Lab – Who Owns Your Data?

Explore the ownership of your data when that data is not stored in a local system.

Part 1: Explore the Terms of Service Policy

Part 2: Do You Know What You Signed Up For?

- Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

- Required Resources
- PC or mobile device with Internet access
- Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and Conditions, is a legally binding contract that governs the rules of the relationship between you, your provider, and others who use the service.

Navigate to the website of an online service that you use and search for the Terms of Service agreement. Below is a list of many popular social media and online storage services.

Social Media

Facebook: https://www.facebook.com/policiesLinks to an external site.
Instagram: http://instagram.com/legal/terms/Links to an external site.
Twitter: https://twitter.com/tosLinks to an external site.
Pinterest: https://about.pinterest.com/en/terms-serviceLinks to an external site.

Online Storage

iCloud: https://www.apple.com/legal/internet-services/icloud/en/terms.htmlLinks to an external site.
Dropbox: https://www.dropbox.com/terms2014Links to an external site.
OneDrive: http://windows.microsoft.com/en-us/windows/microsoft-services-agreementLinks to an external site.

Review the terms and answer the following questions.

1. Do you have an account with an online service provider? If so, have you read the Terms of Service agreement? Yes

2. What is the data use policy? "We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services."

   A more sophisticated policy is available here.

3. What are the privacy settings? Allows users to personalize what information they can display and what information is kept private. Allows users to control who can see what information you share on the platform, allows you to know what data they collect and what they do with it and also allows you to download your own information.

4. What is the security policy?

Organization of Information Security. Facebook has personnel responsible for oversight of security of the Applicable Products.

Physical and Environmental Security. Facebook's security measures will include controls designed to provide reasonable assurance that physical access to Facebook data centers is limited to authorized persons and that environmental controls are established to detect, prevent, and control destruction due to environmental hazards. The controls will include:

1. Logging and auditing of physical access to the data center by employees and contractors;
2. Camera surveillance systems at the data center;
3. Systems that monitor and control the temperature and humidity for the computer equipment at the data center;
4. Power supply and backup generators at the data center;
5. Procedures for secure deletion and disposal of data, subject to the Applicable Product Terms; and
6. Protocols requiring ID cards for entry to all Facebook facilities for all personnel working on the Applicable Products.

Personnel

a. Training. Facebook will ensure that all personnel with access to Covered Data undergo security training.
b. Screening and Background Checks. Facebook will have a process for:
    i. verifying the identity of the personnel with access to Covered Data; and
    ii. performing background checks, where legally permissible, on personnel working on or supporting aspects pertaining to the Applicable Products in accordance with Facebook standards.
c. Personnel Security Breach. Facebook will take disciplinary action in the event of unauthorized access to Covered Data by Facebook personnel, including, where legally permissible, punishments up to and including termination.

Security Testing. Facebook will perform regular security and vulnerability testing to assess whether key controls are implemented properly and are effective.

Access Control.

a. Password Management. Facebook has established and will maintain procedures for password management for its personnel, designed to ensure passwords are personal to each individual, and inaccessible to unauthorized persons, including at minimum:
    i. password provisioning, including procedures designed to verify the identity of the user prior to a new, replacement, or temporary password;
    ii. cryptographically protecting passwords when stored in computer systems or in transit over the network;
    iii. altering default passwords from vendors;
    iv. strong passwords relative to their intended use; and
    v. education on good password practices.

b. Access Management. Facebook will also control and monitor its personnel's access to its systems using the following:
    i. established procedures for changing and revoking access rights and user IDs, without undue delay;
    ii. established procedures for reporting and revoking compromised access credentials (passwords, tokens etc.);
    iii. maintaining appropriate security logs including where applicable with userid and timestamp;
    iv. synchronizing clocks with NTP; and
    v. Logging the following minimum user access management events:
        1. Authorization changes;
        2. Failed and successful authentication and access attempts; and
        3. Read and write operations.

Communications Security

a. Network Security
    i. Facebook will employ technology that is consistent with industry standards for network segregation.
    ii. Remote network access to Facebook systems will require encrypted communication via secured protocols and use of multi-factor authentication.
b. Protection of Data in Transit
    i. Facebook will enforce use of appropriate protocols designed to protect the confidentiality of data in transit over public networks.

Vulnerability Management. Facebook has instituted and will maintain a vulnerability management program covering the Applicable Products that includes definitions of roles and responsibilities for vulnerability monitoring, vulnerability risk assessment, and patch deployment.

Security Incident Management

Security Incident Response. Facebook will maintain a security incident response plan for monitoring, detecting, and handling possible security incidents affecting Covered Data. The security incident response plan at least includes definitions of roles and responsibility, communication, and post-mortem reviews, including root cause analysis and remediation plans.

Monitoring. Facebook will monitor for any security breaches and malicious activity affecting Covered Data.

In the event of any express conflict between the Applicable Product Terms and these Data Security Terms, the Applicable Product Terms will govern solely with respect to your use of the Applicable Products and solely to the extent of the conflict. Facebook may update these Data Security Terms from time to time to reflect evolving security standards.

5. What are your rights regarding your data? Can you request a copy of your data? As a user of the platform, I am able to manage what data I can share with others and how much of it I can share. I can also download a copy of my data ranging from messages, posts shared, saved items, payments, stories, reels, and etc.

6. What can the provider do with the data you upload? "We use information we collect to provide a personalized experience to you, including ads, along with the other purposes we explain in detail below.

   For some of these purposes, we use information across our products and across your devices. The information we use for these purposes is automatically processed by our systems. But in some cases, we also use manual review to access and review your information.

   To use less information that's connected to individual users, in some cases we de-identify or aggregate information. We might also anonymize it so that it no longer identifies you."

7. What happens to your data when you close your account? Do You Know What You Signed Up For? After 30 days, your account and all your information will be permanently deleted, and you won't be able to retrieve your information. It may take up to 90 days from the beginning of the deletion process to delete all the things you've posted. Yes I know what I signed up for.

After you have created an account and agreed to the Terms of Service, do you really know what you have signed up for?

In Part 2, you will explore how the Terms of Service can be interpreted and used by providers.

Use the Internet to search for information regarding how the Terms of Service are interpreted.

Below are a few samples articles to get you started.

Facebook:

http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.htmlLinks to an external site.

iCloud:

http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.htmlLinks to an external site.

Dropbox:

http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/Links to an external site.

Review the articles and answer the following questions.

1. What can you do to protect yourself? I can alter my privacy settings which Facebook allows me to personalize such by changing who can view my profile and how much of it they can view. Another thing is to always read Terms of Use and Privacy Policy of products or services that use your information so you are aware how you are able to use the product and how the service uses your information.

2. What can you do to safeguard your account and protect your data? Two Factor Authentication so you can prevent any external threats on a personal level. Secure personal identification numbers and financial information – don't share it online. Only accept connections from people you know. Force unrecognized devices and sessions to logout. Only access social media through a secure network and avoid free public Wi-Fi at all cost.