Lewis Joseph Feik
Security Awarness
Week 5 Lab

Lab – Who Owns Your Data?

Objectives

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

Lewis Joseph Feik
Security Awarness
Week 5 Lab

Part 1:

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/policies

Instagram:
http://instagram.com/legal/terms/

Twitter:
https://twitter.com/tos

Pinterest:
https://about.pinterest.com/en/terms-service

Online Storage

iCloud:
https://www.apple.com/legal/internet-services/icloud/en/terms.html

Dropbox:
https://www.dropbox.com/terms2014

OneDrive:
http://windows.microsoft.com/en-us/windows/microsoft-services-agreement

Lewis Joseph Feik
Security Awarness
Week 5 Lab

Review the terms and answer the following questions.

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

Yes I currently have a service with an online providor and yes i have read terms and services agreement.

b.
What is the data use policy?

Explains how the provider collects, stores, and processes your personal information (e.g., email, IP address, usage logs).
Usually states that data is used to provide services, maintain security, improve features, and comply with legal obligations.
Often includes sharing rules (with partners, vendors, law enforcement when required).

c.
What are the privacy settings?

User-facing controls that let you choose how much of your data is visible or shared.
Examples: profile visibility (public/private), sharing of activity, data collection preferences, ad personalization, or cookie consent.
Sometimes you can limit what others can see about you, or opt out of analytics.

d.
What is the security policy?

Describes the technical and organizational measures taken to protect your data.
Typically includes: encryption (at rest and in transit), access controls, monitoring, incident response, and employee training.

Some providers certify compliance with standards (ISO 27001, SOC 2, GDPR, HIPAA depending on context).

e.
What are your rights regarding your data? Can you request a copy of your data?

Under most modern data protection laws (like ***GDPR*** *in Europe or* ***CCPA*** *in California): You have the right to access your personal data.*
You can request a copy in a portable format.
You can request corrections or deletion ("right to be forgotten"), within legal/contractual limits.
You can withdraw consent for certain types of processing.

Lewis Joseph Feik
Security Awarness
Week 5 Lab

f.

What can the provider do with the data you upload?

They may process it for providing the service (e.g., storage, running applications).

Some providers analyze data for troubleshooting or performance improvements.

Terms usually prohibit the provider from selling your private data but may allow aggregated/anonymous usage for analytics.

They cannot legally repurpose your personal data beyond what you consented to (if they comply with GDPR/CCPA).

g.

What happens to your data when you close your account?

Typically, your data is scheduled for deletion after a grace period (30–90 days is common).

Some information may be retained for legal, regulatory, or security reasons (e.g., financial records, abuse-prevention logs).

Backups may persist temporarily until overwritten.

If allowed, you should download/export your data before closing the account.

Part 2:

Do You Know What You 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-

iCloud:http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-

Lewis Joseph Feik
Security Awarness
Week 5 Lab

Dropbox:

http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/

Review the articles and answer the following questions.

a.

What can you do to protect yourself?Read the Terms of Service / Privacy Policy carefully

-*Look especially for sections about what rights you're granting the service (to host, scan, share, delete content).*
-Watch for changes: many services reserve the right to change terms anytime; you want to know how you'll be notified and what options you have if you disagree.

1. ***Limit what you upload or share***
   -*Don't store or upload sensitive information unless absolutely necessary.*
   -Use encryption for files before uploading (so even the service can't see contents).
   -Be cautious about sharing links, permissions, or anything publicly visible.

2. ***Use privacy settings and consent controls***
   -*Turn off or limit data sharing / data collection features wherever possible (e.g. disable ad personalization, disable or limit tracking).*
   -Use strong account settings: two-factor authentication, strong passwords.

3. ***Keep backups in your control***
   -*Maintain local copies of important data so you're not entirely dependent on the cloud service.*
   -If you close your account or a service changes policy, you still have your own archive.

4. ***Monitor notifications of changes***
   -*When a service changes its terms, they often send you an email or post notice. -Read those notices. If you disagree, you may need to move awayor negotiate opt-outs.*
   -For example, with Dropbox, when they introduced a binding arbitration clause or changed government request policies, users were given a chance to opt out (in some cases).

5. ***Opt out of unfavorable provisions if possible***
   -*Some terms allow you to opt-out of certain clauses (e.g., arbitration, class action bans). If that bothers you, opt-out according to the instructions.*
   -Sometimes you can refuse or disable certain features (e.g. sample submission, data sharing) in privacy settings.

6. ***Use additional protection tools***
   -*Encrypt data yourself before uploading (end-to-end encryption).*
   -Use VPNs for secure connections.
   -Use file versioning and tools that can restore from past versions.

7. ***Know your legal rights***
   -*Depending on where you live, laws like GDPR (EU), CCPA (California), etc., give you rights like accessing your data, deleting it, correcting it, or preventing certain use.*

8. ***Close or deactivate carefully***
   -*Before closing an account, download/export your data.*
   -Check what happens to data after account closure (if some data is retained for -legal or security reasons).
   -Remove your content where possible.

b.
What can you do to safeguard your account and protect your data?

1.Secure Your Login

- *Use a* ***strong, unique password*** *(12+ characters, mix of letters, numbers, symbols).*
- *Never reuse passwords across accounts.*
- *Store passwords in a* ***password manager****.*
- *Enable* ***two-factor authentication (2FA)*** *— preferably with an authenticator app or hardware key (not just SMS).*

2. Control Access

- *Review and remove* ***unused devices*** *logged into your account.*
- *Revoke access for* ***third-party apps*** *or services you no longer use.*

- *Set up **login alerts** to notify you of suspicious activity.*

3. Manage Privacy Settings

- *Adjust **privacy controls** to limit who can see your data (friends only vs. public).*
- *Turn off or restrict **location sharing**.*
- *Limit data collection for ads and marketing (opt out where possible).*

4. Protect Your Data

- ***Back up important files** locally (external drive) in case cloud storage fails.*
- *Encrypt sensitive files **before uploading** to cloud services.*
- *Be careful what you post — once it's online, it can be copied or shared even if you delete it later.*

5. Stay Updated

- *Keep your **OS, apps, and antivirus software updated** to patch vulnerabilities.*
- *Install security updates promptly (especially on phones and laptops).*

6. Watch Out for Scams

- *Be alert to **phishing emails** or fake login pages.*
- *Double-check links before clicking; don't download attachments from unknown senders.*
- *Use official apps or websites only.*

7. Exercise Your Rights

- *Many platforms let you **download a copy of your data**.*

- *Request deletion of data if you stop using a service.*
- *Know your rights under laws like **GDPR** or **CCPA** (access, correct, delete, restrict processing)*