legal skirmishes over the whistleblowers set a pattern in this legal area. Contrary to popular belief, Edward Snowden was not the first NSA employee to reveal the illegality of classified programs in the wake of 9/11, just the highest profile one. The drama around Snowden's revelations also reflected the reality that, as the years rolled on, the scope of NSA spying grew exponentially.

The program that Bush authorized in late 2001 was titled STELLARWIND. It allowed "data mining" of Internet activity, e-mail communications, phone calls financial transactions. The fact that this was done on a massive scale precluded the formal vetting done by a FISA court.

Bush's rationale for this program was that the U.S. had failed to stop the 9/11 attacks because its defenses were too timid, not aggressive enough. For instance, in the year 2001, FISA granted 932 warrants. What Bush was doing dwarfed that.

STELLARWIND was briefly discontinued in 2004 when Deputy Attorney General James

Comey refused to renew it while his boss John Ashcroft was in the hospital. To his credit, when visited in the hospital by Bush's representatives, Attorney General Ashcroft himself refused to sign. Bush then got FISA court chief judge Collen Kollar-Kotelly to approve the program – 30 months after it started. (*The Guardian* June 27, 2013)

## **A Mainstream Scandal**

With the release of the *Times* story in December 2005 and Risen's book, *State of War*, a month later, the controversy was propelled into the major media onto the front pages and into the lead stories of TV news shows. That's when the real trouble began.

The divisive issues were those of civil liberties, civil disobedience and the fundamental one: were what FISA, Bush and the NSA doing constitutional? Or, if under the cover of an undeclared "war on terror," were Frank Church's fears and Coppola's nightmare vision now coming to fruition?

William Binney was one of the very first to protest from the inside in the wake of the *New York Times* story. Binney had 32 years in the NSA and was considered one of the finest cryptographic analysts they had. He had devised a program called THINTHREAD against incoming foreign communications. But the Bush White House ordered the NSA to drop the privacy controls on the program that guaranteed Americans would not be surveilled.

Since Binney understood that spying on Americans was illegal without a warrant, he and his friend and colleague Kirk Wiebe began making unwelcome entreaties to Congress and the Defense Department, even a Supreme Court justice. (*Vanity Fair*, "The Snowden Saga" May 2014)

As a reward for "going through channels," Binney and Wiebe were flagged as leak suspects with their NSA superiors steering the FBI in their direction, Binney said in an email to me. Binney added that the NSA "apparently got our names from the DOD IG's [Inspector General's] office – as we were the ones to file the DOD IG complaint about NSA fraud waste and corruption." (Bureaucratically, the NSA is under the Defense Department.)

Binney had his house raided by FBI agents. He was dragged out of the shower with a gun aimed at him. The excuse for the raid was the agents were looking for the sources for the *New York Times* story.

## **NSA Whistleblowers**

Thomas Drake was another NSA official who had complained about NSA abuses to other government agencies. He then went to the newspapers, specifically the

*Baltimore Sun*. Drake was formally charged under the Espionage Act of 1917. The government had no real case under that statute, but the expense and time of the legal ordeal essentially broke up Drake's life. Today he is employed by an Apple Store. (ibid)

But the role of Drake goes much further than the *Vanity Fair* article took it. That article stated that Drake had exposed waste, fraud and abuse at NSA, which is only part of the story. He went much further than that.

In a memorandum sent to President Obama on Jan. 7, 2014, predating the *Vanity Fair* piece, Drake revealed a major reason why he was charged and why others, like Binney, resigned. This memorandum was signed by Binney, Drake, former NSA division chief Ed Loomis, and Kirk Wiebe, former NSA senior analyst. To my knowledge, *Consortiumnews.com* was the only outlet that has printed it in its entirety.

The document states that National Intelligence Director James Clapper lied to Sen. Ron Wyden on March 12, 2013, during a formal session of the Senate Intelligence Committee. Wyden asked if the NSA collected any type of data on millions or hundreds of millions of Americans. Clapper replied in the negative. Yet this collection was going on since STELLARWIND.

What the memo revealed was that the whole public scandal about STELLARWIND was unnecessary because Binney, Loomis and Wiebe had devised a much better program called THINTHREAD. This did much the same thing, but it had encryption formulas entered into it so that records relating to American citizens would remain secret at least until a FISA court could decide on whether or not probable cause existed to open them.

The program was also cross-relational: "It united data associated with terrorists/criminals from all databases." And it was relatively cheap. THINTHREAD was developed in-house for a paltry \$3 million and could be fully deployed for about \$300 million. But NSA Director Michael Hayden vetoed this program in favor of an outside contractor's program called TRAILBLAZER, a decision made three weeks before the 9/11 attacks.

### **Bloating a Budget**

One of the bureaucratic "advantages" of TRAILBLAZER was that it cost more than ten times as much as THINTHREAD and allowed the NSA and various members of Congress thus to show that they were doing more about terrorism and helping out some favored contractors even though TRAILBLAZER ultimately proved a failure and a waste of some \$3.8 billion.

However, after 9/11, money was really no worry at the NSA. With the FBI and CIA

taking the brunt of the blame for the failure to stop the attacks, Hayden had a great opportunity to build up the NSA's budget and image, taking the code-breaking agency into the forefront of the U.S. intelligence community.

After 9/11, Drake tried unsuccessfully to revive THINTHREAD, but failed to scrape together enough money to complete a THINTHREAD content analysis program on NSA databases. This was how Drake learned that the NSA's information on some of the 9/11 hijackers was not shared outside the agency.

Drake discovered that the NSA had produced a lengthy analytic report that broke open the entire structure of Al-Qaeda and associated groups, including the content of phone calls between hijacker Khalid al-Midhar in San Diego with the known Al-Qaeda safe house communications center in Yemen.

Drake's information, of course, undermined the whole Bush/Cheney argument that if the U.S. only had a bulk collection program prior to 9/11, the attacks could have been prevented. Instead, the problem was an analytical failure to understand the import of information already collected. Piling on vast amounts of additional data arguably made the problem worse, burying the analysts in an unimaginably giant haystack of data and expecting them to locate the crucial needle.

As Drake noted, it was Vice President Dick Cheney who in pursuit of collecting as much data as possible got Hayden to violate the Fourth Amendment restrictions about the NSA's spying on Americans.

In an ironic twist, Cheney misused the Khalid al-Midhar case transforming it into an example of how the NSA could have prevented the attacks if it only had more data when, in fact, the NSA had this information in hand. But contradicting high-level officials on such sensitive matters will get employees not just drummed out of an agency, but indicted. As it did Drake.

### **Snowden and Drake**

All of this is apropos to any informed discussion regarding the new film about Edward Snowden called *Citizenfour* because Snowden was well aware of what happened to Drake. Snowden once said people in the NSA were afraid to go public because of what had been done to Drake.

But why did Snowden approach filmmaker Laura Poitras? In August 2012, documentary director Poitras released a short film called *The Program*, which was billed as a work in progress. It was largely based on interviews with Binney in which he discusses his work on STELLARWIND and how, unbeknownst to him, that program was turned on Americans after the 9/11 attacks.

The short film also mentioned a huge depository being built in Utah to house massive amounts of data gathered by the NSA. Because of her work on this and other politically relevant films, Poitras told PBS that she was placed on Homeland Security's Watch List and that she was frequently detained during border crossings with her work products searched.

But the first person we see in *Citizenfour* is not Snowden. Neither is it Poitras. It is columnist and blogger Glenn Greenwald, because of the three people Snowden tried to get in contact with to publicize the spy scandal at NSA, Greenwald was the first. (For some reason, the film leaves out the third person: *Washington Post* reporter Barton Gellman.)

The film takes its title from the fact that Snowden used that rubric as his encrypted email signature when he made some of his initial contact attempts. But Snowden was too mysterious and vague for Greenwald to deal with. Snowden also wanted him to employ some exotic encryption devices and sent Greenwald tutorials on how to use them. Greenwald put them aside and Snowden disappeared back into the blackness of cyberspace. That was in December of 2012.

## **Reaching Out**

In January 2013, *Citizenfour* tried again, this time with Poitras. Greenwald had written about Poitras and her problems with Homeland Security, and Snowden had seen the film about Binney. Unlike Greenwald, Poitras was familiar with PGP encryption keys and even more exotic devices.

Snowden assured her, "I am a senior member of the intelligence community. This will not be a waste of your time." And this is how the film begins, with Poitras showing blown-up versions of these enigmatic early emails from an anonymous source claiming to be high up in the Intel community.

Poitras does not want to continue the communications stateside so she goes to Berlin to learn more about her anonymous informant. At this point, the film relates part of the Binney story. It also begins to touch upon the misuse of FISA courts in the massive overreach of NSA and describes the new storage facility in Utah.

Somehow Poitras was allowed to film a hearing before a court about the government's use of a private phone company, AT&T, to monitor thousands, if not hundreds of thousands of cell phones. The lawyers for the government clearly do not want to disclose certain aspects of the program. One of the judges gets the message and says words to the effect that you would rather us not be here at all.

Poitras cuts to a briefing by an Occupy Wall Street technology leader. He is



telling a small room full of representatives how the government and the NSA can trace their calls through their cell phones and also their financial transactions through their bank cards and credit cards. In other words, the government can trace their actions day by day to put together where they were at certain times.

Since we know the Occupy Wall Street movement was under surveillance, this scene has a chilling overtone to it because it cuts to the quick of what Frank Church was worried about: NSA surveillance turned on domestic targets for purely political purposes. In this case, it was the suppression of a leftist populist movement.

### **Meeting in Hong Kong**

From here Poitras cuts to a series of officials, like Clapper, misrepresenting the reach and impact of programs like STELLARWIND. We then go to Snowden's communications requesting a formal meeting with Poitras and Greenwald in Hong Kong. This happens on June 3, 2013.

Much of this part of the film is shot in Snowden's rather small rented room in a Hong Kong hotel. Poitras is never on camera. But Ewen MacAskill from *The Guardian* is. Since the paper employed Greenwald, the whole project came under the UK newspaper's purview.

The American editor of the paper, Janine Gibson, wanted a veteran presence in the mix. So MacAskill is the second person in the room as we watch the renegade NSA employee begin to disclose some of the deepest secrets of the so-called "war on terror."

Snowden talks about one of the things that actually disgusted him while working for the NSA, that the employees actually got to watch drone strikes in real time on their desktop computers. They would watch the drones approach the target and then circle it for, at times, hours on end.

Snowden then says to Greenwald that he does not want the issue to be about him personally. That is not the way he sees it. To Snowden, this is rather a simple schematic, it's State Power vs. Citizen Power. He then adds that the great promise of the internet has now been compromised because of the use of it as a tool of surveillance.

Here, I should interject an example to convey how real that Snowden's issues are. A few months ago, in advance of a major conference on the Kennedy assassination in Pittsburgh, a former investigator for the House Select Committee on Assassinations asked me by email how I got a summary of an interview that he did with the late David Phillips. Like Snowden, he sent me his

communications encrypted. But even at that, I did not wish to reply online.

When I saw him in person, I explained to him how I got the Top Secret summary but I had held back from communicating this information by email because of the chilling effect caused by knowledge about programs like STELLARWIND.

### **Through the PRISM**

As the documentary unfolds, Snowden explains two more programs: TEMPORA, and PRISM. For TEMPORA, the NSA contracted out work to the British GCHQ, the NSA's UK equivalent, to tap into hundreds of the world's fiber optic network cables, which allows for spying on more than 600 million telephone actions per day.

But beyond that, the program allows the user to intercept emails, check people's access to internet web sites, and see what they are posting on Facebook.

This is conducted through the so-called Five Eyes alliance, the loose union of the intelligence communities of America, England, Canada, Australia and New Zealand. Poitras takes her camera to the wind-blown coast of England and shows how the GCHQ has attached probes to trans-Atlantic cables when they hit British soil.

Another program, PRISM, is used by the NSA domestically. Snowden secured a 41-frame Power Point presentation on it. The aim of this program is to collect private electronic data belonging to users of major internet carriers like Gmail, AOL, Skype and YouTube.

With the exposure of PRISM, Snowden cut out one of the most often used defenses by both the Bush and Obama administrations, namely, that they were collecting only "metadata," that is, only the times and durations of communications. PRISM collects the contents of emails, online chats, cloud-stored files, and much more.

In fact, PRISM is so intrusive that there is a dispute over whether or not the aforementioned companies have agreed to let their clients be spied on. The companies denied they had cooperated with the NSA. But the government says the FISA courts have issued orders to do so that are presented to the companies in question. (See, for example, ["Everything You need to Know about Prism"](#), by T.C. Sottek and Joshua Kopstein, in *The Verge*, July 17, 2013)

Brad Smith, a general counsel for Microsoft, gave the game away. Quoted for attribution, he said, "We believe the U.S. Constitution guarantees our freedom to share more information with the public, yet the government is stopping us." (ibid) In other words, these private companies are now under the thumb of the NSA. But they don't want to be held liable for a class-action lawsuit on

invasion of privacy.

### **Real-Time Access**

As Snowden notes in the film, PRISM is not just a recording device. It can be channeled backward and forwards in time. That is, once the target is identified, PRISM can access all the information from the company's databank, from the past to the present and monitor it into the future.

One of the disclosures made by Snowden that had a huge impact and that the film properly plays up was the fact that Verizon had agreed to turn over records of millions of its customers to the NSA and FBI. This court order required the company to turn over on an "ongoing, daily basis" all phone calls in its systems, both within the U.S. and between the U.S. and other countries. (*The Guardian*, June 6, 2013)

This began in April 2013, and was renewed at 90-day intervals. In other words, it was done under President Obama. Without Snowden, it is unlikely this story would have ever seen the light of day because the court order expressly barred Verizon from disclosing the existence of the FBI's request for the records or the court order itself. (ibid)

This points out a matter not dealt with in the film. Namely that Chief Justice John Roberts has stacked the FISA courts with judges who simply will not say no to any national security request, no matter how much it infringes on privacy and the Fourth Amendment. They have, for all intents and purposes, become rubber stamps for administration requests.

As we watch the film, one of the issues Greenwald and Snowden discuss is how much of the story should be about Snowden, who isn't seeking out notoriety. He simply tells Greenwald that he grew up in North Carolina and Maryland and that he ended up working for the NSA through subcontractor Booz Allen Hamilton.

### **Snowden's Biography**

But, actually, Snowden's life is much more interesting than he lets on and in my view should have been a bigger part of this film. Snowden comes from a military family. His father and grandfather were both in the Coast Guard, and he was born in the port town of Elizabeth City, North Carolina. In fact, many of the men in Snowden clan had careers in either law enforcement or the military.

The family moved to Maryland when Snowden was nine. In high school he became ill with mononucleosis, dropping out before his sophomore year. At this time, he became very interested in computer technology and took a number of advanced classes in community colleges and earned certification as a systems engineer.

He became obsessed with computer technology and tried to tear down systems to see how they worked. He then reconstructed them so they would work better. He began hanging out at an online chat room called Ars Technica.

When 9/11 happened, Snowden favored invading Iraq. And in May 2004, he joined the Army. "I felt I had an obligation as a human being to help free people from oppression," he said later. (op. cit. *Vanity Fair*) After arriving at Fort Benning, Georgia, Snowden broke both legs in a training accident. After he was released from the military, he joined the CIA in 2006.

Snowden himself could not believe it. On Ars Technica he wrote, "I don't have a degree of any type. In fact, I don't even have a high school diploma. . . . and my co-workers have BSs, MSs and ten to fifteen years of experience. Employers fight over me. And I'm 22."

Snowden worked in network security, allowing him to have a top-secret clearance. Less than a year later, he was transferred to Geneva with a diplomatic cover as part of the mission to the United Nations. He was given a four-bedroom government-issue apartment. And in some of his online posts, he said he was having a very nice time.

But it was also in Geneva that Snowden began to become ambivalent toward his job. As part of an undercover mission, he saw how the CIA got a banker drunk, encouraged him to drive, and then after he got in an accident, recruited him as an informant.

Snowden told *The Guardian* that he witnessed several instances like this in Europe and concluded, "Much of what I saw in Geneva really disillusioned me about how my government functions and what its impact in the world." (ibid)

Indeed, it was at this point, in about 2008, that Snowden first thought about leaking confidential documents, in part because he felt that the Democratic candidate for president, Barack Obama, might change things.

### **Getting Angry**

Shortly after Obama's election, Snowden left the CIA. To this day, there are several versions why. But most observers agree that Snowden came back to America as somewhat of an angry young man. His online posts seem to indicate that he was rather conservative. For instance, he railed against Social Security.

But Snowden soon landed a job with Dell Computer, and the NSA was one of Dell's biggest and most secret clients. Snowden began working on NSA projects in Japan, and in summer 2010, he was transferred back to Maryland where the NSA is based. Here he led a team of experts in designing state-of-the-art, cloud-computing

platforms, and also technically sophisticated super computers for breaking passwords. (ibid)

Snowden then took another step upward and another change of locale. He became a high-level systems administrator in Hawaii. But there was also a change in the young man's attitude. He now wore a sweatshirt sold by the Electronic Frontier Foundation, whose motto was "Defending your rights in the digital world."

Snowden also began to complain about the NSA's unlawful though authorized surveillance. When he was brushed off, he began to use his clearance and position as a systems administrator to delve into areas that were not related to his job description. In the summer of 2012, Snowden made his first illegal downloads.

Snowden also applied for a job directly with the NSA and was offered a position though he felt it was not high enough in the bureaucracy. So, he turned it down and applied for a position at Booz Allen Hamilton, a company owned by the politically well-connected Carlyle Group. He got a job in cyber security, saying later: "My position with Booz granted me access to lists of machines all over the world that the NSA hacked."

By this time, spring 2013, Snowden was in communication with Greenwald, Poitras and Gellman. In May, he had all his documents ready to go. To this day, no one knows how many there were. Snowden kept downloading Top Secret documents until the end.

Finally, on May 17, he told his girlfriend he was leaving on a business trip. He went to Honolulu Airport and ended up in Hong Kong. He booked a room at the Mira in the Kowloon area.

### **Libertarian Leanings**

All of this is only dealt with glancingly in the film, if at all. To me, it seems of paramount interest because, unlike say the Cambridge Five, the infamous British spy ring recruited by the Soviet Union, Snowden did what he did not for ideology but because he was genuinely offended by the NSA's invasion of citizens' privacy.

Politically speaking, Snowden appears to be more or less a moderate with libertarian leanings. If I were Poitras, I would have insisted some of this background make it into the film.

There is another aspect of the Snowden saga that I feel was slighted. We watch as Greenwald tells Snowden not to try and hide his identity. In fact, Snowden paid for his room at the Mira Hotel in Hong Kong with his own credit card.

Greenwald says words to the effect: just do it out in the open, let them react to who you are.

Here *Citizenfour* introduces Julian Assange and Wikileaks, with Assange aware of the harsh imprisonment of his leading source Pvt. Bradley (now Chelsea) Manning arranging for Snowden to get out of Hong Kong before the State Department could close in on him. Assange and his assistant Sarah Harrison get Snowden a flight to Moscow for a stopover en route to his planned destination in Latin America. But the U.S. government charges Snowden under the Espionage Act and he has no choice but to seek asylum in Russia. Since the State Department cancelled Snowden's passport, he remains in Russia.

Towards the end of the film, there are two ominous episodes. As Greenwald and his partner are traveling back to their home in Brazil, his partner is detained at Heathrow Airport for nine hours, the legal limit without making an arrest.

Journalist Jeremy Scahill then makes an appearance and poses the question: If one wants to communicate sensitive information today and be sure it's not intercepted, how does one do it? The answer is to return to Watergate days, with conversations in parking lot garages late at night, while avoiding electronic communications.

The last scene is a bit problematic. Greenwald is visiting Snowden in Russia. They talk about how many people are on the Watch List today and communicate via written messages which are then ripped up.

Snowden is shocked at the figure of 1.2 million people, and we see this on a torn paper. I thought this was all strained. What was the need of communicating with written messages in Moscow? And both participants must have known the camera was there. After all it zoomed in for close-ups on the paper. So why rip up the paper on camera?

This was using the techniques of a dramatic scenarist in a documentary. Greenwald and Snowden came close to being actors here, rather than participants in a real-life drama.

There will be future movies on the Snowden story with actual actors playing the key protagonists, including a feature film by director Oliver Stone. But this documentary is a creditable first offering in the field.

**James DiEugenio is a researcher and writer on the assassination of President John F. Kennedy and other mysteries of that era. His most recent book is Reclaiming Parkland.**

---