COMPUTER ETHICS: PRIVACY
ESSAY#2, DUELING ANALYSES

DUE: Friday, October 11, 2013

Your second essay assignment is similar to the first. The major difference is that I expect you to use a bit more sophistication in your ethical analysis. This paper will probably be somewhat longer than the first, but should be less than 1500 words. Again you must email the paper to `croyden@cs.holycross.edu` by 2:00 p.m., October 11, 2013 **and** turn in a printed version in class the same day. I prefer the electronic version of your paper to be in rich text format (RTF).

First, read the attached articles about recent governement surveillance and how meta-data can be used to identify people of interest. In class and in our readings we have been discussing issues of Privacy and Surveillance in today's IT society. The attached articles describe the data collection that has been carried out by the National Security Agency (NSA) as well as an article showing how data similar to phone "metadata" can be used to determine information about people and their associations, including some information that those individuals might not realize could be learned from their phone information. Your essay should analyze and draw a conclusion about the following question. Should the government be allowed to collect and "mine" personal data (including phone metadata) without an individual's knowledge or permission?

You should support your analyses using information from our class readings and discussion, from the attached articles and from the articles you find in your research.

Your paper should be written in seven sections. Give each of these sections the title shown below in bold face. Skip a line between each section.

Section I. Names.: The first thing in this section should be your own name. On the next line, name the course (CSCI 328), the assignment (Essay #2. Computer Ethics: Privacy, Dueling analyses), and the title of your essay. These four items should appear on separate lines, single spaced.

Section II. Reference(s): You should research the topic for your essay and find at least 2 addtional articles on the topic. Describe carefully where your reader could find the references you used in preparing to write the essay. For each website you cite, include the URL, the author or organization, the article title, the magazine or program title, the date of publication, page numbers, the date you accessed it, and the date it was last updated (if available). In addition to identifying your primary source(s), if you use someone else's words or ideas anywhere in your paper, you should indicate that use with quotes or with a paragraph set off with indentations and blank lines. Always advertise

your sources and use complete endnotes. To not do so risks the serious charge of plagiarism. (One good source for citations is The Little, Brown, Handbook, 2nd Edition, by H. Ramsey Fowler. Endnotes are discussed on pages 480-489.)

Section III. The Technology Issues: Explain to your reader the most important points in your article /topic pertaining to the technical issues. Assume the reader is a reasonably intelligent undergraduate liberal arts student with some technical expertise about computers. Be concise, but don't leave out any details important to the ethical issue.

Section IV. Stakeholders/The Human Values at Stake: In this section, explain to your reader why the technical issues in this article/issue are important to humans. List all the "players" and tell what is at stake for them in the ethical issue. What people, groups of people, and/or organizations either care or should care about this issue/decision? How are they affected, directly or indirectly, by the issue/decision? What are the costs and benefits, the risks and opportunities, involved? The questions should not be answered one after another in your section; that would be clumsy. Instead, think about all these questions and then write a concise answer to the following broad question: "Who are the stakeholders in this situation, and what human values do they have at stake?"

Section V. Utilitarian Analysis: Using the criteria of a utilitarian analysis, describe how the issue should be decided and why. Remember, in this type of analysis the consequences are central.

Section VI. Deontological Analysis: Review in the textbook what Johnson considers deontological. Make an argument about the ethical issue using a deontological strategy.

Section VII. Conclusion: Decide which of the arguments you wrote for the previous two sections was more convincing. Explain why you find that argument more satisfying. Make sure that your analysis looks at more than one possible conclusion, and then justify why you picked the conclusion you did. You are required to take and defend a position on this issue. "I'm not sure what to do" is not an acceptable conclusion. You don't have to be certain, but you do have to make a decision. Your essay should talk about what is right to do.

Clear thinking is revealed in clear writing. Spelling, grammar, and style all count. Follow the instructions above carefully.

One of the aims in this course is to become more aware of the technical decisions being made in our society, and how they change our society and our lives. This paper gives you a chance to look for one such decision, to consider it in detail using two philosophical theories, and then explain your conclusion.

1) Link to article on Metadata:
http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/

2) Article on US government surveillance:

U.S. Confirms That It Gathers Online Data Overseas

By CHARLIE SAVAGE, EDWARD WYATT and PETER BAKER
Published: June 6, 2013, New York Times
http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0

WASHINGTON — The federal government has been secretly collecting information on foreigners overseas for nearly six years from the nation's largest Internet companies like Google, Facebook and, most recently, Apple, in search of national security threats, the director of national intelligence confirmed Thursday night.

The confirmation of the classified program came just hours after government officials acknowledged a separate seven-year effort to sweep up records of telephone calls inside the United States. Together, the unfolding revelations opened a window into the growth of government surveillance that began under the Bush administration after the terrorist attacks of Sept. 11, 2001, and has clearly been embraced and even expanded under the Obama administration.

Government officials defended the two surveillance initiatives as authorized under law, known to Congress and necessary to guard the country against terrorist threats. But an array of civil liberties advocates and libertarian conservatives said the disclosures provided the most detailed confirmation yet of what has been long suspected about what the critics call an alarming and ever-widening surveillance state.

The Internet surveillance program collects data from online providers including e-mail, chat services, videos, photos, stored data, file transfers, video conferencing and log-ins, according to classified documents obtained and posted by The Washington Post and then The Guardian on Thursday afternoon.

In confirming its existence, officials said that the program, called Prism, is authorized under a foreign intelligence law that was recently renewed by

Congress, and maintained that it minimizes the collection and retention of information "incidentally acquired" about Americans and permanent residents. Several of the Internet companies said they did not allow the government open-ended access to their servers but complied with specific lawful requests for information.

"It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States," James Clapper, the director of national intelligence, said in a statement, describing the law underlying the program. "Information collected under this program is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats."

The Prism program grew out of the National Security Agency's desire several years ago to begin addressing the agency's need to keep up with the explosive growth of social media, according to people familiar with the matter.

The dual revelations, in rapid succession, also suggested that someone with access to high-level intelligence secrets had decided to unveil them in the midst of furor over leak investigations. Both were reported by The Guardian, while The Post, relying upon the same presentation, almost simultaneously reported the Internet company tapping. The Post said a disenchanted intelligence official provided it with the documents to expose government overreach.

Before the disclosure of the Internet company surveillance program on Thursday, the White House and Congressional leaders defended the phone program, saying it was legal and necessary to protect national security.

Josh Earnest, a White House spokesman, told reporters aboard Air Force One that the kind of surveillance at issue "has been a critical tool in protecting the nation from terror threats as it allows counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities, particularly people located inside the United States." He added: "The president welcomes a discussion of the trade-offs between security and civil liberties."

The Guardian and The Post posted several slides from the 41-page presentation about the Internet program, listing the companies involved — which included Yahoo, Microsoft, Paltalk, AOL, Skype and YouTube — and the dates they joined the program, as well as listing the types of information collected under the program.

The reports came as President Obama was traveling to meet President Xi Jinping of China at an estate in Southern California, a meeting intended to address among other things complaints about Chinese cyberattacks and spying. Now that conversation will take place amid discussion of America's own vast surveillance operations.

But while the administration and lawmakers who supported the telephone records program emphasized that all three branches of government had signed off on it, Anthony Romero of the American Civil Liberties Union denounced the surveillance as an infringement of fundamental individual liberties, no matter how many parts of the government approved of it.

"A pox on all the three houses of government," Mr. Romero said. "On Congress, for legislating such powers, on the FISA court for being such a paper tiger and rubber stamp, and on the Obama administration for not being true to its values."

Others raised concerns about whether the telephone program was effective.

Word of the program emerged when The Guardian posted an April order from the secret foreign intelligence court directing a subsidiary of Verizon Communications to give the N.S.A. "on an ongoing daily basis" until July logs of communications "between the United States and abroad" or "wholly within the United States, including local telephone calls."

On Thursday, Senators Dianne Feinstein of California and Saxby Chambliss of Georgia, the top Democrat and top Republican on the Intelligence Committee, said the court order appeared to be a routine reauthorization as part of a broader program that lawmakers have long known about and supported.

"As far as I know, this is an exact three-month renewal of what has been the case for the past seven years," Ms. Feinstein said, adding that it was carried

out by the Foreign Intelligence Surveillance Court "under the business records section of the Patriot Act."

"Therefore, it is lawful," she said. "It has been briefed to Congress."

While refusing to confirm or to directly comment on the reported court order, Verizon, in an internal e-mail to employees, defended its release of calling information to the N.S.A. Randy Milch, an executive vice president and general counsel, wrote that "the law authorizes the federal courts to order a company to provide information in certain circumstances, and if Verizon were to receive such an order, we would be required to comply."

Sprint and AT&T have also received demands for data from national security officials, according to people familiar with the requests. Those companies as well as T-Mobile and CenturyLink declined to say Thursday whether they were or had been under a similar court order.

Lawmakers and administration officials who support the phone program defended it in part by noting that it was only for "metadata" — like logs of calls sent and received — and did not involve listening in on people's conversations.

The Internet company program appeared to involve eavesdropping on the contents of communications of foreigners. The senior administration official said its legal basis was the so-called FISA Amendments Act, a 2008 law that allows the government to obtain an order from a national security court to conduct blanket surveillance of foreigners abroad without individualized warrants even if the interception takes place on American soil.

The law, which Congress reauthorized in late 2012, is controversial in part because Americans' e-mails and phone calls can be swept into the database without an individualized court order when they communicate with people overseas. While the newspapers portrayed the classified documents as indicating that the N.S.A. obtained direct access to the companies' servers, several of the companies — including Google, Facebook, Microsoft and Apple — denied that the government could do so. Instead, the companies have negotiated with the government technical means to provide specific data in response to court orders, according to people briefed on the

arrangements.

“Google cares deeply about the security of our users’ data,” the company said in a statement. “We disclose user data to government in accordance with the law and we review all such requests carefully. From time to time, people allege that we have created a government ‘backdoor’ into our systems, but Google does not have a ‘backdoor’ for the government to access private user data.”

While murky questions remained about the Internet company program, the confirmation of the calling log program solved a mystery that has puzzled national security legal policy observers in Washington for years: why a handful of Democrats on the Senate Intelligence Committee were raising cryptic alarms about Section 215 of the Patriot Act, the law Congress enacted after the 9/11 attacks.

Section 215 made it easier for the government to obtain a secret order for business records, so long as they were deemed relevant to a national security investigation.

Section 215 is among the sections of the Patriot Act that have periodically come up for renewal. Since around 2009, a handful of Democratic senators briefed on the program — including Ron Wyden of Oregon — have sought to tighten that standard to require a specific nexus to terrorism before someone’s records could be obtained, while warning that the statute was being interpreted in an alarming way that they could not detail because it was classified.

On Thursday, Mr. Wyden confirmed that the program is what he and others have been expressing concern about. He said he hoped the disclosure would “force a real debate” about whether such “sweeping, dragnet surveillance” should be permitted — or is even effective.

But just as efforts by Mr. Wyden and fellow skeptics, including Senators Richard J. Durbin of Illinois and Mark Udall of Colorado, to tighten standards on whose communications logs could be obtained under the Patriot Act have repeatedly failed, their criticism was engulfed in a clamor of broad, bipartisan support for the program.

"If we don't do it," said Senator Lindsey Graham, Republican of South Carolina, "we're crazy."

And Representative Mike Rogers, Republican of Michigan and the chairman of the House Intelligence Committee, claimed in a news conference that the program helped stop a significant domestic terrorist attack in the United States in the last few years. He gave no details.

It has long been known that one aspect of the Bush administration's program of surveillance without court oversight involved vacuuming up communications metadata and mining the database to identify associates — called a "community of interest" — of a suspected terrorist.

In December 2005, The New York Times revealed the existence of elements of that program, setting off a debate about civil liberties and the rule of law. But in early 2007, Alberto R. Gonzales, then the attorney general, announced that after months of extensive negotiation, the Foreign Intelligence Surveillance Court had approved "innovative" and "complex" orders bringing the surveillance programs under its authority.

Reporting was contributed by Eric Schmitt, Jonathan Weisman and James Risen from Washington; Brian X. Chen from New York; Vindu Goel, Claire Cain Miller, Nicole Perlroth, Somini Sengupta and Michael S. Schmidt from San Francisco; and Nick Wingfield from Seattle.