Chapter 3

Privacy

Is Privacy Dead?

With so many news headlines recently about privacy invasions, it may seem as if privacy is dead. Some people say, well, all my data is out there already, and I have nothing to hide, so I don't care. I'm a needle in a haystack. Others fear using websites and tools used by most people (like Facebook) because they've heard scare stories about what these sites know about us.

It's true that in many ways our data is no longer private, but it's also true that we can take steps to make our data more private. That's what this section is about. You can learn to use tools like ad blockers, private browsing, private search engines, anonymous browsers, encrypted messaging, and more. I'll define these tools, explain how to get them, and discuss under what circumstances you might want to use them.

Private Browsing and Searching

Targeted Advertising

Have you ever noticed that ads appearing on Facebook or other websites are showing you products that you recently looked at elsewhere? This can feel quite eerie, and some people fear that Facebook is spying on them. There are even those who fear that Facebook is listening to their conversations through the microphone on their phone.[1]

What's actually happening is something called "targeted advertising." It works like this: there are ad networks whose goal is to show you relevant ads, based on your web browsing behavior. They use a bit of code called a "third-party cookie" to do this. Cookies have been in use by websites for a long time. They are bits of text that are stored in your browser for the purpose of saving your preferences for a particular site—preferences like your username, your zip code (for weather sites), your game scores, and the like. Cookies set by the site you are currently on are called "first-party cookies." They save your information in order to make it easier for you the next time you visit. Third-party cookies are used by ad networks, and they are shared by all the members of an ad network. So if you are browsing for new shoes on one site, the next day you might see ads for similar shoes on other sites or on Facebook. Some people don't mind this because they are seeing ads that are relevant for things they are interested in. Others don't like it and feel it to be an invasion of privacy.

If it bothers you, there are ways you can opt out. One of the easiest ways is to install an ad blocker extension in your web browser. One of the most popular ad blockers is Adblock Plus. It's a free, open-source tool that you can install in browsers like Chrome, Safari, Firefox, and more. It can hide ads and disable tracking with those third-party cookies described above. You can get mobile app versions for iOS and Android as well. For a good list of recommended privacy tools like this, see the article "Best Ad Blockers and Privacy Extensions," by John Corpuz, on Tom's Guide.[2] Most of these tools have the ability to whitelist particular sites. You may want to allow ads on certain sites you want to support since they rely on advertising dollars. It's just a quick click of a button in your browser to allow ads on a particular site.

Adblock Plus
https://adblockplus.org

Adblock Plus for iOS
https://itunes.apple.com/us/app/adblock-plus-abp-remove-ads-browse-faster-without-tracking/id1028871868?mt=8

Adblock Plus for Android
https://adblockplus.org/android-install

To turn off targeted advertising in Facebook, go to your Settings, Ads, Ad Settings, then "Ads based on your use of websites and apps." You can choose to turn it off or leave it on. Facebook reminds you that you will still see ads, just not those based on what you do on other websites. Facebook calls these "interest-based ads."

This type of targeted advertising is so common and on so many sites that it almost seems creepy—you look at something, and suddenly it appears on all the other sites you visit.[3]

Your Search Engine History

If you wonder how easy it is for others to see your search history, the answer is, *very* easy. If you share your computer with others and have a snoopy friend or family member, all they have to do is visit the History menu of your browser. The History menu was designed to be a convenient way to go back to sites you've visited in the past, especially when you can't remember what they were called. Just browse through your history until you find the site you're looking for. But sometimes people use this feature to see what sites others have been visiting.

Also, Google tracks your search history when you are logged into any Google services, such as Gmail, YouTube, Google Voice, Google Contacts, and so on. You can log out of Google before you do a search, but it's possible that not being logged in will decrease the relevancy of your Google results. Google uses your previous searches to "personalize" your results. It is possible to delete your search history by visiting your My Activity page. From there you can delete individual searches or delete your entire history. If you've never looked at your My Activity page, it's worth taking a look at. You might be surprised how much data is there.

Google—My Activity
https://myactivity.google.com

To keep your searches private from people who share your computer, you can use private browsing (known as Incognito Mode in Chrome). This allows you to open a new private window where your search and browsing history won't be tracked. This feature is found in the File menu of your browser; look for New Incognito Window or New Private Window. You can do this in your mobile browsers also. In Safari on an iPhone, tap the squares to open a new tab, then tap Private. You'll get a window that looks different and reminds you that you are in Private mode. To turn it off, tap Private again—it's a toggle.

Websites and Apps for Privacy

Another solution for private browsing is to use special apps or search engines. Two of the best are Firefox Focus (a mobile app for iOS and Android) and DuckDuckGo (a private search engine website and mobile app).[4] Firefox Focus is set up for automatic private browsing. It doesn't track you or let ad networks track you. You type into a search box and browse from there. You can hit the Erase button when you're finished to erase everything you've done in that session. It's handy for an occasional private search on your mobile device. It's not convenient to use it as your primary browser because it doesn't have features we've come to expect, like tabs and bookmarking. But it's great as a supplement to your primary browser.

DuckDuckGo is a search engine that is focused on protecting your privacy. It doesn't track your searches ever. You can find it on the web or use the DuckDuckGo mobile app for Android or iOS.

DuckDuckGo
https://duckduckgo.com

Using Private Mode or these special privacy apps will hide your searches from those who share your computer, but certain parties can still see what you've searched—your internet service provider, your employer (if you are on a company network), and the individual sites that you visit (since they keep logs of the IP addresses of visitors). And in early 2017, the US Senate voted not to implement privacy regulations that would have required ISPs to get your consent before selling your web browsing data to advertisers.[5]

So if you don't want your ISP to have your browsing data, there are some other useful tools. The first is a VPN (virtual private network), discussed in the last chapter. A VPN will encrypt your entire session so that even your ISP can't see which sites you are visiting.

If you also want to be anonymous, there is a useful tool called Tor (The Onion Router). It consists of software and a global network of servers that make it difficult to trace web traffic back to its source.[6] It works by sending your traffic through a relay of different servers, each with a layer of encryption that is peeled back at each relay in order to find out where to send it to next. This makes it very difficult to find out which computers are visiting which sites. Tor has a desktop web browser and mobile apps for many different platforms. You can download the browser the website and find the mobile apps in the iTunes store or Google Play. There are several different apps, and two of the most highly recommended ones are Onion Browser (iOS), and Orbot (Android).

Tor
https://www.torproject.org

Onion Browser
https://mike.tig.as/onionbrowser

Orbot
https://guardianproject.info/apps/orbot

If you need anonymity, Tor is a good option. It can be slow, however, since it's sending your traffic through so many relays, so it's not practical to use for everything. Who uses Tor? It's used by criminals on the dark web, journalists who need to protect their sources (and themselves), people in countries with restricted internet, and everyday users who value privacy. Even though criminals sometimes use it, it also has many positive uses for activists, whistleblowers, law enforcement, IT professionals, and people researching sensitive topics.[7]

Your Location History

Many mobile apps use location tracking features to provide useful information, like directions and traffic reports or weather for your current location. Often the location tracking continues even when you're done using the app.

If you've never checked the location settings for the apps on your mobile devices, it can be surprising to see how completely your movements can be tracked. For an example, take a look at your location history on a map in Google's Timeline. You'll see all the places where Google has tracked you, going back in time. Most of this data is from the location services on your mobile phone. Android users have this data collected routinely, and Apple users have it collected if you use Google Maps or Google search on your iPhone or iPad. Your location data is tracked from cell towers, Wi-Fi, and GPS satellites. If you don't want to be tracked this way, you can turn off your location history in Google on the Help page. You can pause tracking temporarily or turn it off permanently. You can also delete all of your past location history.

Google—Timeline
https://www.google.com/maps/timeline

Google Support—Manage or Delete Your Location History
https://support.google.com/accounts/answer/3118687

It's also a good idea to check the location settings for individual apps. On Apple devices (iOS 11), you can do this by going to Settings, Privacy, Location Services. On that screen, you can see a list of all your apps that use location data. You can turn off Location Tracking entirely for all apps, but if you do that, you won't be able to use many important features of your phone, such as navigation in Google Maps. So instead, look at the list of apps, and for each one, select Never, While Using the App, or Always. I set most of my apps to While Using the App, but for Google Maps, I keep it on Always because it's needed for navigation, real-time traffic and transit updates, and seeing places near me. I use these features often, so I feel the trade-off is worth it. When you are on the screen for each app, be sure to read the notes about how the app uses your location. For example, I have a travel app called App in the Air. The note says, "App in the Air will use your location information to identify nearby airports and enable in-airport navigation." These notes make it easy to know what features you will lose if you set it to Never.

At the bottom of the iOS Location Services screen, after the list of apps, is a choice called System Services. Here you can turn location on or off for features like Compass Calibration, Emergency SOS, Find My iPhone, Location-Based Apple Ads, and so on. For detailed advice on which settings to choose, see Christian Zibreg's blog post "How to Stop iPhone from Tracking Your Location," *iDownload Blog.*[8] For instructions on how to manage your location settings on Android, see Brittany McGhee's article "How to Stop Android Apps Accessing Your Location."[9]

If you would like to learn more about what your location history can show about you, along with the privacy implications, read "Location Tracking" on the privacy website Me and My Shadow.[10] As you can see, there is a trade-off between the convenience of location services and the privacy implications. Luckily, most modern mobile devices have fine-grained settings, as described above, that you can use in ways that make sense for you.

Facebook Privacy Settings

If you use Facebook, you'll find it useful to check your privacy settings and ad settings. From the Facebook Settings screen, start by looking at the section called Privacy. Here you can make choices under "Who can see my stuff?" "Who can contact me?" and "Who can look me up?" For each item, such as Future Posts, you can select from choices like Public, Friends, Friends Except..., Specific Friends, Only Me, and Custom. Using these options, you can make lists of groups of friends and fine-tune who sees your posts. You can also choose who can send you friend requests and who can look you up by your email address or phone number.

Another section of Facebook settings that's worth looking at is the Ads section. You may want to begin with the subsection called Ad Settings. Here you can say Yes or No to "Ads based on your use of websites and apps." This is the targeted advertising that we discussed earlier in the chapter. Facebook calls this "online interest-based advertising" and reminds you that if you say No, you'll still see ads; they just won't be based on your interests and therefore probably less relevant.

If you don't want all of your friends to see everything that you like on Facebook, you can turn that off in the subsection called "Ads with your social actions." The two choices for this are No One or Only My Friends.

Another part of the Ads section that is worth looking at and adjusting is the subsection called Your Interests. Here you'll see many specific topics related to things you've clicked on or liked on Facebook. It's worth looking through these and deselecting the topics that are not of interest to you. Some of these are very broad, like Air Travel, and others are specific, like Human Rights Watch. For each of these, Facebook tells you that "you have this preference because you liked a page related to [fill in the topic]." If you care about the type of ads you see on Facebook, this could help make the ads more relevant to you.

Facebook has a page that describes how it collects information about you for targeted advertising. It's worth reading to understand how this works.[11] M.J. Kelly, a blogger for Mozilla, also recommends checking your app settings to see what Facebook apps you're sharing information with. To learn more about Facebook privacy, see M. J. Kelly's blog post "Facebook Privacy Tips: How to Share without Oversharing."[12]

More Privacy with Encryption

Encrypted Messaging

An excellent way to keep your messaging private is to use an app that encrypts all of your messages by default. This means that even if your network traffic is being monitored, no one can read the contents of your text messages, not even those who run the app's servers. One of the best apps for this is called Signal, from Open Whisper Systems. It's recommended by security experts like Bruce Schneier and also by Edward Snowden.

Signal
https://signal.org

Signal is available for desktop and mobile platforms and is very easy to use. See its website for links to the apps for various platforms, including iPhone, Android, Mac, Windows, and Linux. The Electronic Frontier Foundation has some useful guides to using Signal,[13] but it's so easy, you likely won't need a guide. You can also make secure video calls or voice calls with Signal. Signal is free and open-source, and Open Whisper Systems doesn't do any kind of ad tracking.[14] It's a nonprofit, supported by grants and donations.

Of course, if you want encrypted communication, you'll need to convince those you communicate with to use Signal. Signal is very good for situations where you need the most secure and private communication. If you back up your phone to a cloud service, your Signal messages are not included. They stay safely encrypted on your device. When you share your contact list with the app, so you can find other users, Signal encrypts the list before it goes to the server. It's used only to match you with people in your contacts list who also have Signal.

When would you need this level of privacy? You might use Signal if you are worried about snooping from your government, law enforcement, employers, or criminal groups. You might be an activist, a journalist protecting sources, or just someone who cares a lot about privacy. News sources like the *New York Times* recommend that people use Signal and similar apps to send them confidential tips.[15] This is a good app to recommend to someone you know who is in a situation that requires very strong privacy.

To learn more about how Signal compares to other secure messaging apps, read Michah Lee's article "Battle of the Secure Messaging Apps: How Signal Beats WhatsApp" in the *Intercept*.[16] Signal is worth using for keeping your messages and phone calls completely private.

Encrypted Email

If you want to communicate securely by email, there are some useful tools that will enable that. Most email providers have a web version, and you should always look to see if the address bar contains `https` at the beginning of the URL (instead of `http`). This is known as transport-layer encryption and is often used by retail websites and banks.

This is good, but even with https, your email provider still gets an unencrypted copy of your messages. If you are worried about government or law enforcement contacting your email provider with a warrant to read your messages, this won't give you privacy. For example, let's say you are working for a company and learn of wrongdoing that you would like to report to the media by email. Even if your company email uses `https`, the company will still be able to read your messages, so it's not a good idea to use its system if you are a whistle-blower.

This is when a fully encrypted email app becomes useful. One of the best and easiest ones to use is a webmail app called ProtonMail. It's a secure email system, based in Switzerland. It stores all of your email fully encrypted, so even ProtonMail itself can't read your messages. If a warrant was issued for your messages, they would have nothing to turn over. It has a web version and mobile apps for iOS and Android.

ProtonMail
https://protonmail.com

Learn more about ProtonMail in Melanie Pinola's article "ProtonMail Is the Easiest Way to Send and Receive Encrypted Emails," in Lifehacker.[17]

Another encryption tool you might want to try is Mailvelope. It's a browser extension for Chrome and Firefox that you can use to encrypt messages in various webmail providers, like Outlook.com, Yahoo Mail, or Gmail. Learn more in Andy Wolber's article "Simple Security: How Gmail, Mailvelope, and Virtru Make Encrypted Email Easier," in TechRepublic.[18] You may also want to check the Mailvelope installation guide, which describes the basics of how it works.

Mailvelope
https://www.mailvelope.com

Mailvelope Installation Guide
https://www.mailvelope.com/en/help

Metadata: What It Reveals

End-to-end encryption is very useful, but it protects only the contents of your communication, not the fact that you communicated with someone. Metadata is associated with your communications, and this can be mined to learn things about you.

For example, someone who has access to your phone call metadata could find out that you called a suicide prevention service, or an HIV testing service, or your gynecologist and then Planned Parenthood, and so on. They don't know what was said, but they might conclude things about you. If you are calling from your cell phone, then your location can be tracked as well. Metadata that can be found (if you use encryption without a VPN) include which websites you visit, what phone numbers you call or message, and your IP address (which tells the location of your computer).

If you want to protect your metadata, security experts recommend using Tor, a VPN, or both at the same time as full encryption. (Tor and VPNs were discussed earlier in this report). This will make you anonymous (or nearly so, for all practical purposes).[19] To learn more details about Tor, what it's used for, who uses it, and why, see Will Nicol's article "A Beginner's Guide to Tor: How to Navigate through the Underground Internet," in Digital Trends.[20]

Webcam Privacy and Internet of Things

Remote Camera Hacking

Have you ever thought about covering your laptop or desktop computer's camera? Does that seem too paranoid? If you search Google for "laptop camera hacked," you'll see many stories of people who were spied on. It turns out that this kind of spying is something that's fairly easy to do, and there have been many instances of spying on random people through their webcams.[21]

Security experts recommend that you cover your laptop camera, because even on Macs (which are usually less vulnerable to malware), the indicator light for your camera can be turned off as part of a hack.[22] So you have no idea that your camera is recording.[23]

According to former hacker (now security expert) Kevin Mitnick, even your cell phone camera can be hacked by those willing to pay the cost of the software to do it. For someone who has physical access to your phone and knows your passcode, there is software that anyone can buy online to enable this kind of spying, for example, Flexispy. Remember, someone has to have access to your phone to do this, so it's usually done by someone who knows you, such as a significant other who suspects you of cheating.

Flexispy
https://www.flexispy.com

Cell phone cameras can be hacked remotely, but that is very, very expensive, so it's usually done by only nation states or government agencies like the FBI, law enforcement, or the NSA. There are software exploits that can be purchased for more than a million dollars that will let someone remotely spy on an individual's iPhone without being easily detected.[24] Android exploits are a bit cheaper, since Android devices are easier to hack.

Experts recommend the simple solution of covering your computer's webcam. You can search online for "webcam cover" for commercial solutions, or try one of the simple DIY approaches from Jacob Brogan's blog post, "What's the Best Way to Cover Your Webcam?" from *Slate*.[25] I use his suggestion of Japanese washi tape, since it's easy to remove without leaving a residue.

It's also recommended that you keep your operating systems up-to-date on your computers and mobile devices. Whenever software vulnerabilities are found (such as those that could enable remote camera hacking), vendors rush to release updated versions that fix the problem. So it's a good idea to install updates soon after they are released.

Smart Home Devices

Smart speakers like Amazon Echo and Google Home have some people worried. Do we really want a device that is always listening in our homes? Luckily, it's not as awful as it seems.

The way these devices work is that they listen for the assigned "wake word," such as "Alexa," or "Hey Google." Then they record what you ask them, stopping the recording when they begin to answer a few seconds later. So even though the microphones need to be on in order to hear your wake word, they aren't recording except after each wake word and before each answer.

These devices send your questions to the cloud in order to pull the information they need from the internet. So your questions are stored on Amazon's or Google's servers. You can choose to go online and delete particular recordings, or all of your recordings if you like. For Amazon, go to your Alexa mobile app and look under Settings, History. From there you can see and hear all of your saved recordings and delete them one by one. If you want to delete all of them at once, you can do that from your computer's web browser on the Amazon site, under Manage Your Content and Devices, Your Devices, Amazon Echo, Manage Voice Recordings. From there you can delete all of the saved recordings. Google has the same features on its My Activity page. Look for Assistant, choose that and see each recording, which you can delete one by one. To delete a whole batch of recordings (or all of them), look for the three dots on the top menu bar of My Activity. In that menu, select Delete Activity By, then choose Assistant as the product, and enter a date range. From there you can delete a batch of recordings.

Google—My Activity
https://myactivity.google.com

It's also good to know that you can turn off the microphones anytime you like on these devices (if you aren't going to use them for a while). This is handy when you are listening to a podcast or TV show that mentions your wake word frequently. The off button for an Echo is on the top, and for Google Home is on the back.

Other privacy features are available as well, such as setting a PIN code for voice purchasing on the Echo (so you can order products by voice only if you know the PIN). Google Home has a way to train it to recognize different people in your household and connect each person only to their own calendar so that others can't access your appointments. Amazon's Alexa service has also added the feature of recognizing individual voices after you train it. You can also choose to turn off personal results (calendar, upcoming flights, etc.) in the settings for Google Home.[26]

For more details on controlling your privacy on these devices, see David Nield's Field Guide article "How to Lock Down Your Privacy on the Amazon Echo and Google Home."[27] And for some interesting thoughts about the future of internet-connected devices, see "The Internet of Things Connectivity Binge: What Are the Implications?" by Lee Rainie and Janna Anderson, Pew Research Center.[28] This article consists of interviews with several experts and concludes with this thought: "Despite wide concern about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the next few years, tying machines to machines and linking people to valuable resources, services and opportunities."[29]

Notes

1. Emma Hinchliffe, "Why Everyone Is So Convinced Facebook Is Spying on Their Conversations," Mashable, October 7, 2017, http://mashable.com/2017/10/07/why-it-feels-like-facebook-is-spying/#It3XCCGa8aqZ; Antonio Garcia Martinez, "Facebook's Not Listening through Your Phone. It Doesn't Have To," *Wired*, November 10, 2017, https://www.wired.com/story/facebooks-listening-smartphone-microphone.
2. John Corpuz, "Best Ad Blockers and Privacy Extensions," Tom's Guide, July 6, 2017, https://www.tomsguide.com/us/pictures-story/565-best-adblockers-privacy-extensions.html.
3. For a good story that explains the details of targeted advertising, see the article "Facebook's Not Listening through Your Phone. It Doesn't Have To," by Antonio Garcia Martinez, in *Wired*, November 10, 2017, https://www.wired.com/story

/facebooks-listening-smartphone-microphone.

4. Nick Nguyen, “Introducing Firefox Focus—A Free, Fast Private Browser for iPhone,” *Mozilla Blog*, November 17, 2016, https://blog.mozilla.org/blog/2016/11/17/introducing-firefox-focus-a-free-fast-and-easy-to-use-private-browser-for-ios; DuckDuckGo homepage, accessed January 5, 2018, https://duckduckgo.com.
5. Jon Brodkin, “Senate Votes to Let ISPs Sell Your Web Browsing History to Advertisers,” Ars Technica, March 23, 2017, https://arstechnica.com/tech-policy/2017/03/senate-votes-to-let-isps-sell-your-web-browsing-history-to-advertisers.
6. Lee Mathews, “What Tor Is, and Why You Should Use It to Protect Your Privacy,” *Forbes*, January 27, 2017, https://www.forbes.com/sites/leemathews/2017/01/27/what-is-tor-and-why-do-people-use-it/#41e4fbb97d75.
7. Learn more about use cases for Tor on the “About Tor” page from the project website (https://www.torproject.org/about/torusers.html.en).
8. Christian Zibreg, “How to Stop iPhone from Tracking Your Location,” *iDownload Blog, April 28, 2016,* www.idownloadblog.com/2016/04/28/how-to-stop-phone-location-tracking.
9. Brittany McGhee, “How to Stop Android Apps Accessing Your Location,” AndroidPIT, February 7, 2017, https://www.androidpit.com/how-to-stop-android-apps-accessing-your-location.
10. “Location Tracking,” Me and My Shadow, last updated February 15, 2017, https://myshadow.org/location-tracking.
11. See the page “About Facebook Ads,” Facebook, https://www.facebook.com/ads/about.
12. See M. J. Kelly’s blog post “Facebook Privacy Tips: How to Share without Oversharing,” *Mozilla Blog, January 25, 2017,* https://blog.mozilla.org/internetcitizen/2017/01/25/facebook-privacy-tips.
13. Electronic Frontier Foundation, “How to: Use Signal on iOS,” Surveillance Self-Defense, last reviewed March 17, 2017, https://ssd.eff.org/en/module/how-use-signal-ios; Electronic Frontier Foundation, “How to: Use Signal for Android,” Surveillance Self-Defense, last reviewed March 17, 2017, https://ssd.eff.org/en/module/how-use-signal-android.
14. Read the Privacy Policy (https://signal.org/signal/privacy) for more information.
15. “Got a Confidential News Tip?” *New York Times* website, accessed January 5, 2018, https://www.nytimes.com/newsgraphics/2016/news-tips.
16. Michah Lee, “Battle of the Secure Messaging Apps: How Signal Beats WhatsApp,” The Intercept, June 22, 2016, https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signal-beats-whatsapp.
17. Melanie Pinola, “ProtonMail Is the Easiest Way to Send and Receive Encrypted Emails,” Lifehacker, March 17, 2016, https://lifehacker.com/protonmail-is-the-easiest-way-to-send-and-receive-encry-1765491376.
18. Andy Wolber, “Simple Security: How Gmail, Mailvelope, and Virtru Make Encrypted Email Easier,” TechRepublic, July 13, 2016, https://www.techrepublic.com/article/simple-security-how-gmail-mailvelope-and-virtru-make-encrypted-email-easier.
19. Glenn Fleishman, “Anonymous Browsing with Tor Reduces Exposure but Still Has Risks,” Macworld, January 17, 2017, https://www.macworld.com/article/3152823/security/anonymous-browsing-with-tor-reduces-exposure-but-still-has-risks.html.
20. Will Nicol, “A Beginner’s Guide to Tor: How to Navigate through the Underground Internet,” Digital Trends, January 29, 2016, https://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet.
21. Mark Yates, “Time to Tape Over the Camera on Your Laptop,” AVG, September 26, 2016, https://www.avg.com/en/signal/why-you-should-cover-the-camera-on-your-laptop-or-tablet; Charlie Osborn, “Shodan: The IoT Search Engine for Watching Sleeping Kids and Bedroom Antics,” ZDNet, January 26, 2016, www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy.
22. Bruce Snell, “IoT and Privacy: Keeping Secrets from Your Webcam,” McAfee, February 10, 2016, https://securingtomorrow.mcafee.com/consumer/family-safety/iot-and-privacy-keeping-secrets-from-your-webcam.
23. Ashkan Soltani and Timothy B. Lee, “Research Shows How MacBook Webcams Can Spy on Their Users without Warning,” *Washington Post*, December 18, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/?utm_term=.58f6603424b6.
24. Chris Synder, “Hackers and Governments Can See You through Your Phone’s Camera—Here’s How to Protect Yourself,” Business Insider, March 7, 2017, www.businessinsider.com/hackers-governments-smartphone-iphone-camera-wikileaks-2017-3.
25. Jacob Brogan, “What’s the Best Way to Cover Your Webcam?” from *Slate*, September 15, 2016, www.slate.com/blogs/future_tense/2016/09/15/the_best_ways_to_cover_a_webcam.html.
26. See the Google Home help page “Data Security & Privacy on Google Home,” accessed January 5, 2018, https://support.google.com/googlehome/answer/7072285?hl=en.
27. David Nield, “How to Lock Down Your Privacy on the Amazon Echo and Google Home,” April 27, 2017, https://fieldguide.gizmodo.com/how-to-lock-down-your-privacy-on-the-amazon-echo-and-go-1794697554.
28. Lee Rainie and Janna Anderson, “The Internet of Things Connectivity Binge: What Are the Implications?” Pew Research Center, June 6, 2017, www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications.
29. Ibid.