Facebook's Privacy Policy: https://www.facebook.com/note.php?note_id=+322194465300

Facebook is an online social networking service. The original concept for Facebook remains somewhat of a mystery, but Facebook as we know it today began in 2004 when Harvard University student Mark Zuckerberg launched what he called "thefacebook," which was an online tool for fellow Harvard students to connect and share photos of themselves around campus at school events. The idea soon spread to other colleges, and eventually the public, and by late 2011 there were more than 500 million users, which, according to USA Today, represented 7 percent of the world's population. Facebook is better known as a social utility. The site offers users a variety of ways to publicly or privately share data about their life, and to find friends, classmates and others who might interest them. Users can post public thoughts on others' pages, send them private emails or chats, search for people from their past or connect with people with the same interests as them.

Facebook's privacy policy was written by the founders of the site. Facebook is a certified licensee of the TRUSTe Privacy Seal Program. This means that their privacy policy and practices have been reviewed by TRUSTe, an independent organization focused on reviewing privacy and security policies and practices, for compliance with its strict program requirements. Facebook's privacy policy was recently updated on August 29th, 2013. The intended audience for this policy would be the users of Facebook. Or implicitly, the intended audience were advertisement and third party companies that use Facebook as a media outlet. The language of Facebook's privacy policy was formal but simple, it did not use ostentatious words. Thereby, the policy could be understood by anyone over the age of 13. Thirteen being the minimum age required to join Facebook, thus legally all users should be able to understand the privacy policy. The policy is further broken down in sub sections, this makes navigation to answers to particular questions faster. Facebook's privacy policy takes into account collaborative filtering. It is explicitly stated that information from cookies is stored in order to predict what the user may enjoy and to customize advertisements for the user's enjoyment. Facebook also implements a primarily opt-in policy. Most Facebook applications are opt-in, and due to recent controversies most third party applications have been made opt-in too.

1. What data is collected and why it is needed?

   Data is collected by Facebook at many different times.

   - **Firstly, while registering for Facebook the user's Personal information is collected.** This includes the user's name, email, gender, and birth date. Users are also given the option of adding their address, phone number, current employment status, company name, university name, family members, relationship status etc.

Facebook ask for the users date of birth to verify that the user is over 13 and so that the users access can be limited to age appropriate content and advertisements. This information can be changed at any time, but the data once entered will remain in Facebook's database. This information could later be used to recommend friends for the user, friends from the same university or workplace or friends living in the same city with the same interests. This information is also shared when Facebook interacts with third party sites, such as Zynga, amazon or Instagram. Personal information can also be used by Facebook to contact the user in case of unauthorized use of the users account or in the case of sharing sensitive information.

- **Secondly, all shared Content is collected.** This includes photos, videos, links, comments, wall post contents, messages etc. All of this data has metadata linked with it, Facebook can be prevented from storing this data if the user removes this metadata before uploading any content. The Electronic Privacy Information Center (EPIC) has accused Facebook of gathering facial data from user's photos to develop a facial recognition system. Since users give Facebook access to their pictures and general content, this suit was not pressed. It did, however, open the public's eyes to how their information is being used. Facebook often use shred content to serve personalized advertising to users. For example, a user's picture with a soccer ball might prompt soccer related ads on the user's profile. If the user has location services turned on and their location is visible when posting messages, this is regarded as any content and is this freely added to Facebook's database. Any service that supports location service would have to present the user with an opt-in choice of whether they want to participate, as per Facebook's privacy policy. For example, the new Foursquare system allows the user to check in at various locations in order to gather points that can lead to a free meal or free pass for buses or the metro. Location services can also be used to find friends in the immediate area, it can also be used to find restaurants as per the users tastes (thanks to Facebook's ties to yelp) or their banks ATM's in the area.
- **Transactional Information.** Facebook often retains details about transactions or payments made. This means it has the user's credit card information as well as billing location. This information however, is added only after the required permissions have been met.
- **Cookie and Browser Information.** When Facebook is accessed from a computer, mobile phone or other device, the user's browser type, location, and IP address, as well as the pages visited are recorded. This is done so that Facebook can detect points of illegal entry or hacking better. If a user were to log onto Facebook from a new electronic device, a message pops up to verify that it is actually the user themselves. Cookie information is recorded to make Facebook easier to use, to make advertising more accurate and for security purposes Cookies are used to know when the user is logged into Facebook and also to know when the user is interacting with Facebook Platform applications, websites, widgets and advertisements. The use of cookies may be turned off to prevent this.

2. How users are notified when and if information about them is being collected? (Hint: maybe the policy is the only notification.)

   The policy is the first notification of information being used. The information listed above are all used by default. All Facebook services, such as wall posts, pictures, shared content and personal information can be used by Facebook for whatever they see fit as the user has chosen to share this information with Facebook. Third party sharing sites, Facebook platform applications, widgets and advertisements have a mandatory opt-in or opt-out policy, although users are first asked for access to their personal and shared information. Only after agreeing with the terms of the host, can the companies gain access to the user's information. Even for turning location services on, a pop up indicates that this is now done. In case of credit card information being shared, the third party company has a privacy agreement of their own that the user has to accept, and usually an email is sent to the user to indicate their participation.

3. What does the policy say about opt-in or opt-out choices for mailing lists or other communications?

   The user can choose to opt-out of mailing lists or other Facebook connect and Facebook platform lists. Most third party site services are opt-in, but advertisements and business ventures tied in with advertising such as Facebook beacon are often opt-out. Facebook beacon is tied in with Fandango, Ebay etc. and often broadcasts any traffic on the system to the user's friends and posts it on their public profile. Facebook Beacon was later changed to opt-in, as are many other advertising options. Now almost all services on Facebook are primarily opt-in.

4. How does the policy distinguish between personal information that has differing levels of sensitivity?

   Personal information like name, age, university affiliation, workplace and other publically stated information on the users profile are used freely by Facebook and shared across all third party hosts. More sensitive information like credit card information or phone number and address are only shared after permission for such is received from the user. On Facebook can further regulate the information shared through their privacy settings, if they so wish users can now hold back even public information like age and shared content.

5. How long is the data stored?

   Data is stored as long as the Facebook user remains active. Removed data will persist until 90 days after it was deleted, in the form of cookies. This information however will not be shared with anyone. Data that has been shared with another user or shared with third party hosts can never be deleted completely as the information belongs to 2 different users.

6. How does the policy address the security of personal data from unauthorized access and use?

   All data is highly regulated by Facebook. All account information in kept on a secured server behind a firewall. When the user enters sensitive information (such as credit card numbers and passwords), the information is encrypted using secure socket layer technology (SSL). Facebook also uses automated and social measures to enhance security, such as analyzing account behavior for fraudulent or otherwise anomalous behavior. Facebook may limit use of site features in response to possible signs of abuse, may remove inappropriate content or links to illegal content, and may suspend or disable accounts in case of violation reports from other users.

7. How does the policy address the accuracy of personal data?

   All information entered by the user is deemed as accurate. Facebook cannot make sure of a person's age, name or background. Once the user has used Facebook enough, the background information from the user's cookies and other activities could prove the accuracy of the data provided by the user. If at any time, a user's information is found to be inaccurate, the user is notified to either change or remove that piece of information.

8. How can customers see, and if necessary correct, personal information?

   Facebook has an option on every user's profile whereby they can change any information they see fit. The user can also control which information they choose to make public.

9. Five terms. Some of the answers to these questions depend on the interpretation of certain words and phrases. These may be everyday terms or they may be obviously special terms with legal implications. Make a list of FIVE terms that you think would need to be defined more precisely for you to be able to understand the policy in more detail. (Hint:

   An example of such a term is "personally identifying information." DON'T use this as one of your list.)

   a. Facebook uses "automated and social measures" to enhance security
   b. We use cookies to "protect both you and Facebook"
   c. "unlawful multi-level marketing"
   d. "In-network privacy features allow you to keep your information from being accessed by other users." They do not however curb third party sites once the user has given it access.
   e. Facebook "Help users share expressive and relevant content"
   f. "advertisements and we may use any of the non-personally identifiable attributes"

PART 2

In 2002, Hassan Elahi was detained in Detroit when he was suspected of hoarding explosives in a Florida locker. His name was added, by mistake, to a US government watch list and he had to undergo strenuous questioning for six months. Elahi, although exonerated through

lie detector tests, decided to cooperate with the government, but in his own way. Elahi fought this assault for privacy by overloading the government with minute details about his personal life. Elahi started sending emails and posting pictures about his minute to minute life, he even wore a GPS tracker to notify the government of his every move. Elahi claims that by overloading the government with this information he is simultaneously saying everything and nothing about his life. Elahi prosthesis that the best way to obtain privacy is to give it away. His theory proved itself when the government stopped bothering him after his overflow of information. Elahi uses some rhetorical strategies for framing his evidence, he emphasizes a detailed story over presenting a lot of facts and statistics. He also controls the space given to supporting versus contrary evidence. Elahi selects and frames evidence linked to the system of values that support his outrage at his lack of privacy.

Mikkfo Hypponen, a cyber-security expert warns the world that more than the next killer virus they should be concerned about how companies have now started building their own backdoors and Trojans in software. In today's technological world, data storage has become cheap and thus most corporations prefer to keep data rather than delete it. Hypponen claims that the government and corporations have become more adept at using viruses as weapons. Hypponen protested against NSA claims that all data routed through US servers would be under digital surveillance. This effectively cripples encryption algorithms. Hypponen says that if there's no right to privacy, there can be no true freedom of expression and opinion, and therefore, there can be no effective democracy. The world is changing, but the change might not be for the better. Hypponen expertly chooses labels and names that guide the audience's response to this issue. By using things like emails, phone conversations and text messages Hypponn shows the relavenace of the issue privacy. His evidence also abides by the STAR system, making his arguments stronger. He also places contrary information, the part about someone asking him why this mattered so much, in a subordinate position. Hypponen employs a classical argument, aimed at a skeptical audience.

Beth Noveck founded the White House Open Government Initiative, which developed administration policy on transparency, participation and collaboration. Open platforms and the explosion of apps sets a precedent for thinking about "opening up the API of government." Noveck prosthesis that the government's methods are too outdated and that the next great superpower will be one to combine the hierarchy of the institution that is one which retains public values while incorporating diversity and network flow. The open government revolution Noveck wishes for comes in two stages; the first is opening up information for better decisions and the second phase is sharing decision-making power. Noveck presents a number of choice examples that promote her opinion, she gives facts and statistics. She starts off with a scenario and by the end of her talk the audience can see a solution emerging. All the examples Noveck used were situation much like our present one which were eventually solved thereby hinting that our problem can be solved if her opinions were taken into account. She fosters connections with the audience by openly addressing underlying values, lack of appropriate transparency in information sharing, that the audience shares.

John Wilbanks believes that the concept of privacy takes away from our major objectives. Wilbanks claims that privacy laws actually inhibit progress toward finding solutions to healthcare problems. Performing a medical or genomic experiment on a human requires

informed consent and careful boundaries around privacy. Wilbanks says that if these policies did not exist, a solution would present itself faster. Wilbanks hopes to think through the ethical and procedural steps and to create an open, massive, mine-able database of data about health and genomics from many sources. Wilbanks supports the idea of pooling medical research and records, including personal information about genomes and disease risk, and making that pool of information available to health researchers. Wilbanks draws on his audience's rational thought, he claims that lives can be saved if they had more information. For example he states that cancer medicine does not work on a good percentage of patients, if these patients personal history were available the doctors could skip those medicines and work on different cures. Wilbanks provides contextual and interpretive comments when presenting data. This helps the audience see the argument from Wilbanks' perspective.

Alessandro Acquisti studies the behavioral economics of privacy (and information security) in social networks. Professor Acquisti claims that with the advent of social media, the boundaries between public and private information, have been blurred considerably in the past decade. Privacy economics analyses what people share online and what they get in return. His team's surprising studies on facial recognition software showed that it can connect an anonymous human face to an online name – and then to a Facebook account -- in about 3 seconds. Other work shows how easy it can be to find a US citizen's Social Security number using basic pattern matching on public data. Acquisti claims all is not lost yet though, technology could work the other way in which the people could reap the benefits of big data while protecting their privacy. Acquisti uses his own research to convince his audience of the seriousness of the situation. Acquisti forces his audience to rhetorically think about this problem of privacy, by implying that facial recognition when combined with other repositories could expose people. Acquisti uses argument as an inquiry, by forcing the audience to think so the boundaries between public and private information.

Data mining is the process of searching through many records in one or more databases and looking for patterns or relationships among them. I think that by merging social network profiles and the National Driver Register (NDR) database would be useful. Often in police investigations, criminals are often identified by the NDR or DMV database. With the growing crime rates, more often than not people have a social media page and not a driver's license By combing these two databases, I believe the rate at which criminals could be identified and found would be faster. Looking at it from a corporate perspective, social media sites like Facebook and Twitter would be glad for the extra advertising, also if the government were to support the initiate of social media sites, these sites would grow at a phenomenal rate. Social media sites get more freedom and better sponsorship. From a government perspective, having more criminals caught or just being able to have a larger population base to select from is important. The government could also use these social media sites to make big announcements, or broadcast news information. Social media sites could start a news banner that would have regular postings. If bank databases are added on to this system, the government would have a greater access to people. That is, with information about bank numbers and statement information, the police would find it easier to freeze accounts or track a suspected offender. The city would be a lot safer and criminals may be caught in a timely manner. This would benefit both the citizens as well as the government and in this case social media sites too.