COMPUTER ETHICS: PRIVACY
ESSAY#2, DUELING ANALYSES

DUE: Monday, April 23, 2012

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. The paper should be three to four pages long. Again you must email the paper to `croyden@cs.holycross.edu` by 10:00 a.m., April 23, 2012 **and** turn in a printed version in class the same day.

First, read the attached articles about privacy in the internet age. In class and in our readings we have been discussing issues of Privacy in an IT society. In our discussions, and as described in the attached articles, data mining technology can result in people, organizations or the government learning things about individuals that those individuals might not realize could be learned from their online information. Your essay should analyze and draw a conclusion about the following question. Should companies or the government be allowed to "mine" personal data without an individual's permission?

You should support your analyses using information from our class readings and discussion and from the attached articles. You must also find at least 2 more articles from reliable sources (as we discussed last semester) on this issue.

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 (MONT 113G), 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. 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 III. 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? 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 IV. 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 V. Deontological Analysis: Review in the textbook what Johnson considers deontological. Make an argument about the ethical issue using a deontological strategy.

Section VI. 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.

Section VII. Reference(s): You should research the topic for your essay. 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 cite your sources as we discussed in the first semester. In the text, cite the author and year in parentheses after the cited text. In the References section list all your sources using MLA or APA format. (If you're not sure which to use, I prefer APA).

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.

http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/?page=1
The Boston Globe, Johnson, C.Y., Archived column
Accessed 10-7-2009

September 20, 2009
Project 'Gaydar'
At MIT, an experiment identifies which students are gay, raising new questions about online privacy.

By Carolyn Y. Johnson

It started as a simple term project for an MIT class on ethics and law on the electronic frontier.

Two students partnered up to take on the latest Internet fad: the online social networks that were exploding into the mainstream. With people signing up in droves to reconnect with classmates and old crushes from high school, and even becoming online "friends" with their family members, the two wondered what the online masses were unknowingly telling the world about themselves. The pair weren't interested in the embarrassing photos or overripe profiles that attract so much consternation from parents and potential employers. Instead, they wondered whether the basic currency of interactions on a social network - the simple act of "friending" someone online - might reveal something a person might rather keep hidden.

Using data from the social network Facebook, they made a striking discovery: just by looking at a person's online friends, they could predict whether the person was gay. They did this with a software program that looked at the gender and sexuality of a person's friends and, using statistical analysis, made a prediction. The two students had no way of checking all of their predictions, but based on their own knowledge outside the Facebook world, their computer program appeared quite accurate for men, they said. People may be effectively "outing" themselves just by the virtual company they keep.

"When they first did it, it was absolutely striking - we said, 'Oh my God - you can actually put some computation behind that,' " said Hal Abelson, a computer science professor at MIT who co-taught the course. "That pulls the rug out from a whole policy and technology perspective that the point is to give you control over your information - because you don't have control over your information."

The work has not been published in a scientific journal, but it provides a provocative warning note about privacy. Discussions of privacy often focus on how to best keep things secret, whether it is making sure online financial transactions are secure from intruders, or telling people to think twice before opening their lives too widely on blogs or online profiles. But this work shows that people may reveal information about themselves in another way, and without knowing they are making it public. Who we are can be revealed by, and even defined by, who our friends are: if all your friends are over 45, you're probably not a teenager; if they all belong to a particular religion, it's a decent bet that you do, too. The ability to connect with other people who have something in common is part of the power of social networks, but also a possible pitfall. If our friends reveal who we are, that challenges a conception of privacy built on the notion that there are things we tell, and things we don't.

"Even if you don't affirmatively post revealing information, simply publishing your friends' list may reveal sensitive information about you, or it may lead people to make assumptions about you that are incorrect," said Kevin Bankston, senior staff attorney for the Electronic Frontier Foundation, a nonprofit digital rights organization in San Francisco. "Certainly if most or many of your friends are of a particular religious or political or sexual category, others may conclude you are part of the same category - even if you haven't said so yourself."

The project, given the name "Gaydar" by the students, Carter Jernigan and Behram Mistree, is part of the fast-moving field of social network analysis, which examines what the connections between people can tell us. The applications run the gamut, from predicting who might be a terrorist to the likelihood a person is happy or fat. The idea of making assumptions about people by looking at their relationships is not new, but the sudden availability of information online means the field's powerful tools can now be applied to just about anyone.

For example, Murat Kantarcioglu, an assistant professor of computer science at the University of Texas at Dallas, found he could make decent predictions about a person's political affiliation. He and a student - who later went to work for Facebook - took 167,000 profiles and 3 million links between people from the Dallas-Fort Worth network. They used three methods to predict a person's political views. One prediction model used only the details in their profiles. Another used only friendship links. And the third combined the two sets of data.

The researchers found that certain traits, such as knowing what groups people belonged to or their favorite music, were quite predictive of political affiliation. But they also found that they did better than a random guess when only using friendship connections. The best results came from combining the two approaches.

Other work, by researchers at the University of Maryland, College Park, analyzed four social networks: Facebook, the photo-sharing website Flickr, an online network for dog owners called Dogster, and BibSonomy, in which people tag bookmarks and publications. Those researchers blinded themselves to the profiles of half the people in each network, and launched a variety of "attacks" on the networks, to see what private information they could glean by simply looking at things like groups people belonged to, and their friendship links.

On each network, at least one attack worked. Researchers could predict where Flickr users lived; Facebook users' gender, a dog's breed, and whether someone was likely to be a spammer on BibSonomy. The authors found that membership in a group gave away a significant amount of information, but also found that predictions using friend links weren't as strong as they expected. "Using friends in classifying people has to be treated with care," computer scientists Lise Getoor and Elena Zheleva wrote.

The idea behind the MIT work, done in 2007, is as old as the adage that birds of a feather flock together. For years, sociologists have known of the "homophily principle" - the tendency for similar people to group together. People of one race tend to have spouses, confidants, and friends of the same race, for example. Jernigan and Mistree downloaded data from the Facebook network, choosing as their sample people who had joined the MIT network and were in the classes 2007-2011 or graduate students. They

were interested in three things people frequently fill in on their social network profile: their gender, a category called "interested in" that they took to denote sexuality, and their friend links.

Using that information, they "trained" their computer program, analyzing the friend links of 1,544 men who said they were straight, 21 who said they were bisexual, and 33 who said they were gay. Gay men had proportionally more gay friends than straight men, giving the computer program a way to infer a person's sexuality based on their friends.

Then they did the same analysis on 947 men who did not report their sexuality. Although the researchers had no way to confirm the analysis with scientific rigor, they used their private knowledge of 10 people in the network who were gay but did not declare it on their Facebook page as a simple check. They found all 10 people were predicted to be gay by the program. The analysis seemed to work in identifying gay men, but the same technique was not as successful with bisexual men or women, or lesbians.

"It's just one example of how information could be inadvertently shared," said Jernigan. "It does highlight risks out there."

The researchers treated their data anonymously, never using names except to validate their predictions during data analysis. The only copy of the data is on an encrypted DVD they gave to a professor, and they said they got the approval of an ethical review board at MIT. The students, who have since graduated, discussed the paper with the Globe, but did not provide a copy of it because they are hoping to have it published in a journal.

Facebook spokesman Simon Axten could not respond to Jernigan and Mistree's analysis, since it is not public, but pointed out that it is something that happens every day.

"In general, it's not too surprising that someone might make inferences about someone else without knowing that person based on who the person's friends are. This isn't specific to Facebook and is entirely possible in the real world as well," Axten wrote in an e-mail. "For example, if I know that someone has certain political views because that person makes them known in some way (say, by putting a bumper sticker on his car), and then I see the person walking out of a movie with friends I don't know, I might assume those friends also have those political views."

Privacy has become a growing and evolving concern as social networks learn how to deal with the fact that they provide a resource that brings people together, but also may endanger privacy in ways they did not anticipate. Social networks like Facebook already give people power over that information, with privacy features that allow people to hide their profiles, and even make their list of friends invisible to outsiders, as well as from select friends.

Because the features and services offered on social networks are new, they also evolve in response to user demand that may not always be anticipated by the company. In 2007, for example, Facebook introduced Beacon, a feature that broadcasted friends' activities - such as buying movie tickets on a specific website - like targeted advertisements. That drew an angry response from users concerned about privacy, and prompted an apologetic blog posting from Facebook cofounder Mark Zuckerberg, along with modifications that meant people could opt out.

Computer scientists are identifying the ways in which anyone from a potential employer to an advertiser might be able to make informed guesses about a person. But there are limits to online privacy, and ultimately, say some experts, people will simply have to weigh the costs and benefits of living online.

"You can do damage to your reputation with social networking data, and other people can do damage to you. I do think that there's been a very fast learning curve - people are quickly learning the dos and don'ts of Internet behavior," said Jason Kaufman, a research fellow at the Berkman Center for Internet and Society at Harvard University who is studying a set of Facebook data. "Potentially everything you ever do on the Internet will live forever. I like to think we'll all learn to give each other a little more slack for our indiscretions and idiosyncrasies."

http://www.parade.com/articles/editions/2007/edition_09-16-2007/APrivacy
Parade Magazine, Flynn, S., Archived column
Accessed 10-7-2009

In our digital world, it may be impossible to protect personal information.
Is Anything Private Anymore?
By Sean Flynn
published: 09/16/2007

Kevin Bankston was a closet smoker who hid his habit by sneaking cigarettes outside his San Francisco office. He expected anonymity on a big city street. But in 2005, an online mapping service that provided ground-level photographs captured him smoking—and made the image available to anyone on the Internet. This year, Google's Street View project caught him again.

Coincidence? Absolutely. Yet Bankston's twice-documented smoking highlights a wider phenomenon: Privacy is a withering commodity for all of us.

What you buy, where you go, whom you call, the Web sites you visit, the e-mails you send—all of that information can be monitored and logged. "When you're out in public, it's becoming a near certainty that your image will be captured," says (the newly nonsmoking) Bankston.

Should you care? I've interviewed numerous people on all sides of the privacy debate to find out just how wary we should be.

One thing is clear: In today's world, maintaining a cocoon of privacy simply isn't practical. Need a mortgage or a car loan? A legitimate lender is going to verify a wealth of private information, including your name and address, date of birth, Social Security number and credit history. We all make daily trade-offs for convenience and thrift: Electronic tollbooths mean you don't have to wait in the cash-only lane, but your travel habits will be tracked. The Piggly Wiggly discount card saves you $206 on your annual grocery bill, but it counts how many doughnuts and six-packs you buy. MySpace posts make it easy to keep in touch with friends, but your comments live on.

So how do you live in a digital world and still maintain a semblAnce of privacy? Experts say it's crucial to recognize that those bits of data are permanent—a trail of electronic crumbs that is never swept away, available to anyone with the skills and inclination to sniff it out.

Privacy may not feel like much of an issue for those in their teens and 20s. They've grown up chronicling their lives on popular social networking sites like MySpace or Facebook for easy retrieval by friends and strangers alike. But some young people don't realize that what was funny to college buddies might not amuse a law-firm recruiter. Employers regularly research job applicants on the Internet. Some colleges are helping students prepare: Duke University hosts seminars on how to clean up a Facebook account. "You learn why posting pictures of you riding the mechanical bull at Shooters is a bad idea," says Sarah Ball, a senior whose own page is secure and clean.

Amy Polumbo, 22, restricted her page on Facebook to 100 or so people who knew her password. "It was a way for me to keep in touch with friends all over the country," she says. But after she was crowned

Miss New Jersey in June, someone downloaded pictures of her and threatened blackmail. She thwarted the attempt by releasing the photos herself (they're quite innocent) but suffered weeks of embarrassment.

"I know how easy it is for someone to take advantage of you on the Internet," says Polumbo. "The Web is a place where people can destroy your reputation if you're not careful."

In fact, all kinds of transgressions now are easily retrievable. An employee at a New York City bank watched his reputation shrink when his colleagues pulled up an article from a small-town newspaper about his drunk-driving arrest two years earlier. Divorce lawyers have been issuing subpoenas for electronic tollbooth records to use in custody cases. (You say you're home at 6 p.m. to have dinner with the kids, but Fast Lane says you're getting off the Massachusetts Turnpike at 7 p.m.) Abbe L. Ross, a divorce lawyer in Boston, finds a gold mine in computers: financial data, e-mails, what Web sites a soon-to-be-ex spouse looks at and for how long. "I love to look through hard drives," she says.

Details about you already are stashed in enormous databases. Unless you pay cash for everything, data brokers almost certainly have compiled a profile of you that will be bought and sold dozens of times to marketers and direct-mail firms. "There's almost nothing they can't find out about you," says Jack Dunning, who worked in the junk-mail business for 35 years. Right now, there are roughly 50,000 such lists for sale in a $4 billion a year industry. Now junk mail is going digital: Companies can use personal profiles and records from Internet search engines to tailor advertising—both what you see and precisely when you see it—to individual consumers.

And new databases are being created all the time. Most of the major proposals for health-care reform, for example, include compiling medical records into easily and widely accessible digital files. In July, the FBI requested $5 million to pay the major phone companies to maintain logs of your calls—information the Feds can't legally stockpile themselves but might find useful later.

Surveillance cameras are increasingly ubiquitous in our post-9/11 world. Indeed, New York City plans to ring the financial district with them, as central London did several years ago.
Of course, there are upsides. London's network of cameras helped capture failed car bombers in June. And streamlined electronic medical records would make health care safer and more efficient.

Still, most experts say we need to be vigilant about the increasing encroachments on our privacy.

The ability to collect information and images has outpaced the security available to protect them. Since January 2005, nearly 160 million personal records have been stolen or inadvertently posted online.

And even if information stays secure, the big question remains: Who should be allowed to access these databases? The FBI might find evidence against a few bad guys in millions of phone records, but the government could track all of your calls too. (President Bush has acknowledged that the National Security Agency tapped phone calls, though whose and how many is unknown.)

Even more disturbing: All of those data files can be linked and cross-referenced. At the 2001 Super Bowl in Tampa, fans were scanned with cameras linked to facial-recognition software in a hunt for

suspected terrorists. Some privacy advocates worry that police could videotape anti-war marches and create a library of digital faces or start mining Web pages for personal information.

Kevin Bankston was only caught smoking, but he's worried about larger implications: "The issue isn't whether you have anything to hide," he says. "The issue is whether the lack of privacy would give the government an inordinate amount of power over the populace. This is about maintaining the privacy necessary for us to flourish as a free society."

How To Protect Your Privacy
No one is going to protect your privacy for you. Here are some ways to take control:

Be stingy with personal information. Don't readily give a cashier your address, phone number or Social Security number. Always ask how the information will be used.

Be vigilant in cyberspace. A basic firewall is a must for your home computer. Never give any personal information in response to an e-mail.

Practice anonymity. Want the benefits of the grocery store's discount card without leaving a record of every Twinkie you buy? Ask to sign up as A. Nonymous.