Philip Peng
CIS 125
Matt Blaze, Christopher S. Yoo
April 26, 2011

Digital Transparency
The Next Step After Digital Privacy

What is Digital Privacy

On April 20th, 2011, Free Software Foundation founder Richard Stallman came to University of Pennsylvania to give a speech titled "A Free Digital Society" (Stallman). In his talk, Stallman touched on a heated topic dating back long before even the invention of the internet: digital privacy. Privacy can be defined as a person's privilege, or, in some states where law enforces it, a person's right to non-disclosure of personal information. This includes personal details and background such as views, actions, location, and even history. Digital privacy pertains to the availability of an individual's private information in digital form via the internet and electronic tracking or communication devices.

> As written in the US Constitution, the Fourth Amendment to the Bill of Rights is as followed:
> *Amendment IV – 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.*
> ("Bill of Rights")

Having being written and approved over 200 years ago, the Fourth Amendment gives the rights of privacy of US citizens within their homes, but it does not protect against the recent invasions of personal privacy brought upon us by the advancements of technology over the past 100 years.

Especially with the proliferation of data collection and our daily reliance on technology in this post dot-com information age, the protection of private information has become an ever-growing issue.

We now live in an age where Facebook has become an imminent factor in social interactions and Google has allowed us to easily access a plethora of archives and databases previously inaccessible by physical means. It is unsurprising then that, while governments and corporations around the world jump at this opportunity to harvest such rich resources, society campaigns and fights to prevent such information from becoming public. *Privacy.org*, for example, tracks and publishes stories and articles about privacy infringements on a daily basis. But at what point does our fight for privacy become so radical that it blinding and even irrational? In a world where privacy is a technological impossibility, are our efforts to protect our digital privacy working?

Stalin's Dream

In his "A Free Digital Society" speech, Stallman likened our world of digital technology today as, in his own words, "Stalin's Dream" (Stallman). Joseph Stalin (1879-1953) was the communist leader of the Soviet Union (USSR) from 1941 until his death in 1953 ("Biography: Joseph Stalin."). During his iron-fist rule of the Soviet regime, Stalin introduced numerous policy reforms that empowered the military to build a vast information and espionage network feared by both those inside the USSR and out. Stallman compared today's digital networks on ordinary citizens to the surveillance networks in place in the USSR over 50 years ago, arguing that that digital information traffic today is a grave threat to our freedom and privacy. Except unlike in the days of Stalin where perpetrators had to force information out of their victims through violent physical means, we willingly record our personal information in readily-accessible digital form.

When one looks at the amount of personal information stored through digital means today, it is difficulty to disagree. Lets take a look at Microsoft's Windows operating system (OS) for example. For the past many years, Microsoft Windows has been the top OS used both consumers and industry worldwide. When it comes to digital privacy, however, Microsoft's track record is anything but clean. In 2002, the Federal Trade Commission (FTC) filed charges against Microsoft for failing to "properly protected the privacy and security of people who provided personal information through the company's online identification services," declaring that Microsoft had "lied about the effectiveness of its measures to protect users' personal information" (Schwartz). Consequently, Microsoft agreed to being monitored for the next 20 years to ensure that privacy conditions laid out by the consent order would be met. Effectively, Microsoft was being legally forced to actually comply with the privacy policies that users had signed when they agreed to using Microsoft's services.

Despite the closed source nature of the OS and having a long history of privacy infringements, users continue to use Windows as their primary operating system, with OS market shares steadily hovering at 90% (NetMarketShare). These users freely accept privacy policies pushed forth onto them without ever knowing or being able to find out what security measures Microsoft uses to enforce such policies. With so many users entrusting their personal information to large corporations such as Microsoft, how can we ensure the protection of our data from surveillance? The fact is, unless stronger legislation is introduced forcing companies like Microsoft to fully disclose what they are doing to protect such info, is we can't. Before FTC's intervention, there was no insurance for users on the protection of their privacy apart from the blind trust. Unless changes are made to force the disclosure of privacy-protection methods, the information we willingly give to companies such as Microsoft may

easily be compromised. If only there existed some way to **clarify** the integrity of such privacy-protection methods.

The potential leaking of private information is not restricted only to the internet, however. Another prime example of digital technology that threatens our digital privacy are cell-phones. These technological wonders have made life extremely convenient. Both portable and wireless, cell-phone users can easily access their daily schedules, emails, and even GPS location. What most users forget, however, is that others can too. When surfing on 3G/4G networks or even while using wifi, users are constantly transmitting and receiving data through wireless means. But what insurance do these users have in knowing that their data won't be collected by third parties and used for other purposes without their consent? The scary answer is: currently none.

Just last week, the American Civil Liberties Union (ACLU) pinned Michigan police on their use of devices claimed to be able to snoop into private cell-phone data. These portable “extraction devices” are capable of bypassing security passwords and downloading text messages, photos, videos, contacts, and even GPS information from nearby cell-phones in under two minutes, all without the knowledge or consent of the cell-phone owner (Hickey). Not only does this clearly violate the Fourth Amendment, but Michigan police have refused to disclose the details of their use of such devices. In essence, the police could be reading through your private emails just by walking by. Unless the method of data extraction is made public, cell-phone users would have no way of protecting themselves against such privacy intrusions. In response to ACLU's petitions, the Michigan police has offered to comply, but with a “processing fee” of $500,000, a cost many-fold the total cost of all the devices themselves (Hickey). Why is it necessary that we are forced to pay to find out about how information about us is being

collected? More importantly, why isn't there anything forcing the police to make their methods more **transparent**?

The US Government and the FBI

A federal government can be described as a political organization given the authoritative power to approve legislative policies that can control and change the state of a country. It is assumed, or rather, hoped, that governments carry out actions with the interest of its citizens first in mind. The US government is elected by US citizens and thus entrusted with the responsibility of representing our concerns. Can one then can assume that we should accept and agree on everything the US governments does? After all, governments listen and are there for the people, right?

While one can argue that it is hard and often impossible to carry out actions that will satisfy everyone, there is a difference between acting in the best interest of the majority of the population and acting in the best interest of the government itself. When it comes to digital privacy, however, its difficult to accept the illusion of our government always fighting “for the greater good”. There are many historical cases where government agencies have overstepped boundaries and invaded personal digital privacy without our consent. The greatest perpetrator of such actions is none other than the FBI: the “Federal Bureau of Investigation” or what I call the “Federal Bringer of Insecurity”.

One such digital privacy infringement was well documented by *Washington Post* writer Barton Gellman. In his November 6th, 2005 article titled, “The FBI's Secret Scrutiny”, Gellman unveils the FBI's unfounded and frightening investigations and cross-examinations into the lives of ordinary Americans (Gellman). In his article, Gellman tells the tale of George Christian, an everyday sysadmin

in charge of managing the digital records of three dozen Connecticut libraries. In the summer of 2005, Christian was approached by FBI agents with a letter demanding that he surrender “all subscriber information, billing information and access logs of any person” who used one of the computers under Christian's control. In addition, the letter threatened Christian to not tell anyone of the content of this letter.

As an FBI-stamped letter is considered a national security letter, the FBI did not not need the approval of any judge. National security letters (NSLs) were created in the 1970s for the purpose of espionage and terrorism investigations and enabling bypassing of consumer privacy laws (Gellman). Following the 9/11 terrorist attacks on the twin towers, the US government, under Bush administration, passed an act entitled “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001”, also known as the “USA Patriot Act” (“Public Law 107”). Since the introduction of the Patriot Act, the FBI has abused the powers enabled by NSLs to secretly spy on the private lives of ordinary US residents and visitors, even without evidence or allegations indicating possible terrorism involvement. With the FBI issuing over 30,000 NLSs every year (Gellman), the US government has empowered themselves with the ability to unsolicitedly review the records of average Americans, much of which is stored and can easily be accessed in digital form.

Luckily, not only did Christian refuse to hand over such sensitive records, but his employer, Library Connect Inc., filed a public lawsuit against the FBI protesting the unreasonable demand. With the assistance of the ACLU, the FBI eventually dropped the effort. In their responding letter, the bureau wrote that they “will not seek to enforce the national security letter delivered to your client, Library Connection, Inc., by FBI personnel on or about July 12, 2005” (Waterman). Ann Beeson, Associate

Legal Director of the ACLU, applauded the result, pointing out, "while the government's real motives in this case have been questionable from the beginning, their decision to back down is a victory not just for librarians but for all Americans who value their privacy" ("Government Drops Demand for Library Records"). While this was a landmark victory for Americans across the country, it is also a stark reminder of the dangerous powers that government can exert in invading the digital privacy of the innocent in the name of "justice". The scarier part is, had Christian and his employer not brought this issue to light, we the public would never have known about it. The potential dangers that tools such as NLSs can bring are far from **clear**.

The Invisible Bogeyman

"For your protection" and "to protect the people" are often the phrases that government officials will respond with when asked privacy questions. In an ideal world where the government is a transparent and trust-able figure, this may be acceptable; however, as pointed out earlier, they are far from it. Ever since Bush's introduction of radical "public protection" policies, the government has done a great job of instilling fear into the public of potential terrorist attacks threatening the lives of Americans. The sacrifice in exchange for this "protection", however, is our privacy. But is giving up our personal privacy really necessary in fighting the dangers of terrorism, or are we being brainwashed by propaganda?

As Stallman puts it, the government "will always say, 'If only we could collect all the information about everything, our job would be easier.' It sure would, but we can't tolerate their jobs being too easy as that would be very dangerous" (Stallman). The dangers that Stallman refers to are not those of the "bogeyman" terrorists that governments always insist lurk in every corner, but rather the

dangers that governments can inflict by gaining access to your information and using it without your knowledge. Yes, its possible that your neighbour could be a terrorist. In fact, there's even a chance that you may be one. How large is that chance? Arguably much, much smaller than the measures the government has taken warrants.

After the September 11th, 2001 attacks on the US World Trade Centre, the total death count tallied by New York officials amounted to 2,752 ("New York reduces 9/11 death toll by 40"). In response to this act of terror, the Bush administration declared war on Afghanistan, and later Iraq. While official numbers are always dubious and always grossly underestimated, rough estimates Afghan citizen deaths due to the war float at almost 3,000 (Herold) and Iraq civilian deaths at over 100,000 ("Iraq Body Count"). In the meanwhile, recorded US fatalities amount to 1,407 and 4,768 in Afghanistan and Iraq respectively ("Iraq Coalition Military Fatalities By Year / Afghanistan Coalition Military Fatalities By Year"). Just the American death total alone is double that of 9/11's, yet the government continued to insist that their actions were in the best interest of saving American lives. And the general public continue to buy it.

How does this have to do with our digital security? While we may argue that whatever happens in a far away country is none of our concern, we still allow the government to use the reason of terrorism to do whatever they want, including over-collection and introducing the potential of abuse of our information. On September 21, 2001, only 10 days after the attack, Oracle CEO Larry Ellison called for the creation of a national ID system, offering to donate the (Oracle-written) software for implementing such a system (Black). Not surprisingly, the population was heavily in support of this; a poll conducted by the Pew Research Centre for the People & the press revealed that "70% of Americans

said they favored a law requiring citizens to carry a national ID card at all times that would have to be produced upon request to a police officer" (Black). But would such a radical system actually work in preventing future terrorism? Would forcing the terrorists onboard the 9/11 airplanes to carry an extra ID card have prevented the attacks? Absolutely not. All such a system would do is empower police officers to walk up to any law-abiding citizen and be given access to their identity, as well as other private information, all under a legal umbrella. There are a lot more effective and less costly methods of increasing national security without requiring citizens to sacrifice their personal privacy.

By over-exaggerating the dangers of terrorists and claiming that their actions will prevent further deaths, despite numbers indicating otherwise, the government spoon-feeds us excuses that allow them to carry out excessive privacy-invading actions. Because we have allowed ourselves to accept the threats of these "invisible bogeymen", we accept these privacy-invading actions without question like sheep. As Stallman comically points out, "Why don't we have a global war against car accidents? I assume that's because it wouldn't serve any other ulterior motive" (Stallman). Its important that we prevent ourselves from being mislead by propaganda and giving up our privacy in fear of **invisible** bogeymen.

What Do We Really Want?

According to Facebok founder Mark Zuckerberg, the age of privacy is over. In his six-minute interview with TechCrunch founder Michael Arrington, Zuckerberg points out, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. The social norm is just something that has evolved over time" (Kirkpatrick). Despite all the vocal opinions that people express about wanting to protect their privacy, the reality is, most people

don't actually care that much.

In a recent experiment by web software expert Gary LosHuertos, LosHuertos visited a random cafe in the middle of New York City and pulled out his laptop. LosHuertos started up a spying program for snooping on users using Facebook through the cafe's free wireless, then notifying the users through their own Facebook accounts that they had been hacked. Instead of seeing expressions of anger or furious typing, however, his victims ignored the warnings and continued on surfing the web. One victim even continued shopping on Amazon. LosHuertos was absolutely stupified; “What's absolutely incomprehensible is that after someone has been alerted to the danger (from their own account!) that they would casually ignore the warning, and continue about their day” (Sullivan). It was as if his victims really just didn't care. As long as the invader didn't spam their Facebook Wall, privacy to them was nothing more than a catch phrase.

Consumer behaviour studies agree. Research by privacy expert Larry Ponemon showed that two thirds of American adults are “privacy neutral” and, while they claim to care about privacy, they “barely lift a finger in an effort to preserve it” (Sullivan). Why is it that so many Americans feel so passionate about such an important issue, but do nothing to help it? Privacy expert Alessandro Acquisti explains; “the more technology savvy among us have this feeling that we're giving it up, but we realize it is close to impossible to protect your personal information, not even if you start living like the Unabomber in a cabin. If you want to function as a normal person in society you have to.” (Sullivan). The reason the average American does next to nothing to protect his/her privacy is simple; trying to “do something” is either too hard or futile. We live in a digital age where we rely on services and technology that we often have no clue about and outside our control. The current state of our privacy is lies on whether or not we

are willing to inconvenience ourselves to protect information that will probably be accessible through some other mean one way or another. Telling a person to not use Facebook, for example, is impractical as the social benefits of using such a service often outweighs the loss what little privacy still exists. What path, then, should we take to break these dense and **impenetrable** barriers?

What is Digital Transparency

Lets step back and look at the issue of privacy from a philosophical view. Privacy focuses on the protection, or rather, *hiding* of personal information. But why should we be so secretive of information such as our location and who our best friends are? One can argue that we should actually be willing to give up our personal information. We should not be afraid to let our actions be known. We do things because we want to or because we believe in the things we do. There is no moral reason to hide ourselves; hiding would indicate that you are trying to pretend to be someone else or trying to prevent others from seeing who you really are. If we are demanding for privacy, it means that we have something to hide. If we believe it to be something that we have to hide, then its probably something bad that we should not have done in the first place. Returning to reality, however, there do exist dangers in revealing certain information such as financial information, criminal records, and even political views. But why should it be different whether you reveal your political views, for example, to the government or to your best friend?

The true danger of digital information is not the possession of such data but rather what is done with it. Accurate information is the key to making informed decisions. Whether this information is "good" or "bad", however, depends on the motives of the decision maker. Despite entrusting the government to making good decisions for us, rarely do we see the process that lead up to such

decisions, only the results. More important than trying to protect our privacy is finding out what is done with such information. If asked for information about your health records, for example, it is important to know whether that information is being used for anonymous surveys to help improve healthcare or if it will later be used against you in future employability.

Our focus should not be the prevention of the spread of information, but rather preventing its misuse. **Digital transparency** in terms of privacy can be defined as the level of openness and disclosure of how digital data is collected and used. Full digital transparency of government and corporate data collection will allow us to clearly understand what is being done with our private data and how it may affect our lives. If we see the impacts being negative, we can easily raise the red flag and protest against such actions. We should not be afraid to give out our information if we can clearly see that such information is not being abused. Instead of fighting for digital privacy, what we should really be fighting for is digital transparency.

2011: The Year of Digital Transparency

After years of petitioning and public fights for greater privacy protection, the hard work may finally pay off. A few weeks ago, senators John Kerry and John McCain formally introduced the "Commercial Privacy Bill of Rights Act of 2011" (Wolf). If approved, the powerful new bill will impose major and significant obligations on businesses on the transparency of their information collection.

If passed, the new bill will force companies to clearly and concisely disclose all usage of "personally identifiable information" or "PII" (Wolf). A mechanism for individuals to access and

correct their PII will also be required if any is collected (“Significant New Online Privacy Legislation”). Some form of “opt-in” consent from the user will be required for third-party access or public display of sensitive personal info, and an “opt-out” option must be made available as well (Wolf). Effectively, this bill will explicitly force corporations, particularly those offering online services, to implement greater transparency of how they handle private information, as well as give users clear control of the level of visibility of such information. Any third party wishing to access an individual's PII will be legally prohibited from doing so without explicit opt-in consent. No more worries of advertising companies gaining access to your phone number because “it was in the fine print”!

The bill will also give the FTC new powers and responsibilities to monitor and introduce rules concerning the actions of “covered entities”, defined as “any person that collects, uses, transfers or maintains covered information concerning more than 5,000 individuals during any consecutive 12-month period” (Wolf). Not only will such covered entities be under FTC jurisdiction, but so will non-profit and telecommunication carriers. These organizations will have to introduce new processes to respond to non-frivolous complaints and programmatically describe the process upon FTC request to ensure compliance with standards. Details of methods of providing information collection notices will also fall under FTC rulemaking.

So what does this mean? The FTC will no longer need to request the compliance of Microsoft for supervising its privacy policies; the FTC will now explicitly have that responsibility. The police will no longer be able to fly-by analyze your cell-phones as such information will be classified as PII. Depending on how “national security” interests conflict with the new bill, there's a possibility that librarians such as Christian will be able to easily refuse surrendering privacy information on the

stronger basis that he does not have the legal right to. While the new bill won't help prevent misleading government propaganda, it may allow for greater transparency in exact usage of data collected during so called “security background checks”. Even for the lazy, personal privacy will be greater protected as services will no longer be able to slyly bundle in privacy agreements in the long Terms of Agreements' but rather have explicit opt-in/opt-out settings clearly visible and accessible.

Needless to say, the “Commercial Privacy Bill of Rights Act of 2011”, if passed, will most definitely revolutionize online information traffic. The bill will not just ensure greater digital privacy protection; it will introduce and enforce digital transparency. No longer is privacy a matter of ambiguous personal trust in the service provider. With the bill, a new standard will be put in place. What practices will be considered acceptable or not will be clearly defined in legislation. Users will no longer have to worry about not knowing who will have access to their online information or how it will be used. After years of stagnancy, the US government has finally picked up its act. Its time we do too. If the new bill means that digital transparency will finally be realized, we should do whatever we can to push it forward. Shift our fight to digital transparency: the next step after digital privacy.

Works Cited

"Bill of Rights". Cornell University Law School. <http://topics.law.cornell.edu/constitution/billofrights>.

"Biography: Joseph Stalin." PBS. 1999. <http://www.pbs.org/redfiles/bios/all_bio_joseph_stalin.htm>.

"Government Drops Demand for Library Records." American Civil Liberties Union. 26 June, 2006. <http://www.aclu.org/national-security/government-drops-demand-library-records>.

"Iraq Body Count." Iraq Body Count. 8 April, 2009. <http://www.iraqbodycount.org/>.

"Iraq Coalition Military Fatalities By Year / Afghanistan Coalition Military Fatalities By Year." iCasualties. 2009. <http://icasualties.org/>.

"New York reduces 9/11 death toll by 40." CNN US. 29 October, 2003. <http://articles.cnn.com/2003-10-29/us/wtc.deaths_1_death-toll-world-trade-center-names?_s=PM:US>.

"Public Law 107." US Government Printing Office. 26 October, 2001. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html>.

"Significant New Online Privacy Legislation Introduced in Congress as the FTC Presses Ahead with a Novel Enforcement Action Against Google." Sidney Austin LLP. 26 April, 2011. <http://www.sidley.com/sidleyupdates/Detail.aspx?news=4799>.

Black, Jane. "Don't Make Privacy the Next Victim of Terror." Business Week. 4 October, 2001. <http://www.businessweek.com/bwdaily/dnflash/oct2001/nf2001104_7412.htm>.

Gellman, Barton. "The FBI's Secret Scrutiny." The Washington Post. 6 November, 2005. <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html>.

Herold, Marc W. "Towards America's Electronic, Troop-less Wars." Global Research. 1 March, 2010. <http://www.globalresearch.ca/index.php?context=va&aid=17868>.

Hickey, Matt. “ACLU wants to know how Michigan cops use 'data extraction devices'.” cnet News. 19 April, 2011. <http://news.cnet.com/8301-17938_105-20055431-1.html>.

Kirkpatrick, Marshall. “Facebook's Zuckerberg Says The Age of Privacy is Over.” Read Write Web. 9 January, 2010. <http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php>.

NetMarketShare. “Top Operating System Share Trend.” NetMarketShare.com. 25 April, 2011. <http://www.netmarketshare.com/os-market-share.aspx?qprid=9>.

Schwartz, John. “Settling With F.T.C., Microsoft Agrees to Privacy Safeguards.” The New York Times. 9 August, 2002. <http://www.nytimes.com/2002/08/09/business/technology-settling-with-ftc-microsoft-agrees-to-privacy-safeguards.html>.

Stallman, Richard M. “A Free Digital Society.” Science and Technology Wing and Dining Philosophers. University of Pennsylvania, Philadelphia, PA. 20 April 2011. <http://www.stwing.upenn.edu/~pengp/Files/Stallman/>.

Sullivan, Bob. “Why should I care about digital privacy?” msnbc.com. 3 October, 2011. <http://www.msnbc.msn.com/id/41995926/ns/technology_and_science/>.

Waterman, Shaun. “National-Security Letter to Library Group Dropped.” The Washington Times. 26 June, 2006. <http://www.washingtontimes.com/news/2006/jun/26/20060626-110156-3734r/>.

Wolf, Christopher. “Draft 'Commercial Privacy Bill of Rights Act of 2011' Published.” Hogan Lovells. 23 March, 2011. <http://www.hldataprotection.com/2011/03/articles/consumer-privacy/draft-commercial-privacy-bill-of-rights-act-of-2011-published/>.