Computers privacy problems essay

James Fallows explained In his essay, “ Toll underwear,” how much previously dewed information is stored inside a computer, or elsewhere like an IP address. It is mind blowing how much personal information is saved or transferred to another device.

There are many people who feel that their information was pretty safe knowing that all of their mobile devices required a postcode to use them. But, that Is not necessary true when people use a public WI-IF. Let us say I walk Into a McDonald’s with my mobile device, and use their free Wi-If. The information I view while connecting to McDonald’s Wi-If is stored on McDonald’s IP address. That information loud be- E-Mail and Backbone log In, bank and credit card numbers, and anything we search for on the Internet. If someone knew what he or she were doing, he or she could log on to McDonald’s Wi-If and take the stored information.

What makes it worse is any time someone puts information on his or her mobile device, that Information Is stored. James Fallows explains It as, “ cookies, old files, unfortunate browsing histories, and other potentially compromising data left on a machine. So. If I am at home and I filled out my bank information on my computer, and then take the imputer to McDonald’s, that information is viewable to anyone sharing McDonald’s Wi-If. Everything that Is viewed, both before and during using the public Wi-If, is at risk of being hacked.

It Is Impossible to completely protect all private Information, but I can recommend some techniques that can help prevent private information from being seen by unwanted viewers on a public Wi-If. Obviously, the people

using the public Wi-If need to be careful about what information they pull off the Internet. I recommend waiting to pay credit card bills at home. Remember, any Information viewed on a mobile device is stored on that mobile device's cookies and the public Wi-If's IP address. Another technique public Wi-If users can do is deleting their cookies before they connect on the public Wi-If.

Information that is viewed on a mobile device is stored on that mobile device. If the cookies are not deleted before the mobile device connects on a public WI-IF, then any previously viewed Information on that mobile device can be access by someone sharing that Wi-If. The problem tit that technique is Americans do not always think to delete their cookies before they connect to a public Wi-If. Students are not Involved In protecting themselves with using public WI-IF. Students connect to public WI-If's all the time, and It does not seem to be any problems.

There are not too many people who actually know how to steal someone's public information over a public Wi-If. The odds of someone ' OFF students should worry about someone stealing their information. But identity theft does happen, most likely to students who are careless. If students really do not want their private information stolen, they should be careful. How involved students should be when protecting themselves when using a public Wi-If, really depends on how much that student wants to protect his or her information. Not only is it dangerous to privacy when using a public Wi-If, it also effects the privacy when using the internet at home. Just like a public Wi-If, the internet connection at a home has an IP address.

James Fallows explains in his essay, “ Tinfoil Underwear,” that an IP address is similar too telephone number. Telephone numbers and IP address numbers are both made up of random numbers that can easily track the owner. As most people should know, telephone companies keep track of every call that is dialed or answered. Cell phone companies will also keep track of text messaging and other applications usage.

Like telephones, an IP address keeps track of all of the internet information that is sent or received. An IP address specifically keeps track of every E-mail, social networking comment, photos uploaded, bank account information, and much more. Even if the cookies are deleted, the information is still saved on the website that was visited. A majority of the time, an IP address can be tracked to an owner, whether it is from someone’s home internet or someone’s paid Wi-If service. Someone could only use a public Wi-If for internet service without being track, but that would be a big hassle.

There are some good things about the computers saving the information we view. For example, if someone was searching how to make a bomb, knowing how to track that person down could prevent a terrorist attack. Other Han that, it makes me really nervous about how all of my private information is saved on a computer or someone else’s website. I cannot imagine who can view my private information. I would prefer it if every move I made on the internet was untraceable.

Surveillance cameras are also a major problem in privacy, according to the American public. Sherry Turtle, in her essay, “ How Computers Change the Way We Think,” explained about how students are losing their right of

privacy. Turtle wrote that today's students " accustomed to electronic surveillance as part of their lily lives. Turtle felt that students were uninterested in violations of privacy and the increased of surveillance.

I disagree with Turtle on students being uninterested on privacy and increasing surveillance. At my senior year at Larry A. Role High School, my school installed video cameras in the hall ways and some other places in my school. I remember many of the students complaining about how the video cameras were an invasion of their privacy. However, I was calm about the new cameras. Sure, I felt weird, knowing that someone was watching me, but I always felt eke the cameras were more for tracing back for vandalism or big fights.

It was not like the school had a guy watching the camera screens all day. Cameras are k for public places, but the day the government places cameras inside my home, is the day I will become very upset. There are many privacy issues that are out of American society's control. But there is a lot, as individuals, we can do to help with privacy. A majority of Americans have a Backbone account, in which they have complete control over privacy, except for the internet hackers. Backbone has tab that is specifically for rivalry. We can choose who we want to see our Backbone posts or contact majority of Backbone members who have over five hundred friends, really have fake friends.

If a person accepts a friend request from anyone, or even sends out a friend request to every acquaintance that he or she knows, then that person is inviting Just about anyone to look up his or her life events. If a Backbone user

is worried about privacy, he or she should limit their Backbone friends to people who they would trust Ninth their home address. The information social networking users put on their accounts is their choice.