Motivation

As has become all too clear over the past year-and-a-half, what you share or view on social media platforms is probably being shared with more people that you think you’ve authorized, and it is being used to affect what sorts of ads and other publicity get fed to you.

This month’s tech program will look at

- How to change various settings to gain some measure of control over what you see and what you share,
- Safe habits to cultivate online, and
- Critical examination of memes and articles that might otherwise get you to hit Reblog before you’ve thought about it.
Introduction

There are 2 sorts of privacy that you should be concerned with on social media: who can see what you post and whose content will show up in your feed. That is (to be a bit overly simplistic), who can read what you write and who can “force” you to read what they write.

Different users of social media will have different views on how restrictive they want to be with respect to these 2 groups, and they will have different views on the weight they give to the 2 kinds of privacy. The 4 “corners” of the privacy universe would be the person who wants to see everybody’s content and to share theirs with the world, the person who only wants to see and be seen by their friends, the person who is open to seeing anything but only wants to share with their friends, and the person who wants to share with everyone but not to read what they have to say.

Facebook’s various settings allow you to tweak both kinds of privacy so that it more-or-less matches your preferences. Be warned, though, that you can’t reduce the amount of “sponsored content” (ads) that Facebook inflicts, you can only influence what sorts of ads get inflicted on you. Also, Facebook is continuously changing its policies and settings, so if privacy is a concern, you will need to do occasional checkups and to learn new sets of settings.

Facebook settings

Here you see an example of a Facebook Home page. To get to the settings that I need to review and possibly change, I’ve clicked on the downward pointing arrowhead to get the utility dropdown menu. Then I click on Settings to get to the page that coordinates all settings.
That took me to the General Settings page. I’m not concerned with the general settings, so I’ll click on Security and Login in the left-hand sidebar to get to those settings.

The settings here are more related to keeping an account from being hacked than to privacy as such, but everyone using Facebook should know about them. In the top part of the page, you see a section called Where You’re Logged in. If any of the devices listed here are unfamiliar, you should click on the vertical ellipsis (…) on the right-hand side to look into it. If it’s unfamiliar or on a device that you no
longer use for Facebook (or, especially, a device you have given/sold/otherwise transferred to someone else), you should deauthorize it.

When in doubt, deauthorize. If it turns out you were wrong and you still use that device for Facebook, the worst that this will do is make it so you have to log in again on that device.

Scrolling down this page a bit, you’ll see a section headed Two-Factor Authorization. Two-factor authorization is very commonly used by all kinds of Websites, and it is a good way to add a layer of security to your accounts. The way it works is that when you log into a Website that you’ve set it up on, the site simultaneously sends a code to you (generically as a text to your phone, but other options are also available) and takes you to a page where you must enter that code before you can finish logging in.

That process raises some natural questions:

1. Will I have to go through this every time I want to log in?

Not necessarily. In the course of logging in, you can choose to authorize the device you’re logging in on for logging in without a two-factor code. The Authorized Logins item in this section will show all the devices/apps you’ve chosen to allow.

2. Doesn’t authorizing a device/app defeat the purpose of two-factor authorization?

Kind of. If the device doesn’t leave the house much (for example a desktop or a laptop that usually stays home), then the risk is minimal. Particularly since you can deauthorize the device as we saw earlier.

On the other hand, you probably want to always require it on your smartphone or other any other device that you take with you a lot.
Going back to the left-hand sidebar, I click on Your Facebook Information to look at various overviews of my information.

Click on View on the right-hand side of Access Your Information to get to the various categories.
There are several options here. You can look back at your previous posts, comments, likes, and so on. For the present purposes, though, **Friends, Following and Followers**, and **Groups** will be of most interest. Together, these are the entities that might be able to read your content or put content on your feed even if you have made it so that not everyone can, so it’s useful from time to time to make sure that the people in these categories should be in them.

Using Groups as an example, I have clicked on the downward pointing arrowhead. It now points upward, and the choices for examining groups I’m a member of has appeared.
The relevant choices here are of editing how much I want to see from a group ("Edit notification settings") or to dropping out of the group.

**Privacy As Such**

Now I go back to the left-hand sidebar to go to the **Privacy** settings.
What I’ve done up to this point is to secure my account and to clean the lists of friends, groups, and followers/followed people up. The Privacy page is one of the places where I set the general guidelines of what categories of people (Friends, Friends of Friends, Everyone) can interact with me and how. The other place that is relevant to these general guidelines is the Timeline and Tagging page (shown below).
Blocking

Blocking types of ads

You may encounter ads you don’t care to see or a friend of a friend may frequently comment on your mutual friend’s posts with content or demeanor that makes Facebook not at all pleasurable. In such cases, you can block the offending person or type of ad (again note: you cannot reduce the number of ads you see, let alone eliminate them, but your preferences and blocks will influence the types of ads you see).

In the above image, I’ve boxed in the control I’d use to start the process of blocking this ad. Clicking on it yields the choices in the image below.

Notice that blocking (“Hide ad”) is not the only option. Perhaps I found that this is the sort of ad I’d like Facebook to be showing me. In that case, I could choose “This ad is useful”.

10
If I did want to block it, though, I’d be presented with the opportunity to let Facebook know why I blocked it. Some of the choices would result in queuing the ad for review by Facebook to see if it violated their advertising guidelines.

**Blocking people**

Although I’ve used the heading “Blocking people”, I’ll be talking here about both blocking (barring from interacting) and reducing what you see from given individuals.

Clicking on the horizontal ellipsis in the upper right-hand corner of a post drops a menu down with several options. “Save to watchlist” allows you to make a list of posts you want to go back to later, so kind of the opposite of what would be motivating any sort of blocking. In this case, the person posting is a friend, so I wouldn’t be blocking in an absolute sense (if I were, I would be unfriending back in the Information section). However, it might be that my friend’s content just doesn’t interest me, or it might
offend me more often than I can tolerate. In such cases, I could Unfollow (we’d still be Facebook friends capable of directly contacting one another, and my friend would still see my content unless they’d unfollowed me!!!) Alternatively, I might just hide the posts they share from this source (“Hide all from [original poster of the content, here Eons • PBS]”). Or in either case, I could “snooze” them for a month.

To block friends of friends, click on the horizontal ellipsis to the right of one of their comments. Then click “Hide comment.” The specific comment will be hidden, and you will have the option of taking further action as shown below.

If you return to the Settings page and then choose Blocking from the left-hand sidebar, you will see a list of those people who you have blocked.
Apps and Websites lets you edit the various Facebook apps you may have authorized (each of those Facebook games you play collects information on you) and Websites that have access to your data and content.
Still on the Settings page but further down in the sidebar is Ads. Again, you can’t get rid of ads, but this is where you can fine tune what sorts of ads you’d like Facebook to show you.

Here’s the list of advertisers whose ads I’ve hidden. There are other subcategories of advertisers I’ve interacted with, and this page is a one-stop location for reviewing them all.
Online Hygiene

The online world has made it much easier and quicker to share information than it used to be, and that has had many benefits, among them the ability to remain in close contact with friends and relatives who live far away geographically. However, that speed takes away one of the checks that we used to have on the trustworthiness of information: time. In the snail-mail days, if you wanted to share an article, you had to address an envelope, write a note to go with the article, find the stamps, and so on. All of that process gave you the time for any doubts you might have had about the article’s truthiness or biases to bubble up so that by the time you were about to stamp the envelope you might have decided to double check things before going any further. Even to share a rumor, you’d have to get on the phone and engage in conversation with someone who might raise questions that got both of you questioning the rumor.

Now, though, sharing an article or meme is as quick and easy as clicking a button (hence the expression “hitting the reblog button”). Little to no thought is required.

There is no silver bullet for separating truth from rumor, propaganda, and fiction, but here are some things to look for:

1. How trustworthy is your source?

   In this context, you may have to go backwards along the chain. So you know that your friend wouldn’t lead you astray, but what if they got misled? Where did they get the information from?

2. Related to the first point, is the source known to be satirical or a propaganda organ?

   Below are a few popular sites that produce satirical articles that have the look and feel of serious articles¹. Generally, such sites will have a disclaimer somewhere on their articles that they are a

---

satirical site, but this disclaimer is easy to overlook. A good rule of thumb is that if a story seems completely over the top, it’s wise to dig around for other sources to determine whether it’s true or just as it seems: over the top.

- The Borowitz Report
- ClickHole
- Cracked
- The Daily Currant
- The Daily Mash
- The Daily Squib
- The Daily WTF
- The DailyER
- The Onion
- Topeka News
- Weekly World News
- World News Daily Report

The “List of fake news websites” at Wikipedia² is a useful resource list of deliberately misleading sites. If you look at the list, you will notice that many of the sites have names that are almost the same as legitimate sites. That brings us to the next point:

3. Does the site’s URL (the “web address” in the box at the top of the browser control section) look close to a real site’s but with some differences?

As an example, the URL for ABC News is https://abcnews.go.com/. Companies will often buy URLs that are similar to their names and reroute them to their official site, so http://abcnews.com works to get you to the legitimate ABC News site.

Someone bought the deceptively similar URL of http://abcnews.com.co (note the extra .co) to direct traffic to their site which stole the look and feel of ABC News but pushed false stories. If you visit that site, you’ll see that it is now a Parked Domain³. Presumably when it became widely known that the site was fake, the operators had to change tactics. That sort of process is why it is less useful to memorize any list of fake sites than to be in the habit of looking for other signs of whether or not it’s legit.

4. Even if the source is legitimate, is it giving you the whole story?

more entries, but these are the ones I see the most.
² Source: https://en.wikipedia.org/wiki/List_of_fake_news_websites
³ A URL for a domain that someone holds but doesn’t use. The content at such URLs often consists of links to sites of dubious quality.
There are many more than 2 sides to most stories, so reporting should consider the input and points of view of various parties to a story. This does not mean that legitimate stories have to remain agnostic about what the truth of a situation is, but it does mean that they will give a fair hearing before taking their position.

A useful term to know here is **Confirmation bias**. Confirmation bias is our tendency to give more credence to stories that align with our own opinions and biases than to stories that are either independent of them or that tend to contradict them. Two results of confirmation bias are that we tend to do less work to check the truth of stories we agree with, and we resist longer before accepting stories we disagree with initially.

The trick here is what blogger Julia Galef calls **Steel-manning**. Steel-manning contrasts with the more commonly known phenomenon of **Straw-manning**. Straw-manning is the tendency to use a weak form of views you disagree with and to use that as your imagined debating opponent. Since the argument you develop on behalf of the opposition is weak, you can then easily defeat it in your story and, thus, seem to have shown the validity of your position.

In Steel-manning, on the other hand, you actively look for your opponent’s strongest arguments, the ideas being that

a. You will better represent other views than you would naturally tend to, and

b. If your analysis is still better than your opposition’s, then you certainly have a more solid argument.

On this point, then, the summary would be to be aware of your own confirmation bias when reading material that you feel “must be shared” and to look critically at articles that seem too neat and clean to see if they’re straw-manning viewpoints that might contradict their narrative.