Suppose that Angelina Jolie has just returned from North Korea after adopting yet another child. Since North Korea is a known enemy of the United States, her trip could be considered suspicious. Should the government have the authority to access to her friends and family’s private Facebook accounts to see what she has commented about her trip?

How can we, as Americans, keep our nation’s security and our civil liberties balanced? Our nation follows a set of principles such as the Bill of Rights and the Constitution. In the Bill of Rights, the Fourth Amendment states that “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.” However, this amendment needs to be expanded to protect the rights of the modern cyber citizen. In today’s world, there is not only physical property but also vast amounts of virtual property. Just as there is a necessity for warrants in the physical world, these should also be used to protect private virtual information.

What constitutes the difference between public and private virtual information? Public information, as we define it, includes an individual’s internet search history, purchase history, social media, and any webpage that the general public can access on their computers. All public information should be accessible to the government for the purpose of discovering suspicious activity throughout the web. The government must have files they can freely see in order to detect possible dangers and threats. Besides public information, there is also private information, which contains materials that people would feel are more personal. Private information consists of all social security data and credit card and banking information; because  most people view these as highly personal, a search warrant should be required to access these materials.

In current legislation, the Foreign Intelligence Surveillance Act,  security officials must obtain warrants to view citizens’ personal information. However, there are subtle differences between what we view as acceptable policy and what is actually being implemented. One of the differences is that prior to acquiring a warrant, FISA allows a warrantless three day investigation, with which we strongly disagree. On the other hand, our boundaries between public and private information, or what we consider information accessible without a warrant, is more lenient. Our policy allows for searches of easily accessible data for which current legislation requires a warrant..

Today’s domestic surveillance program protects our national security interests. In 2009, the FBI found an Al Qaeda member, nineteen-year-old Hosam Maher Husein Smadi, by monitoring chat rooms.   The program is an effective one, but current warrant policies need modification.