"Never sit at a table you can't walk away from."
—Joss Whedon

2. but it's just my phone number

You'd be surprised by how far one creep or criminal can get with your phone number. It's hard to believe that one little thing can cause so much trouble, but keeping your private life under wraps comes down to controlling certain pieces of information as much as you possibly can. You're about to find out exactly what information I'm talking about and how to protect all of it.

YOU CONTROL WHAT YOU SHARE

It's really important to safeguard pieces of personally identifying information, like your phone number, online. Social media and advertising companies are continually compiling dossiers on you, trying to match information across services

and devices in order to piece together the most complete profile they can. The more complete the info, the more valuable it is when they sell it to and trade it with third parties. From these third parties, your private information becomes public in people-search databases. As if this weren't bad enough, malicious hackers look for clues to your private information in everything you do online.

The armor you build around that identifying information protects every aspect of your privacy. Of course, what you do in private or choose to share with friends is your own business. But if you want to be confident that your information remains personal, only share identifying info with people you trust.

For example, if you enjoy sex or explore aspects of your sexual identity using technology, that experience should belong to you. Only you should get to decide whether it was a good or bad thing to do. Sexuality is one of the most important ways in which we identify, establish, and maintain our boundaries. Just as importantly, you should get to decide if that experience (whether it's sharing intimate photos, talking dirty on the phone or via voice chat, sexting, having any kind of online sex, or just disclosing something on a sexual topic) gets shared with anyone else. Personal information and experiences should be private and under your control, unless you decide otherwise. If you do decide to share that information, you should know exactly what you're agreeing to.

PRIVATE SPACES AND ACTIVITIES

Private exploration, sexual and otherwise, is something we do to better understand ourselves. We experiment with different ideas about who we are and different ways of expressing our identities. Sometimes, we may even play around with being something (or someone) that we're not like at all in the real world. Private spaces are where we get to safely figure out who we are.

Privacy is critical to being able to decide what you like, discover what feels right and wrong for yourself, and findand keep your boundaries. That's just the truth and always has been. What's changed is the role technology plays in our private experiences. If you have a sexual moment in your room, that moment is still all yours unless you choose to share it. But when you have a private moment or experience online, you're taking a risk with your privacy.

Until the online revolution, our private spaces for exploration were our bedrooms and bathrooms, our homes, our phone calls, and our inner fantasy worlds. Now, those spaces can include texts, emails, photos, videos, and direct messages to trusted friends or family members. Online, private spaces include email inboxes, chat rooms, Internet Relay Chat (IRC), social media profiles, not-public messaging systems (Twitter direct messages (DMs), Facebook chat), dating websites, message boards, and all the places where your personal information resides. But those spaces are only private if you can really trust the people you share that information with.

For example, if you send or communicate something private while at work, at school, or even on Facebook, it might not be private because it might not actually be "yours" anymore—legally and, to some degree, practically speaking. The places where you experience private time online and on your phone are usually watched and monitored by the companies who host those services, too.

The problem is that not everyone understands or agrees on what constitutes a private space online, and some people don't know what information they need to protect and keep private. Even one piece of private information can unlock a trail that will expose most, if not all, of the other information it's attached to (just read Mat Honan's story in Chapter 3).

No one has a clear idea about what systems can be trusted completely, what systems should never be trusted, and which

systems to watch very carefully. Worse, many online companies, including some of the big ones you'd think you could trust, have made it their business to take advantage of that confusion and misplaced trust by leveraging privacy laws that are way behind the times to collect, sell, and trade your private information as data, in their databases. That's a problem because it takes away your control over things that could expose or hurt you, like your identifying information and metadata (detailed background information on you) that these companies collect when you use their services. The sad fact is that these companies care about their bottom lines and their corporate advertisers more than they do about you as a consumer, so don't believe otherwise for a minute. Companies like Twitter, Google, and Facebook need to convince you to share your private information because their advertisers "need" access to what rightfully belongs to you.

But you have a choice, and it's not your job to keep corporations wealthy by empowering them to invade your personal space. Your private information and activities should remain private, including all of the following:

- What you say or express in private chat or direct messages
- What you say or express in emails
- What you say or express on the phone
- What you say or express in your personal relationships
- Your text messages
- Personal photos that you share
- Your activity on dating websites
- Information related to your sexual activities and sexual orientation

- Information related to your health and medical records, including searches, doctor visits, and associated communications
- Information related to your gender identity
- Time you spend doing things that you want to keep to yourself
- Anything you keep in private files on your computer or phone

Next, I'll explain what information you should watch most closely and how to ensure that your private activities stay private.

LOCK DOWN YOUR PERSONALLY IDENTIFYING INFORMATION

Lots of things tempt us to give up our email address, phone number, physical address, ZIP code, and so on—sometimes harmlessly.

The information you should guard most closely is your *personally identifying information* or PII, or just your *personal information*. Even a few pieces of PII can be used to identify, contact, or locate you, allowing malicious people to attack you, stalkers to find you, and entities to get more information about you than you want to share. Companies like Facebook and Google use your PII for profit. Don't just give it away.

The following sections list what you should consider personal information, and each is named after a stoplight color so you can see which items are critical. The items on the red alert list can be used directly against you, and you should never give out or share these with any person, company, app, or website that you don't know or trust. The yellow alert list contains items that you should be very careful with because

malicious hackers and stalkers can use them, but they can't hurt you with this information unless they have other pieces of information, too.

If anyone or any company asks for any of the items on your red or yellow lists, be on guard. But don't freak out if you've already given these things to other companies, no matter how shady they are. Even when things go screwy, it's almost never too late.

Red Alert List

Everything in this section can be used to directly hurt or harm you, steal your identity, make you physically unsafe, threaten or expose your loved ones, steal your money, or access your online accounts. *DON'T give this information out, and DON'T publish it online. DO keep close track of where it has been seen and who knows about it.*

Red alert items can't be changed (or are very hard to change) if something goes wrong, so you should watch what happens with everything on this list like a mama hawk:

- Passwords
- Real, full (family) name
- Address of your home, workplace, or school
- Social Security number
- Government ID numbers (driver's license number and passport number)
- Date and place of birth
- Biometric information (fingerprints, facial recognition, voice recognition)
- Computer's IP address (a unique number that identifies your computer on the Internet)

- Specific location (geolocation numbers, like those from your phone or in tagged photos)
- Credit and debit card numbers, security codes, and expiration dates
- Bank account numbers
- Answers to common security questions

Let's talk for a moment about those answers to common security questions. These can include your pet's name, your mother's maiden name, the city you were born in, and often other things that are easy to guess or dig up on your Facebook profile. A million years ago, when Paris Hilton's phone was hacked, the intruder reset her phone's password by getting one security question correct: her dog's name, which was findable on every gossip site in the world.

NOTE *Credit card and bank account numbers are on the red list because while they can be changed, you can usually change them only after there has been a problem. Passwords can also be changed, but anyone that has them also has access to much of your red list information.*

Yellow Alert List

Yellow items can be used with other information to harm you, so avoid giving them out unless you trust the people or companies you share them with. If you choose to share them, keep a close eye on where they appear and who can see them.

Some yellow items can be changed if your personal information falls into evil hands, but changing them isn't easy:

- Name you use day to day, if different from your legal name
- Primary screen name(s)
- Email address (if it's not public)
- Telephone number

- Race, sexual orientation, and gender
- Mailing address (if it's different from your residence; otherwise it's red)
- Country, state, and city of residence
- ZIP code (or postal code)
- Google Voice number

Fortunately, you can make dummy versions of yellow items to use when you don't trust an app, website, social network, or person. Google Voice is on this list because if it's linked to your cell phone number, getting locked out of your Google account means that you'll be locked out of both numbers.

NOTE *Even if yellow items are revealed to bad entities, they still won't sink your ship. Read more about making a dupe copy of your yellow items (and even some Red items) in Chapter 9, "Ninja Tricks."*

If the red and yellow items seem like a lot to manage, or some of the items have already ended up "out there," don't worry. I'll show you how to fix and recover from those big and small privacy mistakes and how to manage your privacy easily going forward.

Green List

Items on your green list are okay to share. This list includes information about you that can't be used to hurt you or that's a dummy version of the real thing. For instance, if the numbers of your single-use credit card are stolen, you'll only lose the amount on the card. That's way better than losing a real credit card, which is tied to your credit score and often various online accounts and could cause a big headache.

Here are some examples of Green items:

- Secondary screen names or account names (say, a throw-away email address that forwards to your primary address)
- Mailing address or PO box
- Digital, online phone number, such as a Skype number
- Email addresses that are not linked to a vital service, such as your bank account
- Photos and videos that don't embarrass you or reveal private information
- Social media profiles on sites where you're confident you understand the privacy settings
- General likes, favorites, and things you enjoy sharing on social media sites
- Single-use or gift credit cards

Apply the red, yellow, and green system to apps and online accounts to judge them for safety. An online account or app that asks for red information gets a red grade. If an app asks for a lot of red or yellow information but doesn't actually require that information in order to function, same thing: the site, account, or app is high risk. Even if it has the best security team in the world, it still gets the red or yellow rating because if it gets attacked, you're in more trouble (and have to do more post-attack cleanup in your life) than with a green app or account.

Information-Sharing Guidelines

As a rule, don't give out personally identifying information too readily. If you wouldn't give some bus driver or a creepy mall cop your home address and phone number, remember

that just because websites ask for (or demand) personal info doesn't mean you have to give it to them. And you can often give fake information to get to the next screen.

Of course, you have to give real billing information when you buy things, but if you're registering with a free site that feels like it's getting too nosy about your business, give it fake information. You're not breaking any law under the sun if you do that. Just don't use someone else's real address; you'll definitely get in trouble for that.

Don't be fooled by websites that offer some sort of reward or prize in exchange for your contact information or other personal details. Usually, your name, browser and computer information, and email address are worth much more to them than whatever they're offering you because they can sell your information to other marketers, who will also resell it. You won't win an iPad, but the marketer will win a few more bucks if you give them your information. And female data sets are always worth more on the market than male ones, because women usually make more buying decisions and spend more money than men. (We're also worth more on the black market for seedy things like hacked webcam access, as mentioned in the story about Miss Teen USA in Chapter 1.)

A couple more things: avoid sending highly personal email to mailing lists and keep sensitive files only on your home computer. Your workplace or school is legally monitoring your Internet use and email on its network, so don't do anything private or sensitive in nature (like banking) on a work or school network. In most countries, employees have little if any privacy protection from monitoring by employers.

HE SAID, SHE SAID

Maybe you're thinking, "Eh, if my phone number gets in the wrong hands, it's really not that that big of a deal. I can always block the caller or hang up. Who cares, right?"

Let me tell you a story.

Every year in Germany, the world's longest-running hacker conference happens just after Christmas—Chaos Communication Congress (CCC). My bosses at CBS have never seen a great reason for me to fly from San Francisco to Hamburg to find news at some hacker gathering to report on over the holidays, when they're all away from the office with their families on the US East Coast. But one year, my interest in hackers and cybercrime got my editors to pay attention to my trip.

I was on my way to the airport Christmas Eve when I got some cryptic Twitter messages from hackers who had told the popular photo-sharing service Snapchat (which supposedly "disappears" your photos after you send them) that the service had a security problem. Snapchat ignored the hackers' warning.

Those same hackers messaged me to say they had found more serious problems with Snapchat and they had written a blog post about it. Right after I broke the news for CBS, malicious hackers took the user information—which included the user's name (the name they registered with), display na,e (handle), and phone numbers—and published all of it online.

On the long flight to CCC, I started chatting with a woman seated next to me about the news story. I explained that parts of Snapchat's huge user information database had been posted online for anyone to download and rifle through, and that the guys who ran Snapchat didn't seem to care.

She asked me whether names, phone numbers, email addresses, or even passwords were online. I told her that as far as we could tell, it was only usernames and phone numbers so far.

Her boyfriend, seated on the other side of the aisle, was listening, and he chose that moment to chime in. "Phone numbers

and names? That's it?" he said. "Oh if it's just phone numbers and our names, whatever."

His girlfriend didn't agree. It was awkward.

This could have been a story about any app, or any of a zillion privacy breaches in the past couple of years. It isn't a story about "right" or "wrong" ways of thinking about privacy. Their reactions just show a great example of the difference between what women and men see as risky exposure. He didn't think it was a big deal for anyone to have his number, username, and real name. She, on the other hand, said it made her worried.

What my seatmate's boyfriend didn't consider is that he could also be a stalking victim—straight guys attract psychos, too. Creeps and stalkers come in all genders and sexual orientations. Men tend to feel a greater sense of physical and social safety, but that feeling is often illusory. Men are victims of malicious activity online all the time, as I'll describe in Chapter 3 with journalist Mat Honan's story.

WORST-CASE SCENARIO

The sad fact is that women have more reasons to be concerned about online privacy than men do, because women are at greater risk for physical violence and are directly targeted more often than men.

What's the worst thing that usually happens to a man's phone number? Someone posts it on Craigslist (or 4chan) in a "call and talk dirty to me" ad. A malicious hacker could then use it to try to reset a password or to try to steal the person's identity (which is actually pretty bad).

But think about what could happen to a woman. Identity theft is awful, but it's not the worst thing. Say you have an online enemy, like an ex or any psycho who's angry, missing you a little too much, unhinged, drunk and upset, or bent on revenge. If that person knows or even suspects that you use

a particular online app like Facebook or Twitter, they can search the app using the information they have (any piece of a real name, username, or phone number) to see if they can find your current information.

Once they get more real information about your world, that stalker, creep, or vengeful ex gets closer to you. They can use your information to try to see what you're up to or, worse, to spy on you, stalk you, or harass you—whether as their real self or with a fake account. Once a heartbroken ex or stalker knows what account to zero in on, they may create a fake account and "friend" you.

Now they can track, harass, bully, and scare you. They can search for your username on other social media sites and apps, like photo sites where you post pictures of your boyfriend, family, pets, school, travels, and workplace. They can search social media sites for a history of your relationships, meaningful or painful experiences, and more. They can use location-tracking websites to follow you and your friends and family. The ways in which companies have woven together our identifying information online means that something as basic as your phone number needs to be protected more than ever.

When that stalker gets your phone number, you're in trouble. With that number in hand, that bad person can call you, find you in online databases, make changes to your accounts and services, or even hack your voicemail.

And it doesn't end there: anyone bent on vengeance will add your number to the dossier they're building about you, likely with the intent to publish it online later, along with your name, usernames, email addresses, and a list of online apps, accounts, and businesses you use. And I'm not talking about signing you up for magazine subscriptions and pizza deliveries, though jerks will do that, too.

I don't have to tell you that exes and stalkers do bad things in real life when they get close enough to the person they're obsessed with. If the malicious creep has posted things online about you to ruin your reputation, like impersonating you or publishing revenge porn of any kind, they could add your phone number to this awful public smear campaign—putting you at serious risk for more stalking and attacks from others.