**INSTRUCTIONS**

Drawing on the assigned readings, **post a thread to Discussion Forum/Topic #2**addressing the following questions.

* Was Snowden engaged in legitimate "whistle-blowing," seeking to inform and protect the American public against government misconduct intended to infringe on their individual liberty and privacy, as he and his supporters maintain?
* Or was his an act of treason (as angry critics and detractors responded) in the midst of a desperate, ongoing, proactive, and possibly new kind of "preemptive" war of national self-defense?

I am interested in your opinion, as long as it is informed and well-supported with evidence—including evidence drawn from the assigned readings.  **Please remember to respond to at least TWO of your fellow students.**

**RESPONSE**

Snowden is undoubtedly a whistleblower by exposing the NSA’s PRISM program. According to Wikipedia, the program can be summarized as the NSA “[collecting] internet communications from various U.S. internet companies.” Although Snowden violated 18 USC 1030 by “intentionally [accessing] a protected computer without authorization, and as a result of such conduct, causes damage and loss” (a.5.A) among other violations, he did so with the intent of informing the American public of a widespread 4th Amendment violation. It can be argued that his violation of 18 USC 1030 allows him to protected from retaliation under the provisions of the Whistleblower Protection Act (ftc.gov) since he “reasonably believed…a violation of law” had occurred. So, the question is, “does computer data and personal digital communications require probable cause to intercept?”

The 4th Amendment of the US Constitution states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” There are sufficient arguments that collecting all internet communications violate the 4th Amendment since probable cause does not exist for every American to justify such action.

USA.gov states that “the executive branch carries out and enforces laws”. The NSA falls under the executive branch’s purview, but is classified as a defense/intelligence agency operating under the Office of the Director of National Intelligence (ODNI) (nsa.gov). But this does not disqualify them from the laws that govern other law-enforcement agencies. Compliance with the Foreign Intelligence Surveillance Act (FISA) and warrants obtained through a non-public process are the justification given the NSA gave in response to Snowden’s disclosures. He just didn’t do it through approved channels by going to *The Guardian* (ftc.gov).

At the most basic level, police can conduct a warrantless search of a vehicle if they have probable cause established in *US v. Ross* (1982). So how does this apply to computers? *Riley v. California* (2014) determined that a search of a phone is unconstitutional if a warrant does not exist (oyez.org). Taking these two cases, we can easily infer that phones, computers, and digital communications constitute “houses, papers, and effects” under the 4th Amendment.

The key phrase in the 4th Amendment is “unreasonable”. If a police officer can come into anyone’s home for a search, regardless of probable cause, then that would be considered unreasonable. A warrant issued by a court for search of everyone’s home in the US is unreasonable. Following that logic, a warrant for a blanket surveillance program of everyone’s “houses, papers, and effects” regardless if probable cause exists for an individual is most definitely unreasonable. Therefore, Edward Snowden is a whistleblower and not a traitor due to the gross 4th Amendment violations by the NSA.