Group 1 Question and Answers

Senior Seminar, Fall 2013 w/ Dr. Shankar

Aaron Richter, Christopher Fernandez, Paul Lewis

1. Dr. Shankar -Comment on open source tools **Paul**
   1. There are a number of good open source tools available in each of the domains we covered in our presentation. For cloud computing, a few of the big names now are OpenStack ([http://www.openstack.org/](http://www.linkedin.com/redirect?url=http%3A%2F%2Fwww.openstack.org%2F&urlhash=m-rg&_t=tracking_disc)) and Apache CloudStack ([http://cloudstack.apache.org/](http://www.linkedin.com/redirect?url=http%3A%2F%2Fcloudstack.apache.org%2F&urlhash=5A6O&_t=tracking_disc)). Ubuntu has a number of cloud related services like Juju for automating cloud services and One for storage and synchronization between devices. There's an opensource social networking project called diaspora\* that I've meant to check out ([https://diasporafoundation.org](http://www.linkedin.com/redirect?url=https%3A%2F%2Fdiasporafoundation.org&urlhash=-ZwE&_t=tracking_disc)). Users of diapora\* can run their own diapora\* server or join an already existing one, and this aims to keep users' data in places that they feel comfortable/trust to keep it. It's also supposed to support cross-posting to other sites like FB, Twitter, and Tumblr. RapidMiner is a huge name in data mining. As far as maintaining privacy, Bruce Schneier made a great post on the Guardian ([http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance](http://www.linkedin.com/redirect?url=http%3A%2F%2Fwww.theguardian.com%2Fworld%2F2013%2Fsep%2F05%2Fnsa-how-to-remain-secure-surveillance&urlhash=x44a&_t=tracking_disc)) and lists good tools like TOR and TrueCrypt, along with practices he follows to help stay secure.
2. Group #2- Question: With the way cloud computing is growing, do you think it will be possible that the government would be able to find ways to gain access to our private data more easily? - **Aaron**
   1. The government already has relatively easy access to our data. The government can serve a subpoena to a cloud storage company to force them to hand over data stored on their servers. This, therefore, is not a matter of technical advancement, but political policy. Regardless of the technology in place, it is up to lawmakers to determine how easily they can retrieve private data. With the growth of cloud storage, however, more and more data is stored on the cloud, widening the pool of data that the government could potentially access. This makes it easier for the government to retrieve data- rather than having to seize an individual’s personal computer, the government can just seize the information store on a cloud company’s server, completely bypassing the creator of the data (in this case, a private individual).
3. Group #3 - Question - What countries around the world offer more privacy protection for it's citizens? What are some of their policies and laws that enforce this protection? - **Paul**
   1. In the short time I've spent looking into it, two countries I've noticed with interesting privacy laws are Germany and South Korea. It seems like the EU requests all of its member countries to establish their own privacy laws, but Germany was apparently the first in the world to establish laws protecting personally identifiable information. Check out Bundesdatenschutzgesetz, or BDSG. Some things that stuck out to me about it are it saying data collected must be done from the individual themself with their express permission, and they can state how long the data can be stored and for what purpose it may serve. In South Korea, check out the Personal Informationa Protection Act (PIPA) and the IT Network Act. Businesses are required to have personal data management officers when collection occurs, and businesses must take means to protect the data in case of intrusion. The laws includes definitions on personally indentifiable information, not leaving out images of the individual, their voice, and information used in conjuntion with other data that could indentify the individual.
4. Group #4 - Question - What impact will the consumerization of IT have on privacy? Many companies are now implementing BYOD strategies and using products such as SCCM to manage PC's and mobile devices. Employees would like to be able to access corporate resources from personal devices. How much privacy should an employee be afforded in this case? How much control should a company have over those devices? **Aaron**
   1. Cloud computing and the consequential outsourcing of IT may actually improve employer-employee privacy relations. IT now does not reside on-site, so the employer may not have direct access to an employee’s private data as they would have if the data was stored on-site. This also relieves potential conflicts of interest, as on-site IT personnel may be persuaded by their employer to release certain private data. With an outsourced IT environment, the cloud company’s personnel operates within a definite privacy contract and will not breach it. With BYOD strategies and management software such as SCCM, employees and employers should agree to separate personal and corporate data. This can be as simple as having different folders for personal and work use, or even different bootable environments (on computers, many mobile devices don’t have that functionality).
5. Group #5 - Question - When it comes to the Terms & Conditions that users agree to, what kind of privacies are the users allowed to have when agreeing to use a web service and how do the web services commit themselves to protect user's personal information? **Chris** 
   1. Usually depending on the web service, every web service has a different terms of agreement an different policies to abide by when you agree to the Terms & Conditions. For example, Twitter states that you retain your rights to any Content you submit, post or display on or through the Services. When you submit anything on Twitter, you grant them acces to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods. The information you put on Twitter is yours but Twitter can use your information. Web services protect user information by creating policies and agreements with third party groups and advertisements that want user information so they do no harm with the user information they obtained from the web service and to protect themselves.
6. Group #6 - Question - With "online trails" becoming longer and more visible, is it possible to "clean up"? Perhaps not with regard to the NSA, but in terms of everyday information left lying around the internet, in an effort to maintain a level of privacy. - **Paul**
   1. I would say there's a difference "cleaning up" and practicing things to minimize what gets left behind online. Rule of thumb: once something is out online, don't assume it will ever go away or not be noticed. In this sense, it is very hard to clean up. This applies to posts on social media sites, forums, blog posts, comments on YouTube, etc. If someone cares enough, they could try to connect these all together to link back to you. But, since this situation shouldn't really apply to many of us, say we want to make it harder for businesses to profile us with our online activity. We can take steps like disabling cookies (fairly impractical for everyday use), using private mode in browsers (not too impractical), enabling Do Not Track (DNT) in your browser (good for your personal devices), and using a plug-in like NoScript to limit what sites can run scripts in your browser.
7. Group#7-Question: - What is the best practice of Privacy 2.0 to avoid companies or third parties websites that publish private records, physical address and location of the user? **Chris**
   1. When signing up or using a web service make sure to read the privacy policies and see if it states anything about how they use your data and what data they collect. Also, there should be a settings link to disable your data as public instead of private. If you're using an “always on” network connection, make sure to install and maintain a firewall. Firewall software prevents your computer from hacking and remote attacks. Manage your passwords responsibly. Do not provide more personal data than you are comfortable with.
8. Group #8 - Question - What are the main differences between an IaaS model and PaaS model, and which one is better for scalability? - **Aaron**
   1. IaaS stands for Infrastructure as a Service, relating to the physical arrangment and storage of data, along with the underlying hardware framework. Rather than every company housing servers, this hardware is outsourced to cloud companies (such as Google, Amazon, or Microsoft) and provisioned according to the client’s needs. PaaS stands for Platform as a Service and sits on top of the infrastructure in IaaS. The cloud company offers development tools (such as databases, web servers, and application deployment tools), again provisioned according to the client’s needs. Therefore, IaaS and PaaS are not mutually exclusive, but designed to be use in tandem with one another. The scalability issue is solved with these clouds service models: SaaS (Software as a Service), IaaS, and PaaS. The infrastructure and platform is provisioned according to the needs of the client company. Scaling up or down is merely a software feat rather than introducing new hardware to the equation. Software is then built on top of this scaling platform, allowing end-users to seamlessly use software built on the cloud.
9. Group #9 - Question - Even though some people do not agree on how the "U.S.A Data Mining and Gathering Programs" are being used, if we look at things another way, which aspects of society (or problems in society) can the U.S.A Government improve (solve) with the resources and data that such programs provide them with? **Chris**
   1. The U.S.A government can gather user data from many web services and can help with preventing future crimes and help with preventing terrorist attack. They can use the data to implement two different types of users; clean users and watched users. Clean users would be users that show no signs of threat within the internet, and watched users that should be watched and carefully examined.

Questions

1. Money 2.0 - **aaron**
2. Media 2.0 - Chris done
3. Paul - Agile Web (?)
4. Aaron - Office2.0 / The synchronized web
5. Chris done
6. Paul
7. Aaron
8. Chris