Data Privacy & Security

February 21, 2022

Privacy on Facebook

- Video from YouTube –*Geeks on Tour -- Session 207*
- https://www.youtube.com/watch?v=aKUbB_jpiPg&t=915s
  - Video on how to stop privacy invasion that exposes your friends on Facebook

Discussion of Privacy Objectives

- Privacy is not sharing information with others who are not supposed to receive it.
  - Information privacy about a person
  - Bodily privacy – 3D face features, retinal scan, finger print etc.
  - Location privacy – where you live and work should be private so that it is an invasion of your privacy to have a drone fly over your house and take pictures, you have less location privacy in public places
- Security – is how information is kept secure from other people. (e.g. username and password, secure storage of information,)

Privacy Rights

- EU has had more privacy regulation that the US for at least the last 25-30 years
- Currently EU operates under GDPR (General Data Privacy Regulation).
  - EU regulates how companies must protect information
  - newest revision adds an enforcement attribute to the legislation with fines to companies that violate the regulation. Fines can be fined 4% of global worldwide revenue. This forces companies to pay attention to data privacy
- Congress is getting ready to develop legislation in the US to ensure data privacy. Technology has moved so fast that our current laws do not protect our privacy. Some states such as California and Washington state have enacted their own privacy legislation but we really need national policy on this topic.
  - Individually you cannot do much about the data collected on you other than refuse to use technology
  - Requires a legislative solution

GDPR Guiding Principles

- **Lawfulness, fairness and transparency** – collection of data needs to be lawful, would normal person expect the uses of the information (was it fair or was it an unexpected use of your private information), were you made aware of how data was to be collected and used (transparency)
- **Purpose limitation** – was the information collected limited to the purpose of gathering the information. Example, if you join a club it is reasonable that the club needs your name and address and email in order to bill you, send you notices etc. But they cannot sell your information to someone who might sell items that club members are interested in unless they explicitly tell you they are doing this.
- **Data minimization** - given the purpose what is the bare minimum of information that I need to know to in order for the purpose.
- **Accuracy** – obligation of the organization is to correct the information in your account if you notify them of errors in your records

GDPR Guiding Principles (cont.)

- **Storage Limitation** – organizations can't keep information for as long as they want; they can only store for as long as it is needed for their stated purpose
- **Security** – organizations must keep information secure so that others who should not have your information cannot access it.

Who must follow GDPR

- Companies/organizations that do business in EU countries.
- Each country has their own regulatory body but they all follow the principles laid out in the GDPR
- US organizations that deal with residents in EU countries must follow GDPR principles.

What are tech companies doing to protect users?

- Apple now allows you to block your information from being used by third parties. https://www.washingtonpost.com/technology/2021/11/26/ios-privacy-settings/
- This means that Facebook and Google can no longer gather your information and share it with third parties that want to sell you something.
  - This definitely had an impact on Facebook earnings this last quarter as they suffered a large revenue loss because of this policy
- Google has announced that they will begin limiting the information they share https://www.nytimes.com/2022/02/16/technology/google-android-privacy.html
- They are not indicating that they will permit users to stop all sharing but will allow some restrictions on some types of data. (They can't stop all sharing as their business model is based on selling your information to third parties)
- Here is how to block ad tracking on Android phones: https://www.news18.com/news/tech/how-to-block-ad-tracking-on-your-ios-and-android-phone-through-these-easy-steps-4011938.html

What is the solution for an individual?

- There is no perfect solution. Each person needs to weigh their own risk tolerance for information sharing.
- Some people will not use technology as they are aware of the fact that they are sharing lots of personal information by using devices such as smart phones. Others don't care and are happy to share personal information with anyone who asks.
- With high security comes inconvenience. Each person has to weigh the risk for themselves. It's your choice but generally you must give up convenience to gain security.
- Generally people who have experienced identity theft are much more conscious of the risks than the average user.

Think before you share!

- Information you post on social media is shared with lots of people you don't know unless you set very tight limits on who can see and access your data.
- People accept terms and conditions in order to use an app – you should read your Terms of Service rights before you agree to these. It is better to forgo using an app rather than give away rights to your information that you are not comfortable with whom and how it is shared.

Levels of Protection

- Device Failure
- Theft
- Someone gets access to my files
- Protect my most sensitive information
  - Financial, banking, tax
- Protect my identity

Security Software

- Free Anti-Malware Programs
  - Windows Defender, Kaspersky, AVG, Bitdefender
- Anti-Malware Suites
  - They offer not only malware protection but also a firewall, an antispam filter, and other extras.
  - Cost from $35 to $80 annually
- Consumer Reports rates them

Cloud Storage

- Best solution for device failure, theft, protect access to files
- Google Drive, IDrive, iCloud and OneDrive all have the same level of encryption and security
- OneDrive Personal Vault
  - Access code is sent to smartphone
  - Closes and locks after 30 minutes unless you authorize to continue