CHAPTER

Privacy controls

4

WHAT ARE PRIVACY CONTROLS?

The "social" part of "social media" means that people are sharing with one another. Sometimes, it's with a very small and carefully controlled group. But more often, it's with large groups of people. Many social media services make users' posts available to anyone on the internet by default.

In some cases, someone may be perfectly fine with their online post being shared broadly. It might even be desirable: someone searching for a job may want their professional profile to be widely viewed. The same is true of public figures, celebrities, and others who make their living from gaining public attention in some way. Plenty of people also like the attention they get from sharing things publicly; it can be exciting if a stranger likes a video or photo you posted.

But not everyone wants to share that publicly or in all contexts. Someone who wants to share their professional profile for a job search may prefer to keep more personal information (like photos of their kids and their travel schedule) limited to a more select group.

Privacy controls allow users the power to limit who can see their posts. Depending on the site, the controls vary greatly. Throughout this book, chapters about specific social media sites will detail their privacy settings. In this chapter, we will overview the major categories of privacy control options.

PRIVACY CONTROLS

PUBLIC/PRIVATE

The simplest privacy control is the public/private setting. On sites that use this, posts are usually public by default and visible by anyone online. Users have one option to restrict visibility of their posts, and that is to make them private. This generally restricts them to be visible by only the user's friends or another approved list of people. For example, Figure 4.1 shows the Twitter privacy options. Next to "Tweet privacy" is the one option for protecting posts: "Protect my Tweets." If the user selects this, the user has to approve anyone who wants to follow their posts.

Many social media sites use some variant of this model. As one other example, Pinterest allows users to create boards (basically an organized collection of posts with a common theme) that are either public or restricted to a specific list of approved viewers.

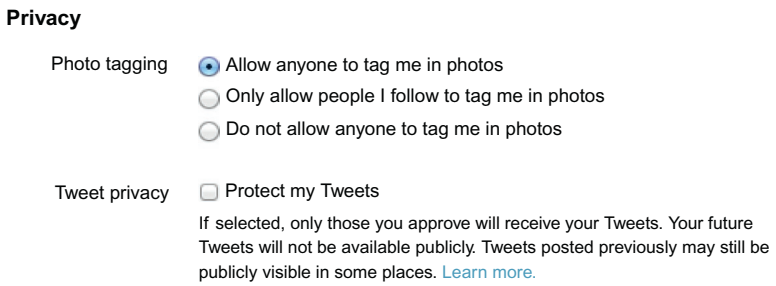

FIGURE 4.1

The privacy settings on Twitter. Note that the only option to keep tweets private is with the "Protect my Tweets" option next to "Tweet privacy."

ITEMIZED PRIVACY

On the more complex end of the spectrum, some sites give users fine-grained control over who can see every post. Facebook is one of these sites. Users can set the privacy level for each post. Facebook provides a default set of options, including Public (visible to anyone on the internet), Friends, Friends except Acquaintances (the latter being a list of casual friends that the user maintains), Only Me (which prevents anyone else from seeing the post), or Custom. Figure 4.2 shows these basic options.

The user can also create custom lists of friends and restrict the post to be visible to only people on a specific list. Examples of lists could be high school friends, fellow Chicago Cubs fans, coworkers, etc. The advantage of these lists is that they can be used to avoid bothering people with certain posts they might not be interested in. For example, you may want to share a link about your profession with your work friends, even though you know your high school friends would not have any interest in it.

Users can also create custom settings for each post. This lets the user pick a default group to share with (e.g., Friends) and then selectively remove others from

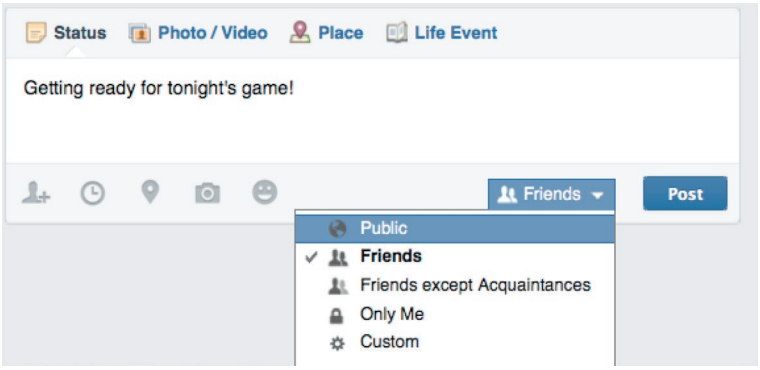

FIGURE 4.2

Facebook's privacy options for a given post.

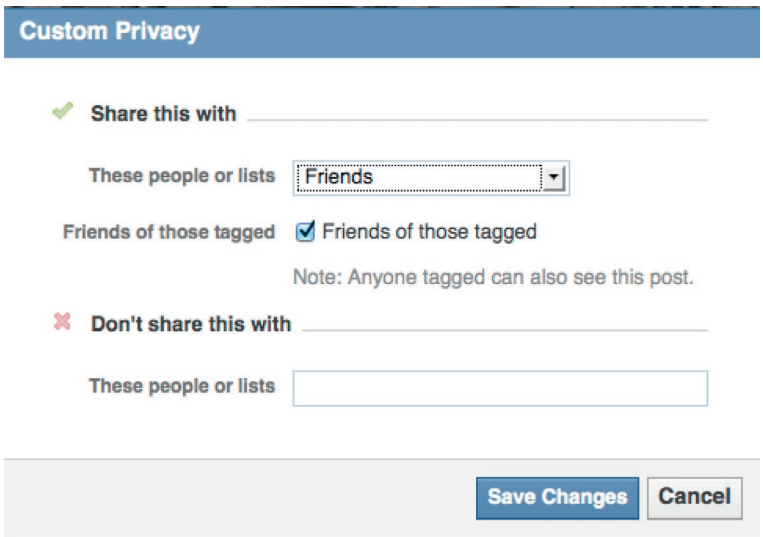

FIGURE 4.3

The Custom privacy setting options on Facebook.

access. For example, if someone rants about work, they may want to share it with all their friends except coworkers. In the options shown in Figure 4.3, they could add their list of coworkers to the "Don't share this with" list. Users can also create a custom list of people who can see a specific post in the "Share this with" section by selecting each person who gets permission to see the post.

Google+ has similar privacy features. They have made friend lists (like the co-workers, high school friends, and fellow Chicago Cubs fans lists mentioned above) even more central to the design of their site. They encourage users to create "circles," which are essentially lists of friends. When sharing a post, users have to explicitly choose which people or circles to share with. This is a bit different than most sites that tend to have a default setting that users can override if they choose (Figure 4.4).

DEFAULT PRIVACY

While these advanced settings are available to users, the fact is that they often are not used. Most users of social media sites have a default setting. They may change that for certain posts on Facebook, for example, but advanced customized privacy levels remain relatively rare.

CASE STUDY: RANDI ZUCKERBERG

Even using the relatively simple privacy settings can be confusing. This was illustrated, perhaps most ironically, in 2012.[1] Randi Zuckerberg, the older sister of Facebook founder and CEO Mark, took a photo of her family all using the then-new Facebook app called "Poke" at the same time. Mark stood in the corner with a slightly

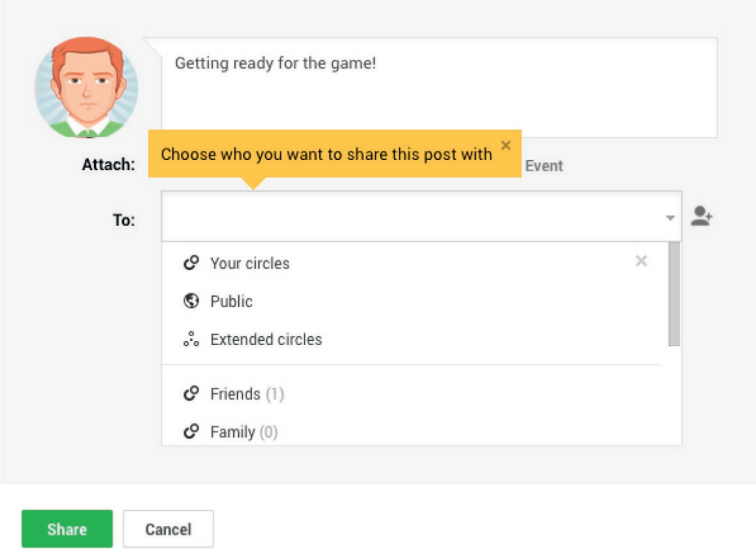

FIGURE 4.4

The Google+ posting interface. If a user tries to post without typing in a setting, they are reminded to choose whom the post will be shared with.

confused look on his face. Randi shared the photo on her Facebook page, with the privacy set to Friends Only.

A short time later, Callie Schweitzer (of Vox Media) tweeted the photo. Randi Zuckerberg sent her a public and angry message saying, "Not sure where you got this photo. I posted it to friends only on FB. You reposting it to Twitter is way uncool."

Schweitzer took the post with the photo down, but not before many other media outlets grabbed a copy. However, Callie got a copy of the photo in a completely legitimate way that Randi Zuckerberg did not expect. Randi had tagged her family members in the photo. Callie was a friend with another of the Zuckerberg sisters. Although Randi had set the privacy level so only friends could see the photo, Facebook's system still allows friends of anyone tagged to see the photo as well, essentially making the picture more public than the original poster intended.

That the complexities of Facebook's privacy controls caused a Facebook insider's post to be widely shared illustrates the difficulties faced by everyone trying to control access to their content. This story also illustrates something that privacy settings within a system can't control: people downloading a user's posts and sharing them somewhere else. Randi Zuckerberg posted her family photo on Facebook, but it was shared widely on Twitter after Callie Schweitzer downloaded a copy and reposted it.

Indeed, it is now commonplace to see media stories with photos pulled from Facebook, Twitter, Instagram, and other sources. If one person has access to the content within a site, that person can save a copy and share it elsewhere. No privacy setting can prevent this, which goes to support the adage that once something is posted online, control over who sees it and how it is used is lost.

PRIVACY AWARENESS

While nearly all social media sites have some privacy options and, as we have seen above, some have very powerful privacy settings, the average user's understanding of privacy controls can be limited. Statistics vary widely about how many users have interacted with privacy controls and how often, but a few demonstrative projects have illustrated—to users and others—how people are often unaware of how much information they are sharing.

CASE STUDY: PLEASE ROB ME

One of the first examples of this was Please Rob Me. As background, the location-sharing social media service Foursquare allows users to "check in" at places, recording their presence there. Foursquare has strong privacy protections, never sharing these check-ins publicly; they are always restricted to a group of approved friends due to the sensitivity of the information. However, Foursquare allows its users to share their check-ins on Twitter. Since Twitter defaults to be publicly visible to everyone on the internet, and the vast majority of users maintain public accounts, the result was people's locations being widely shared. Not only did this allow a user's movements to be tracked, but also it revealed when they left home. A simple white pages lookup (using their Twitter name, which is often a real name, and the name of their current city) would yield an address.

To highlight the insecurity of this oversharing, the Please Rob Me site was launched. It looked for Foursquare posts on the public Twitter feed. The list could be filtered by location (Figure 4.5).

There were a lot of negative reactions to Please Rob Me from people who felt unfairly targeted when their names appeared on it. However, the goal of the site was always to bring awareness to people who were oversharing. The site was not responsible for the privacy problem; the users were making poor choices.

CASE STUDY: TAKE THIS LOLLIPOP

A year later, Take This Lollipop was responsible for raising anxiety levels in millions of people. The interactive, personalized horror film was part art project and part privacy lesson. Facebook users could go to http://takethislollipop.com and log on with their Facebook account. The site then plays a short film where a mentally disturbed stalker becomes increasingly agitated while viewing the user's Facebook page. The movie integrates actual information from the user's account, including photos, friend lists, comments, and messages. Figure 4.6 shows a frame from that movie with the stalker's face reflected on the monitor that is displaying the user's page.

When the site launched, people reacted by believing their accounts had been hacked and suggesting the site had stolen their information. In fact, the users' had set up their accounts with privacy settings that allowed apps to access all this data freely. Even stringent privacy settings often could not prevent an app from accessing some of this information and illustrating how vulnerable their data was.

FIGURE 4.5

The Please Rob Me website, showing people who have just left home, based on their Foursquare check-ins shared through Twitter, with locations.

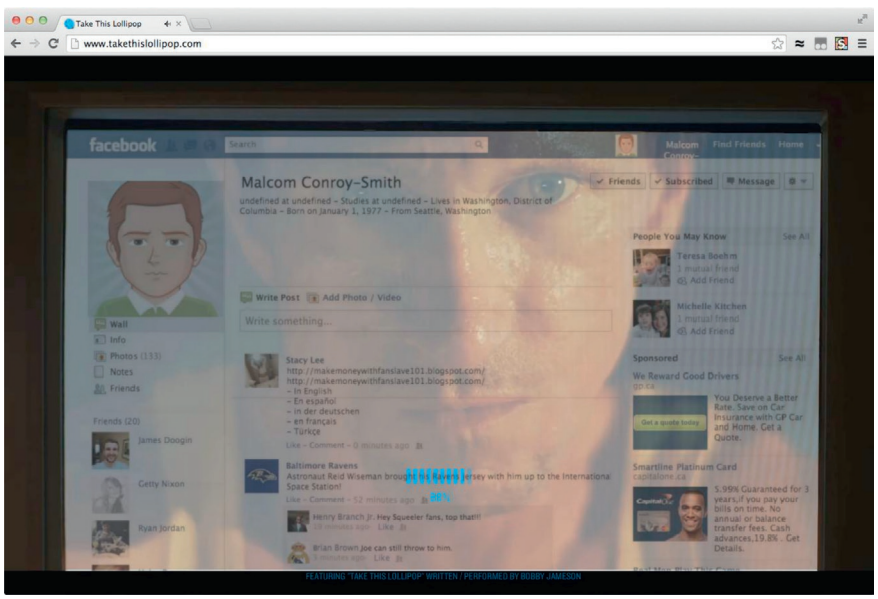

FIGURE 4.6

A frame from the Take This Lollipop movie, showing a stalker browsing the user's Facebook page.

PRIVACY AWARENESS IMPACTS

Research has also shown that these kinds of privacy warning sites can effectively increase people's awareness about privacy. In a scientific study, people took a test where they were asked to check off which pieces of data they believed Facebook apps could access. They were also asked about their level of concern regarding their data. Then, they watched the Take This Lollipop video. When they retook the test, they were significantly more aware of what data was shared and they showed higher levels of concern about their privacy.

There is a long way to go before average users can really understand the complexities of how their social media data is shared, but these two sites illustrate how unaware people often are about this sharing and their reactions when they find out that people can see a lot of what they post.

INVESTIGATING PRIVATE ACCOUNTS

If someone has made their account private, how can you investigate them? Each of the chapters that follow about specific social networks will have suggestions. However, there are a few general techniques. The most basic of these is to try to get approved access to the target's account. It could be that someone you know already has a social connection with the target. This might allow you to access the target's posts by logging on through your associate's account.

On some networks, friends of the target's friends can see some information. Thus, even if you cannot befriend the target, becoming connected to one of the target's associates on the social media site might increase the access you have.

If you want to keep your identity private, one option is to create a fresh account and use that to request a social connection. However, this option should be exercised with caution. It is a violation of the terms of service of *some* social media sites to create accounts with false personal information.

Even if creating a dummy account is not a violation, it may be transparent to the target. Accounts with very little history or few social connections may appear suspicious to the target. Ultimately, this depends on the target's personal preferences. Some people create as many social connections as possible on social media, while others are much more careful about curating their friend lists.

CONCLUSIONS

Privacy controls allow social media users to control who can see their content. These can be simple settings that toggle an account between public and restricted to an approved group, or they can be sophisticated that give users control over every person who can see each individual post.

While privacy controls are important for users, especially when they are sharing sensitive personal information, people often do not fully understand how public their data is nor how to use all the controls at their disposal.

Future chapters will discuss specific tactics for accessing information that is protected on the target's social media profiles. However, the most common and successful strategies generally involve creating closer social connections with the target.

NOTE

1 Hill, Kashmir. 2012. "Oops. Mark Zuckerberg's Sister Has A Private Facebook Photo Go Public." Forbes. December 26. http://www.forbes.com/sites/kashmirhill/2012/12/26/oops-mark-zuckerbergs-sister-has-a-private-facebook-photo-go-public/.