

"hello"

YOUR IPHONE NEEDS A FACIAL

A phone facial strips away the digital grime, keeping your data free from harmful "bacteria"—the hackers, trackers, and unwanted intruders lurking around.



JESSICA

Why a phone facial?

If you're reading this, I assume you are holding an iPhone in your hand. I will also assume that you've set it up, aka it's not fresh out of the box with "Hello" and "Bonjour" flashing on the screen.

So let me ask you...

1. Do you remember how long ago you set it up?
1. What settings did you enable? Which did you skip?
2. Do you know what other permissions you've enabled since its setup?

If you can't remember, it's okay. It's not just you. Almost everyone forgets or ignores this process. I sure did!

And that's the truth.

The good thing is, **it's not your fault**. This kind of behaviour stems from a corporate strategy designed by tech giants to make their devices appear "safe." Let me explain.

Apple iPhones are known for their privacy. Indeed, Apple markets its brand as a privacy champion, prominently featuring the slogan "Privacy. That's Apple" across its website and advertisements⁷. However, researchers have suggested that this is far from the truth⁷. Keeping your data truly hidden from Apple is virtually impossible⁷.

Many people are aware that third-party apps can compromise their privacy, and Apple's App Tracking Transparency feature helps address this concern⁷. However, beneath Apple's seemingly strong skin barrier lies a hidden blemish: Apple's apps are still collecting your data⁷. So, while Apple positions itself as your privacy defender against others, it conveniently omits instructions for limiting the information it gathers through factory default settings and pre-installed applications.



Safari, Siri, Phone, iMessage, FaceTime, Location Services, Find My, Camera, and Touch ID.

Sound familiar?

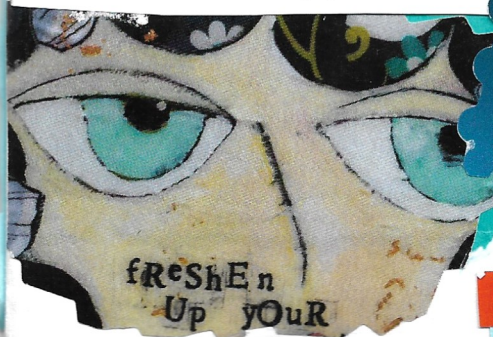
These represent Apple's key apps that are "glued to the platform," meaning they are vital components of Apple's ecosystem and impossible to remove completely⁷. You can't even delete iMessage, Camera, Safari, phone, or the App Store. When you attempt to do so, the only option will be "Remove from Home Screen."

So you may be wondering if you can't delete certain apps, what can you do? Well, here's the bad news: Apple's user interface is deliberately designed to be confusing⁷. When most of us discover we can't delete an app, we simply shrug and move on...this is exactly how Apple gets away with harvesting your data!! They're hoping you'll get frustrated and give up.

Even when you venture into the settings, you have to sift through what seems like a thousand pages, menus upon menus, and hundreds of cryptic labels.

Good news: this zine you are currently holding in your hands is here to help! Just because Apple makes privacy protection difficult doesn't mean it's impossible. If you know where to look, you can control what data Apple collects.

Just as you wouldn't go to bed without washing your face, we can't let your phone sleep with all that digital dirt accumulating in its virtual pores. This zine will walk you through the process of giving your iPhone a full "privacy facial." It will expose hidden settings scattered throughout your iPhone, cleanse away tracking mechanisms, extract unwanted permissions, and help you establish a maintenance routine to keep your digital life truly private.



HOW TO GET STARTED
DO'S AND DON'TS



Table of contents :

Quiz	5
Passcodes & Passwords...	6-7
Lock Screen	6
Application	7
Location Services...	8-9
Siri & Dictation...	10
Bluetooth	11-12
iCloud	13-14
Activity	14
Conclusion	15
References	16

3-in
Facial C



TM/MC

Lets get Protected

Quiz: Is your digital skin safe?

How exposed is your digital skin? Circle your answers:

How many apps on your phone have location access?

- A. 0-5
- B. 6-10
- C. I have no idea (yikes!)

When was the last time you reviewed app permissions?

- A. Last week
- B. Last year
- C. Never (double yikes!)

"How far back did you say?"

Is your phone passcode longer than 4 digits?

- A. Yes
- B. No
- C. What passcode? (triple yikes!)

Do you read privacy policies before clicking "Accept"?

- A. Always
- B. Sometimes
- C. LOL, no one does that

Legend

Mostly A: Your digital skin is glowing!

Mostly B: Your pores need attention. You're doing okay, but a privacy review wouldn't hurt.

Mostly C: Your digital skin is exposed! READ THIS ZINE IMMEDIATELY!!



Passcodes & Passwords: The facial foundation

6

Just as a good facial starts with a clean base, your phone's security begins with solid password protection.

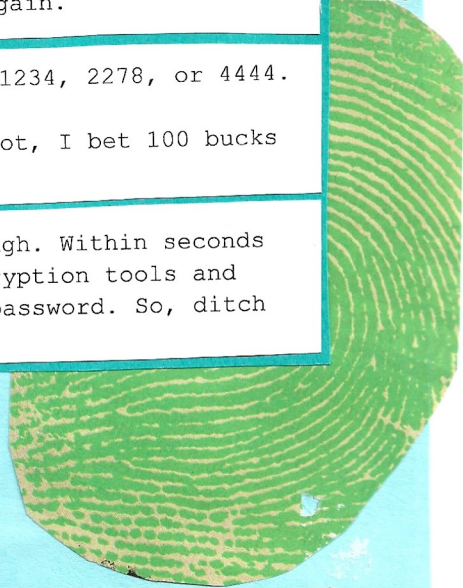
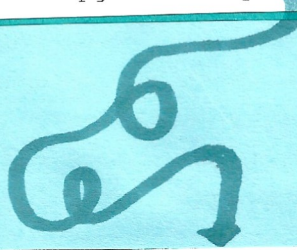
Lock Screen Passcodes

Many of us have lock screen passcodes, and we punch them in a million times a day to stalk our exes on Instagram, text our moms about dinner plans, or get directions from Apple Maps to avoid getting lost...again.

You probably type 3578, 4568, 7777, 1234, 2278, or 4444.

Did I just guess your passcode? If not, I bet 100 bucks I'm getting close.

Let's be real, 4 digits are not enough. Within seconds to minutes, anyone using modern decryption tools and brute force attacks can crack your password. So, ditch the basic code and upgrade today!



Instructions

1. Open Settings and search for "Face ID & Passcode."
2. Scroll down and tap **Set Up Face ID**. Position your face in the camera frame and follow the on-screen instructions.
3. Make sure to enable **Require Attention for Face ID**—this adds an extra layer of security by ensuring you're actively looking at your iPhone when unlocking it.
4. Go back to the **Face ID & Passcode** page, then scroll down to **Change Passcode** and tap it.
5. Enter your old passcode, then tap **Passcode Options**.
6. From the list, choose **Custom Alphanumeric Code** or **Custom Numeric Code** (AVOID the 4-Digit Numeric Code option).

Application Passwords

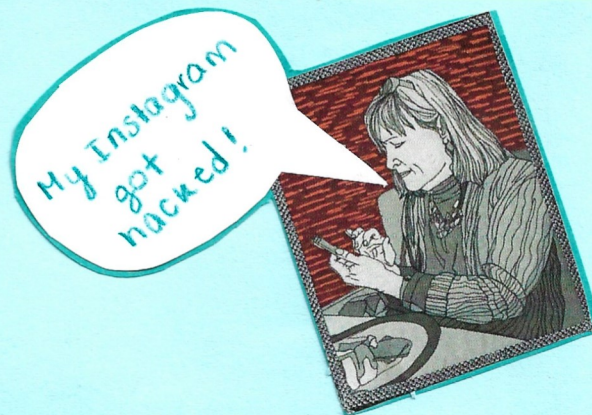
7

Too often, we fall into the trap of using simple passcodes like our childhood pet's name followed by an exclamation mark or numbers.

Milo! or Charliel2 are memoizable but considered unsafe. While these passwords might seem hard to guess, they're far from secure.

And here's the kicker: You never know who's trying to get into your accounts. Your neighbor could be a hacker, or that friendly co-worker could be a private investigator or worse, an undercover cop.

And using a password like "ErikBrown!" because it matches your email (erik.brown@gmail.com) ...still not good enough. You're practically handing hackers and creeps a giant sign that says, "Please, access all my data and spread malware."



Here's the deal: Your password should be at least 12 characters long and include a mix of upper and lowercase letters, numbers, and symbols. Do not include your birthdate, name, or any other identifiable features. The key is randomness or entropy. The more random and meaningless your password is, the harder it is to crack.

To help with memorization, try using:

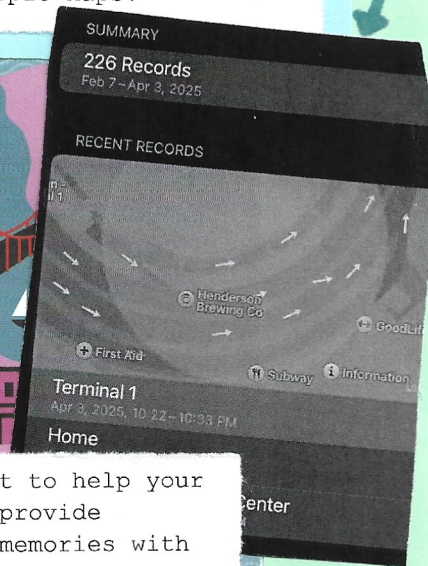
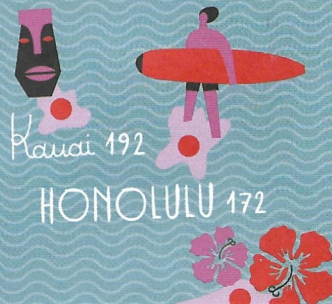
- A lyric from your favorite song or a line from a poem
- A memorable quote from a movie or speech
- An abbreviation of your favorite sentence (e.g., I love Chocolate Chip Ice cream = ILCCIC)

Location Services: The deep pore cleanse

8

ATTENTION!!!

I want you to open your iPhone and go to Settings. Scroll down and tap **Privacy & Security**. Select **Location Services**. Scroll to the bottom of the page and tap System Services. Select **Significant Locations**. You will be asked to enter your iPhone passcode. Once entered, you should see a summary of all the places you've visited. This summary shows how many movement records your device has collected and the time frame. Recent records even display a map of your exact locations even if you didn't use Apple Maps!



Apple explains that this feature is meant to help your iPhone learn more about your travels to provide predictive traffic directions and photo memories with locations⁶.

If this scares you, tap **Clear History** and then disable **Significant Locations** at the top of the page.

186

Malibu 34

Pasadena

HOLLYWOOD 2

CALIFORNIA
you barely know me.

Griffith Park
Observatory

LOS FELIZ BLVD
2
Little
Dom's

Now, moving on to applications. Every time you open an app, you're bombarded with little pop-ups asking for permission to track your location. Most of us mindlessly tap 'Allow' because we're in a hurry to use the app⁸. This is like letting a facialist apply unknown substances to your skin without asking what's in them.

But here's the thing: Apple's pre-installed apps ask for location permission during device setup when you're eager to start using your new iPhone and will blindly agree. I know for myself, I was so excited that I didn't read ANYTHING and accepted EVERYTHING. I don't remember giving my camera, Messages, or the App Store access to my location...but it was on.

Let's check your location settings and make some changes.

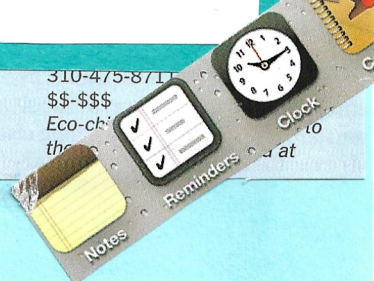
bad things happen.

Fly into
or Long
without
with a GPS.

The Farmer's Daughter Hotel
115 South Fairfax Avenue
323-937-3930

The Avalon Hotel
9400 West Olympic Boulevard
310-277-5221
theavalonbeverlyhills.com
\$\$-\$\$\$

310-475-8711
\$\$-\$\$\$
Eco-chi
the



Instructions

1. Open Settings and tap **Privacy & Security**.
2. Select **Location Services**.
3. Scroll through the apps using your location. Apple's Calendar, Camera, App Store, Find My, Photos, Voice Memos, Weather, and Safari are likely tracking you.
4. Ask yourself: which apps **ACTUALLY** need your location? Hint: Only Weather, Maps, and Find My truly need your location. The rest? They're just nosy!
5. Change location access to "Never" for most apps and set the required apps to "While Using the App".

Add this toner to
your evening skin-
care routine to
promote seriously
smooth skin.

Siri & Dictation: The voice Exfoliation

10

Just as exfoliation removes dead skin cells from your face, controlling your Siri settings removes unwanted voice data collection from your phone.

Think of Siri as that persistent layer of dead skin cells that builds up over time unless you scrub it away every day.

"Hey Siri, what are you doing with my voice recordings?" This is a question most of us never think to ask, but perhaps we should. Siri is always listening, waiting to hear those magic words that activate her.

But what happens to all those recordings of your voice?

For years, Apple contractors manually reviewed Siri recordings to improve the service⁴. Apple contractors reported hearing sensitive information like drug deals, medical conversations, and intimate moments between people⁴. These recordings are from iPhone users accidentally triggering Siri⁴...which seems to happen A LOT.

You should be asking yourself if you need Siri at all. If yes, I encourage you to at least perform a voice exfoliation:

Instructions

6. Open Settings and tap **Privacy & Security**.
7. Scroll down and select **Analytics & Improvements**.
8. Turn off **Improve Siri & Dictation** to prevent Apple from storing and reviewing your audio.
9. Go back to settings and select **Siri and Search**.
10. Choose only one activation method (either **Listen for Hey Siri** OR **Press Side Button for Siri**) to reduce your chances of accidental triggers.
11. Turn off **Allow Siri When Locked**.

Get the hydration your face craves with this skin-loving hyaluronic acid serum. Skin is left with a dewier, brighter appearance and the product's plumping action minimizes the look of fine lines for a smoothing effect.

(listen. listen)

(listen. listen)

(listen. listen)

(one more listen)

Bluetooth: Bringing Cysts to the Surface

11

Have you ever felt a cyst deep under your skin that you couldn't see or pop? Well... that's Bluetooth. Its risks are hidden from view, but deep down it's secretly exposing your data in ways you cannot control (aka you cannot pop it).

Like most, I bet that you probably leave your Bluetooth on all the time.

Why wouldn't you? It's convenient for connecting to your car, headphones, or smartwatch.

But did you know that when your Bluetooth is on, you are exposed to several security threats:

- **BlueJacking:** someone sends you unsolicited messages. It is usually harmless but can be annoying¹⁰.
- **BlueSnarfing:** someone accesses your iPhone through Bluetooth without your permission¹⁰. This allows them to steal personal data, like contacts, messages, calendars, or even files¹⁰. You are more vulnerable to this if you don't have a lock screen passcode or a weak passcode!
- **BluePrinting:** someone gathering information about your iPhone through its Bluetooth address to gain unauthorized access¹⁰.

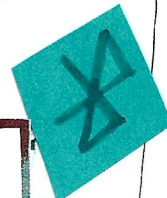
You probably want to turn off your Bluetooth now, am I right? Well here's the kicker: even if you turn off Bluetooth, Apple will turn it back on!

This is due to the Control Center's deception. I can guarantee that we've all swiped down on our iPhone screen to turn off and on Bluetooth or even wifi, data, flashlight, and so forth. However, turning off Bluetooth using this method actually doesn't work at all. When you click Bluetooth off, you're temporarily disconnecting from devices². At 5 AM the next morning, your iPhone will quietly reactivate Bluetooth without your knowledge⁹.

Apple Support
<https://support.apple.com/guide/mac-help/blth1008>

Turn Bluetooth on or off on Mac

You can also turn Bluetooth on or off by clicking the Bluetooth status menu in Control Center and clicking the switch.



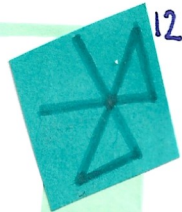
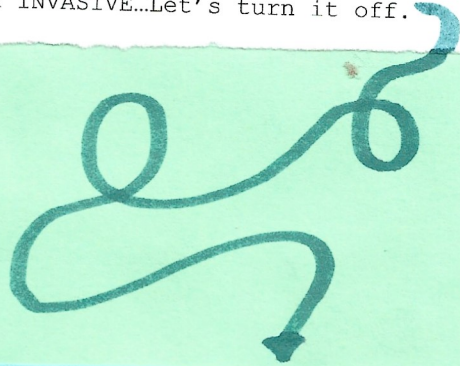
Gift Savings Benefits

So why is Apple so desperate to keep your Bluetooth active? The answer lies in their proprietary tracking system: iBeacon.

These small, invisible transmitters are put everywhere (stores, airports, stadiums, etc.), constantly searching for Bluetooth signals from your iPhone⁵. When your iPhone detects an iBeacon, it notifies apps with location permissions about your precise location regardless of whether these apps are running or not⁵.

Every step you take in an iBeacon-enabled area generates data that helps Apple and other retailers understand you and your purchase behaviour⁵.

SUPER INVASIVE...Let's turn it off.

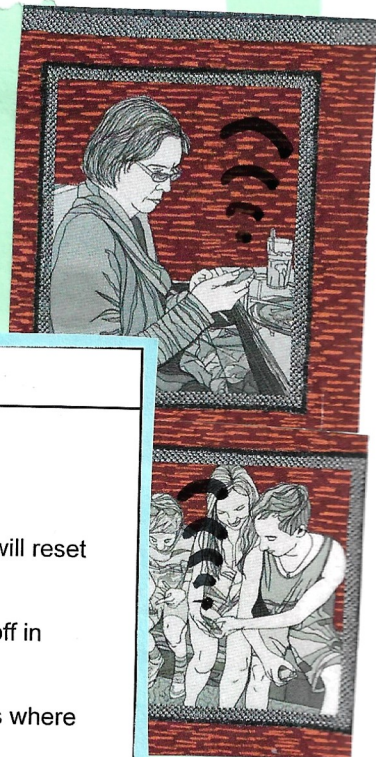


Instructions

12. Open Settings, tap **Bluetooth** and switch it off.

Considerations:

13. Check this setting after every iOS update and this will reset preferences⁵.
14. It is ok to use Bluetooth but make sure to switch it off in settings, not the control center.
15. Consider using Airplane Mode in sensitive locations where you don't want to be tracked.



iCloud: The Moisture Barrier

13

Look up at the clouds. They seem so free, floating in the open sky. But Apple's cloud? Not so much. iCloud may seem airy and harmless, but that lightness masks real risks¹.

After the cleansing and extraction phases of a facial, a good esthetician applies a moisture barrier to protect your freshly treated skin. Similarly, after cleaning up your iPhone's privacy settings, you need to establish proper iCloud settings to create a protective barrier around your data.

When you use iCloud, your photos, messages, notes, contacts, and backups are stored on Apple's servers¹. This is convenient because you can access everything from any device. However, this convenience means losing partial control over your data³. Until recently, Apple held the encryption keys to this data. They could access it at free will and so could anyone with legal authority to make Apple hand it over¹.

In 2023, Apple introduced "Advanced Data Protection" which applies end-to-end encryption to more iCloud data¹. Sounds great, right? But there's a catch:

- **It's opt-in, not automatic:** Apple doesn't alert you to this feature with notifications¹.
- **Not everyone can use it:** Older Apple devices aren't compatible¹.
- **Not all data is protected:** Your contacts, calendar, and iCloud email remain unencrypted¹.

While "Advanced Data Protection" isn't perfect, it still provides significantly more protection than the default settings. Let's turn it on (if your phone is compatible :/).

Instructions

1. Go to Settings and tap your name.
2. Select iCloud.
3. Scroll down and tap **Advanced Data Protection**.
4. Click **Turn On Advanced Data Protection**.
5. Go through the steps. It does take a few minutes so be prepared.

When dry, skin rears its ugly head. At this lotion be you soothing formula r hamide, panthenol ores your skin's mc seven days for a h visage. What's mor e it on your body fc kin-saving benefits

Activity: iCloud Sensitivity Scale

14

Rate how sensitive each type of data is from 1 (share freely) to 5 (ultra private):

- Photos _____
- Notes _____
- Health _____
- Messages _____
- Contacts _____
- Safari _____
- Mail _____
- Calendar _____
- Wallet _____

Now that you've rated your data sensitivity, let's review what's actually in your iCloud.

Instructions

6. Go to Settings and tap your name.
7. Select **iCloud**.
8. Tap **Apps Using iCloud**. Does your iCloud usage match your sensitivity ratings? For any items you rated 4-5, consider turning them off.

Conclusion

Just like regular skin care maintains the health of your complexion, regular privacy check-ups protect your online life from unwanted surveillance and data collection. Take control today by implementing the advice presented in this zine, and make sure to review these settings following each iOS update.

check out these resources !!!

Bolton, T., Dargahi, T., Belguith, S., Al-Rakhami, M. S., & Sodhro, A. H. (2021). On the Security and Privacy Challenges of Virtual Assistants. *Sensors (Basel, Switzerland)*, 21(7), 2312-. <https://doi.org/10.3390/s21072312>

This academic article highlights the growing privacy and security concerns surrounding virtual assistants like Siri.

Klosowski, T. (2020, April 29). 16 Practical Privacy Tips for Your iPhone. *Wirecutter*. <https://www.nytimes.com/wirecutter/guides/iphone-privacy-tips/>

This is a detailed guide on enhancing privacy settings on iPhones.

Ma, Y., Sew, C., Sarsenbayeva, Z., Knibbe, J., & Goncalves, J. (2024). Understanding Users' Perspectives on Location Privacy Management on iPhones. *Proceedings of the ACM on Human-Computer Interaction*, 8(MHCI), 1–25. <https://doi.org/10.1145/3676529>

This is an academic paper that explores how users perceive and manage their location privacy across different apps.

Rose, C. (2012). Ubiquitous smartphones, zero privacy. *The Review of Business Information Systems*, 16(4), 187–191. <https://doi.org/10.19030/rbis.V16i4.7438>

This is an academic paper about smartphone privacy issues. The authors discuss how phone users have zero privacy due to tracking software.

Shilton, K., & Greene, D. (2016). Because privacy: defining and legitimating privacy in ios development. *ICConference 2016 Proceedings*.

This is an academic paper about privacy in iOS development. The authors investigate how iOS developers define and implement privacy features in their applications.

How to cite this zine: Avery, Jessica. (2025). Your iPhone Needs a Facial. Hamilton.

References

1. Bayen, L. (2023, October 27). A critical look at Apple's privacy record. *Tech Policy Press*.
<https://www.techpolicy.press/a-critical-look-at-apples-privacy-record/#>
2. Brandom, R. (2018, February 25). Why does my phone make it so hard to turn off Bluetooth? *The Verge*.
<https://www.theverge.com/2018/2/25/17041440/bluetooth-location-tracking-iphone-android-privacy>
3. De Filippi, P. (2013). *Cloud computing: Analysing the trade-off between user comfort and autonomy*. Internet Policy Review.
<https://policyreview.info/articles/analysis/cloud-computing-analysing-trade-between-user-comfort-and-autonomy>
4. Hern, A. (2019, August 2). Apple halts practice of contractors listening in to users on Siri. *The Guardian*.
<https://www.theguardian.com/technology/2019/aug/02/apple-halts-practice-of-contractors-listening-in-to-users-on-siri>
5. Hill, K. (2014, March 12). *Apple Keeps Turning Bluetooth On When You Update Your iPhone*. *Forbes*.
<https://www.forbes.com/sites/kashmirhili/2014/03/12/apple-keeps-turning-bluetooth-on-when-you-update-your-iphone/>
6. Komando, K. (2020, September 8). Privacy alert: Your iPhone is tracking everywhere you go. Here's how to find the setting. *USA TODAY*.
<https://www.usatoday.com/story/tech/columnist/2020/09/08/iphone-tracking-everywhere-you-go-how-find-setting/5695132002/>
7. O'Flaherty, K. (2024, April 10). *Keeping iPhone Data Hidden From Apple Is 'Virtually Impossible.'* *Forbes*.
<https://www.forbes.com/sites/kateoflahertyuk/2024/04/10/new-apple-iphone-privacy-warning-issued-by-researchers/>
8. Ramokapane, K. M., Mazeli, A. C., & Rashid, A. (2019). Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies*, 2019(2), 209–227. <https://doi.org/10.2478/popets-2019-0027>
9. *Use bluetooth and wi-fi in control center*. (n.d.). Apple Support. Retrieved April 8, 2025, from
<https://support.apple.com/en-us/102412>
10. Vakulov, A. (2025, February 20). 11 types of bluetooth attacks and how to protect your devices. *Forbes*.
<https://www.forbes.com/sites/alexvakulov/2025/02/20/11-types-of-bluetooth-attacks-and-how-to-protect-your-devices/#>
11. Wyatt, S. (2021). Metaphors in critical Internet and digital media studies. *New Media & Society*, 23(2), 406–416.
<https://doi.org/10.1177/1461444820929324>