Or perhaps you need to hide your identity for downloading illegal or copyrighted content through BitTorrent. Proxies are not bulletproof, however. When you use a proxy, remember that each browser must be manually configured to point to the proxy service. And even the best proxy sites admit that clever Flash or JavaScript tricks can still detect your underlying IP address—the IP address you use to connect to the proxy in the first place. You can limit the effectiveness of these tricks by blocking or restricting the use of Flash and JavaScript in your browser. But the best way to prevent JavaScript injection from monitoring you via your browser is to use the HTTPS Everywhere plug-in (see here). There are many commercial proxy services. But be sure to read the privacy policy of any service you sign up for. Pay attention to the way it handles encryption of data in motion and whether it complies with law enforcement and government requests for information. There are also some free proxies, but you must contend with a stream of useless advertising in exchange for the use of the service. My advice is to beware of free proxies. In his presentation at DEF CON 20, my friend and security expert Chema Alonso set up a proxy as an experiment: he wanted to attract bad guys to the proxy, so he advertised the IP address on xroxy.com. After a few days more than five thousand people were using his free “anonymous” proxy. Unfortunately most of them were using it to conduct scams. The flip side, though, is that Alonso could easily use the free proxy to push malware into the bad guy’s browser and monitor his or her activities. He did so using what’s called a BeEF hook, a browser exploitation framework. He also used an end user license agreement (EULA) that people had to accept to allow him to do it. That’s how he was able to read the e-mails being sent through the proxy and determine that it was handling traffic related to criminal activity. The moral here is that when something’s free, you get what you pay for. If you use a proxy with https protocol, a law enforcement or government agency would only see the proxy’s IP address, not the activities on the websites you visit—that information would be encrypted. As I mentioned, normal http Internet traffic is not encrypted; therefore you must also use HTTPS Everywhere (yes, this is my answer to most browser invisibility woes). For the sake of convenience, people often synchronize their browser settings among different devices. For example, when you sign in to the Chrome browser or a Chromebook, your bookmarks, tabs, history, and other browser preferences are all synced via your Google account. These settings load automatically every time you use Chrome, whether on traditional PCs or mobile devices. To choose what information should be synced to your account, go to the settings page on your Chrome browser. The Google Dashboard gives you full control should you ever want to remove synced information from your account. Ensure that sensitive information is not auto-synced. Mozilla’s Firefox also has a sync option. The downside is that all an attacker needs to do is lure you into signing in to your Google account on a Chrome or Firefox browser, then all your search history will load on their device. Imagine your friend using your computer and choosing to log in to the browser. Your friend’s history, bookmarks, etc., will now be synced. That means that your friend’s surfing history, among other information, is now viewable on your computer. Plus, if you sign in to a synchronized browser account using a public terminal and forget to sign out, all your browser’s bookmarks and history will be available to the next user. If you’re signed in to Google Chrome, then even your Google calendar, YouTube, and other aspects of your Google account become exposed. If you must use a public terminal, be vigilant about signing out before you leave. Another downside of syncing is that all interconnected devices will show the same content. If you live alone, that may be fine. But if you share an iCloud account, bad things can happen. Parents who allow their children to use the family iPad, for example, might unintentionally expose them to adult content. 5 In an Apple store in Denver, Colorado, Elliot Rodriguez, a local account executive, registered his new tablet with his

existing iCloud account. Instantly all his photos, texts, and music and video downloads were available to him on the new tablet. This convenience saved him time; he didn't have to manually copy and save all that material to multiple devices. And it allowed him access to the items no matter what device he chose to use. At some point later on Elliot thought it was a good idea to give his older-technology tablet to his eight-year-old daughter. The fact that she was connected to his devices was a short-term plus. Occasionally on his tablet Elliot would notice a new app his daughter had downloaded to her tablet. Sometimes they would even share family photos. Then Elliot took a trip to New York City, where he traveled often for business. Without thinking, Elliot took out his iPhone and captured several moments with his New York–based mistress, some of them quite... intimate. The images from his iPhone synced automatically to his daughter's iPad back in Colorado. And of course his daughter asked her mother about the woman who was with Daddy. Needless to say, Elliot had some serious explaining to do when he got home. And then there's the birthday-present problem. If you share devices or synced accounts, your visits to sites might tip gift recipients off to what they'll be getting for their birthdays. Or, worse, what they might have gotten. Yet another reason why sharing a family PC or tablet can present a privacy problem. One way to avoid this is to set up different users, a relatively easy step in Windows. Keep the administrator privileges for yourself so that you can add software to the system and set up additional family or household members with their own accounts. All users will log in with their own passwords and have access to only their own content and their own browser bookmarks and histories. Apple allows for similar divisions within its OSX operating systems. However, not many people remember to segment their iCloud space. And sometimes, seemingly through no fault of our own, technology simply betrays us. After years of dating several women, Dylan Monroe, an LA-based TV producer, finally found "the one" and decided to settle down. His fiancée moved in, and, as part of their new life together, he innocently connected his future wife to his iCloud account. When you want to start a family, it makes sense to connect everyone to one account. Doing so allows you to share all your videos, texts, and music with the ones you love. Except that's in the present tense. What about your digitally stored past? Sometimes having an automatic cloud backup service like iCloud means that we accumulate many years' worth of photos, texts, and music, some of which we tend to forget, just as we forget the contents of old boxes in the attic. Photos are the closest thing we have to memories. And yes, spouses have been coming across shoe boxes of old letters and photographs for generations now. But a digital medium that allows you to take literally thousands of high-definition photos without too much effort creates new problems. Suddenly Dylan's old memories—some of them very private indeed—came back to haunt him in the form of photos that were now on his fiancée's iPhone and iPad. There were items of furniture that had to be removed from the house because other women had performed intimate acts on that sofa, table, or bed. There were restaurants where his fiancée refused to go to because she had seen photos of other women there with him, at that table by the window or in that corner booth. Dylan obliged his fiancée lovingly, even when she asked him to make the ultimate sacrifice—selling his house once the two of them were married. All because he'd connected his iPhone to hers. The cloud creates another interesting problem. Even if you delete your browser history on your desktop, laptop, or mobile device, a copy of your search history remains in the cloud. Stored on the search engine company's servers, your history is a bit harder to delete and harder to not have stored in the first place. This is just one example of how surreptitious data collection without the proper context can be easily misinterpreted at a later date and time. It's easy to see how an innocent set of searches can go awry. One morning in the late summer of 2013, just weeks after the Boston Marathon

bombing, Michele Catalano's husband saw two black SUVs pull up in front of their house on Long Island. When he went outside to greet the officers, they asked him to confirm his identity and requested his permission to search the house. Having nothing to hide, although uncertain why they were there, he allowed them to enter. After a cursory check of the rooms, the federal agents got down to business. "Has anyone in this household searched for information on pressure cookers?" "Has anyone in this household searched for information on backpacks?" Apparently the family's online searches through Google had triggered a preemptive investigation by the Department of Homeland Security. Without knowing the exact nature of the Catalano family investigation, one might imagine that in the weeks following the Boston Marathon bombing certain online searches, when combined, suggested the potential for terrorism and so were flagged. Within two hours the Catalano household was cleared of any potential wrongdoing. Michele later wrote about the experience for Medium—if only as a warning that what you search for today might come back to haunt you tomorrow. 6 In her article, Catalano pointed out that the investigators must have discounted her searches for "What the hell do I do with quinoa?" and "Is A-Rod suspended yet?" She said her pressure-cooker query was about nothing more than making quinoa. And the backpack query? Her husband wanted a backpack. At least one search engine company, Google, has created several privacy tools that allow you to specify what information you feel comfortable keeping.7 For example, you can turn off personalized ad tracking so that if you look up Patagonia (the region in South America) you don't start seeing ads for South American travel. You can also turn off your search history altogether. Or you could not log in to Gmail, YouTube, or any of your Google accounts while you search online. Even if you are not logged in to your Microsoft, Yahoo, or Google accounts, your IP address is still tied to each search engine request. One way to avoid this one-to-one match is to use the Google-proxy startpage.com or the search engine DuckDuckGo instead. DuckDuckGo is already a default option within Firefox and Safari. Unlike Google, Yahoo, and Microsoft, DuckDuckGo has no provision for user accounts, and the company says your IP address is not logged by default. The company also maintains its own Tor exit relay, meaning that you can search DuckDuckGo while using Tor without much of a performance lag.8 Because DuckDuckGo doesn't track your use, your search results won't be filtered by your past searches. Most people don't realize it, but the results you see within Google, Yahoo, and Bing are filtered by everything you searched for on those sites in the past. For example, if the search engine sees that you're searching for sites related to health issues, it will start to filter the search results and push the results related to health issues to the very top. Why? Because very few of us bother to advance to the second page of a search result. There's an Internet joke that says that if you want to know the best place to bury a dead body, try here of the search results. Some people might like the convenience of not having to scroll through seemingly unrelated results, but at the same time it is patronizing for a search engine to decide what you may or may not be interested in. By most measures, that is censorship. DuckDuckGo does return relevant search results, but filtered by topic, not by your past history. In the next chapter I'll talk about specific ways websites make it hard for you to be invisible to them and what you can do to surf the Web anonymously.