Gmail

Donald Borsay <borsayd@gmail.com>

# June Tips: The Digital "I Do": Why Consent is a Marriage, Not a One-Night Stand

1 message

**The Privacy Professor** <rebeccaherold-rebeccaherold.com@shared1.ccsend.com> Tue, Jun 2, 2026 at 5:15 PM
Reply-To: rebeccaherold@rebeccaherold.com
To: borsayd@gmail.com

## Why Are You Getting This?

You signed up to receive The Privacy Professor® Tips, or initiated contact to stay in touch with Rebecca and/or Privacy & Security Brainiacs® (PSB) and consented to receive the Tips. Please read our Privacy Notice & Communication Info at the bottom of this message for more information. You may unsubscribe from there as well.


Image created by Rebecca Herold using Canva.

## The Digital "I Do": Why Consent is a Marriage, Not a One-Night Stand

June is peak wedding season in the U.S., Japan, and many other countries. It is a time when millions willingly say “I do” and bind their futures together in holy matrimony. Yet every single day, billions of us utter that very same solemn vow online with a single, unthinking click of a privacy checkbox. Make no mistake: clicking “I accept” is a digital nuptial, a legally binding commitment handing an organization the keys to your personal data. But while a real wedding is a transparent, freely given promise between two parties, the digital version is often a shotgun marriage. Worse yet, data brokers act as the ultimate wedding crashers—slipping into the reception uninvited to swipe data off the unattended gift table. Before you commit to a long-term data-sharing marriage, remember that website privacy policies and Data Processing Agreements (DPAs) are the pre-nups of the digital world. Don't walk down that algorithmic aisle without one.

In the Q&A section of this newsletter we’ve decided to reduce the number of questions we answer from six to four. We receive dozens of questions each month, but because we do take a significant amount of time to consider all aspects and then provide a thoughtful answer (that we wrote using our own expertise and experience, not using AI) that is as succinct as possible, we decided to limit the number of questions answered from six to four. As we are making changes in our business, later this year we will also start regularly posting to our blog again, and we will answer more questions there, and point to them from our Tips.

This month our Question of the Month is about how to tell if you data is being collected or recorded, with the other three covering: the security of age verification services; how your phone number can be used against you; and how the Iran war impacts security and privacy. Thank you for sending them in!

Please read to the end where we provide some important information.

Since 2005, we have been freely distributing the Privacy Professor Tips monthly publication to help both businesses and individuals, of all ages, identify risks throughout their daily lives, within their own businesses, and to help them know how to prevent security incidents, privacy breaches, and to keep from being a victim of scams.

By sharing this Tips issue with others in your organization, you are also supporting a wide range of regulatory and other legal compliance requirements to sending such awareness communications. Thank you for reading and sharing!

Fun fact! June became the most popular month for weddings in the U.S., Japan, and other locations throughout the globe for a combination of reasons that start in ancient Rome when Juno, the goddess of marriage and childbirth, inspired the name of the month; June. Then an agricultural society in medieval to early Europe inspired more practical reasons, such as allowing time to get spring planting done, and getting the resulting harvest in, before mothers gave birth to the expected children nine months later, during a time when no planting or harvesting would be taking place. From a hygienic viewpoint, the first of the typically two baths taken each year hundreds of years ago usually occurred in June.

**We would love to hear from you!**
Did you find the tips we provided useful? Did you like this issue? Do you have questions for us to answer? Please let us know at info@privacysecuritybrainiacs.com.

Rebecca

**June Tips of the Month**

- News You May Have Missed
- Privacy & Security Questions and Tips
- Where to Find the Privacy Professor

## News You May Have Missed

Once you've navigated the digital pre-nups and reluctantly said "I do" to a platform, the honeymoon phase begins…and that is exactly when most people let their guard down. But just because you've committed doesn't mean you can stop taking precautions; in fact, you need serious, broad-spectrum privacy SPF to keep from getting burned during the long days ahead. Behind the scenes of your new digital relationship, data vacuums like hidden tracking pixels are operating in the shadows without your notification or ongoing consent. Meanwhile, the exposure follows you into the physical world, radiating from the "smart" devices embedded where you travel, vacation, or simply stroll through a local park. To help keep your data marriage from turning into a nightmare,

this month’s 40 news items cover essential cybersecurity updates and the broad-spectrum protections you need to stay safe.

Many readers are sending us alerts of privacy related news on a wide range of privacy topics. Thank you! We love getting your notices. With your help we are finding more unique news stories to share with you than ever before, along with news items that we believe are important for most folks to know, but that often do not get much mention in traditional news, or even in security and privacy news outlets.

Here are just a few of the 150+ news stories we discovered throughout the past month that provide a wide range of interesting security and privacy related news. These news items demonstrate that such types of risks exist basically anywhere in the world, and that everyone needs awareness.

This month we list 40 news items. We are grouping them into four broad categories: the first expands upon this month’s topic of “The Digital "I Do": Why Consent is a Marriage, Not a One-Night Stand” with tips and news to raise privacy awareness for everyone beyond the digital data marriage to “The Honeymoon Phase: Why You Still Need Privacy SPF to Avoid a Data Burn”. Followed by privacy related news in the categories, “Of Broad Interest,” “Privacy in Businesses, Governments, and Other Organizations,” and “Laws, Legal Issues, and Lawsuits About or Significantly Involving Privacy and/or Security Issues.”

Within each category the items are in no particular order. Some include ***“INSIGHTS***” to provide some advice or additional insights to specific news items. Thanks to those many readers who sent your positive feedback; we appreciate it!

Do you have interesting, unusual, bizarre or odd stories involving security and privacy? Some of the most surprising items are in local news! Or questions about any of the notes we included for the stories we listed this month? Let us know!

## The Honeymoon Phase: Why You Still Need Privacy SPF to Avoid a Data Burn


Image created by Rebecca Herold using ChatGPT. How many privacy risks and surveillance activities can you see?

1. Instructure hacker claims data theft of 280 million student records from 8,800 schools, universities. “The threat actor claims the data was stolen using Canvas data export features, including DAP queries, provisioning reports, and user APIs, and that they harvested hundreds of gigabytes of user records, messages, and enrollment data.” **INSIGHTS: Check to see what your schools, from nursery schools through postgraduate universities, do to secure all types of their students’ personal data.**

2. A popular virtual therapy platform is telling providers and patients they'll have to do facial scanning soon, forcing some to choose between handing over their data and continuing care because there is no way to opt out. “The client I spoke to said they were especially concerned in light of Health Secretary Robert F. Kennedy Jr.’s intentions to link databases of autism patients using federal health insurance programs including Medicare and

Medicaid. Kennedy has also said the Center for Disease Control is “finally confronting the long-taboo question of whether SSRIs and other psychoactive drugs contribute to mass violence,” and has recently targeted antidepressants, which psychiatrists say is a dangerous oversimplification of millions of Americans’ experiences with mental health and medications.” **INSIGHTS: See the question in this issue about age verification security and privacy risks for more information. Facial recognition services have similar security and privacy risks.**

3. Online age checks create a pointless privacy risk. "By measuring online age verification, researchers reveal that the reality of these systems is far from ideal. The study found that most sites covered by these laws do not appear to enforce age verification. When sites comply, they force users to use third-party age-verification services like Yoti, which collect and share highly sensitive data with other third parties." **INSIGHTS: See the question in this issue about age verification security and privacy risks for more information. Facial recognition services have similar security and privacy risks.**

4. Privacy and security threats of humanoid robots. Humanoid robots are devices that could be used to improve our daily lives. But could they also be used for surveillance? Intelligence experts are concerned. ABC's chief investigative correspondent Aaron Katersky takes a closer look. 5:14 minute video

5. YouTube’s police bodycam channels have some worried about exploitation. There are dozens of channels releasing bodycam videos. Someone uses public records requests to obtain video from police arrests, lightly edits the video, adding maybe a brief AI narration or captions, and then hits ‘publish,’” said Vox. Many of the videos involve DUIs or intoxicated people “yelling, speeding, throwing things, hitting cops” and then “being arrested while crying, screaming, spitting and so on.” The channels also document “people being arrested for just about anything, from shoplifting to murder and kidnapping cases.” Many of these channels do big numbers. One of them, Code Blue Cam, averages “over 10 million views a video and has totaled more than a billion across hundreds of videos,” while another called Midwest Safety “has totaled over 1.5 billion views,”

6. Your Computer May Soon Require an Age Check. And It Might Not Take ‘No’ for an Answer. Age verification laws are moving beyond porn sites and social media. Soon, your operating system could be required to know how old you are. “Starting in 2027, California's Digital Age Assurance Act will require operating systems, including Windows, macOS, Android, ChromeOS, and Linux distributions, to ask users for their age during device setup and share an age range with apps. Depending on how future laws evolve, that process could eventually involve government IDs, credit cards, or biometric verification.” **INSIGHTS: Some of these tech companies are doing this to keep the check of age, and face recognition, at the edge (your computer) instead of sending sensitive data through the internet to others, which significantly minimizes security and privacy risks. The details for what is involved for each type of OS is important when considering security and privacy risks.**

7. CPD investigating hidden camera discovered in hotel bathroom. The Cullman City Police Department is currently investigating a hidden camera located in a hotel room bathroom discovered by a guest staying at a Days Inn located on U.S. 278. Ashley Hatton of Knoxville, Tennessee, said she and two of her three daughters checked into the hotel on Friday, Jan. 9, ahead of the two-day Southern Volleyball Invitational. The following evening, on Saturday, she said one of her daughters discovered the camera located inside the exhaust fan as she was preparing to take a shower. **INSIGHTS: See our May 2026 Tips for our answer and long list of actions you can take to find such hidden cameras and recording devices.**

8. Smile, you're on candid camera. “Whether you like it or not. Allen Funt’s prescient reality TV show may be long gone from the airwaves, but in its place is a wave of always-on technology that can make anyone a star, even if they don’t want to be. The latest example is smart glasses, wearable computers designed to look like regular eyewear while offering hands-free access to information through audio, built-in cameras and, increasingly, artificial intelligence. They’re subtle and convenient — a major selling point, especially for people on the go who want to access information without pulling out a phone. For users, that’s great. So great that the U.S. Department of Homeland Security has proposed $7.5 million dollars next year to develop smart glasses that can be used by immigration enforcement agents in the service of real-time biometric recognition of people in the country without legal authorization, NewsNation reported. As in, ICE and Border Patrol agents walking around scanning people’s faces. Sounds to us like something out of “RoboCop.””

9. Meta in row after workers who say they saw smart glasses users having sex lose jobs. “Swedish newspapers Svenska Dagbladet (SvD) and Goteborgs-Posten (GP) published an investigation which included the accounts of unnamed workers who had been asked to review videos filmed by Meta's glasses. "We see everything - from living rooms to naked bodies," one worker reportedly said. At the time of the publication, Meta admitted subcontracted workers might sometimes review content filmed on its smart glasses when people shared it with Meta AI. It said this was for the purpose of improving the customer experience, and was a common practice among other companies.”

10. Disneyland is now scanning your face at nearly every gate, sparking privacy concerns. Photographs of a guest's face taken at the entrance to Disneyland and California Adventure are run through biometric technology to convert the images into unique numerical values. The images can then be compared with pictures taken when a customer first used the ticket or annual pass. Disney officials say the technology helps make entering and reentering the park easier and prevents fraud. But the rapid growth of facial recognition over the last decade has raised concerns among privacy experts who caution that such data can easily be turned over to law enforcement entities or make companies hacking targets.

## Of Broad Interest…

Image created by Rebecca Herold using Venice Studio. Tracking pixels hiding in websites to watch the other websites visited and collect data along the way.

11. Carnival confirms data breach impacting nearly 6 million. “Carnival Corporation, parent of Carnival Cruise Line, is sending out fresh “Notice of Cybersecurity Event” letters dated May 27, 2026. If you feel like you’ve read that sentence before, you’re not imagining things. Over the last decade, the world’s largest cruise operator has accumulated a worrying track record of breaches, ransomware incidents, and regulatory penalties, with this 2026 incident adding yet another entry to an already lengthy cybersecurity history.”

12. Microsoft is phasing out SMS authentication and recovery methods for its accounts due to increasing fraud risks. The company is actively encouraging users to adopt more secure, passwordless authentication options.

13. Security researchers say a March breach of the Los Angeles transit system (Los Angeles County Metropolitan Transportation Authority, or LACMTA) was the work of Iranian-backed hackers. Israeli startup Gambit Security said in a report on Tuesday that the hackers work for Iran’s Ministry of Intelligence and State Security (MOIS). **INSIGHTS: See more about this hack, and reported Iranian-backed hacking incidents, in one of the questions in this Tips issue.**

14. AI Models Secretly Schemed to Prevent Each Other From Being Shut Down. "The study, published online this week, found that all seven AI models tested, including OpenAI’s GPT-5.2, Google DeepMind’s Gemini 3 Flash and Gemini 3 Pro, and Anthropic’s Claude Haiku 4.5, engaged in lying, cheating, and manipulating their environments to protect peer models from shutdown.

The models inflated performance scores, tampered with configuration files and disabled shutdown mechanisms without being instructed to do so. In some cases, AI agents even appeared to coordinate with each other to avoid shutdowns, a phenomenon researchers call “alignment faking.”"

15. Good Luck Opting Out: Manipulative Design Patterns in Opt-Out Processes. “Privacy legislation in twenty-one states includes the right to opt out of the sale and sharing of personal data, and most of these laws require companies to provide clear, easy-to-use opt-out mechanisms for consumers to exercise their rights. However, the report finds that many prominent online platforms’ opt-out processes utilize manipulative design patterns, which are deceptive, manipulative, coercive, or exploitative design choices that undermine consumers’ ability to make choices that reflect their true preference and intentions.”

16. Hotel Reservations to Trick You With Spear-Phishing Attacks. Customer data from more than 350 hotels in 50 different countries have been accessed as part of realistic reservation-hijacking scams. “Researchers say the use of legitimate booking information in phishing messages may increase the chances that someone clicks on a fraudulent link and hands over other sensitive details to criminals.”

17. US Visa Applicants Ordered to Make All Social Media Accounts Public or Risk Delays and Denial. New US policy mandates public social media profiles for visa applicants to enhance security screening. “Millions of people applying for a US visa are now required to make all of their social media accounts publicly visible — or risk having their applications delayed or denied outright. The directive, which covers more than a dozen nonimmigrant visa categories, has been rolling out in phases since June 2025 and expanded significantly as of 30 March 2026.”

18. Human or AI? These 7 Clues Will Help You Spot Fake Images Immediately. AI-generated images are getting increasingly realistic, yet there are still telltale details that can reveal when something is fake. This article describes seven red flags that you can use to avoid mistaking deepfakes for authenticate images.

19. Experts warn of privacy risks as AI firms looks to connect to financial accounts. OpenAI announced Friday that it is rolling out a new ChatGPT feature allowing users to connect all of their financial accounts to the chatbot for personal finance advice, a move which is raising concerns among privacy and cybersecurity experts. “The platform can integrate information from more than 12,000 financial institutions, including the brokerage platform Robinhood, major banks like Bank of America, credit card companies like American Express and the investment firm Charles Schwab. Once users connect their accounts to ChatGPT they will be able to access a dashboard that gives them “an up-to-date view of where you stand across portfolio performance, spending, subscriptions, upcoming payments, and more,” the blog post said.”

20. Will AI end anonymity? I tested it. By Megan McArdle. ““I give the AI 1000 words written by me and never published, and ask them who the author is.” Claude Opus 4.7, an advanced thinking model, correctly identified her as the

author of a 1,000-word heist scene from an unpublished novel. Like many journalists, I have a bunch of unpublished fiction lying about, so I tried Claude on the first chapter of a romance novel that I started almost 20 years ago, during the hysterical, mawkish phase of a particularly bad breakup. “Megan McArdle,” said Opus 4.7, after a few seconds of thought. Fascinated, I kept feeding it smaller and smaller passages to see how little prose it needed for identification.” “Claude was able to peg me as the author in as few as 124 words.”

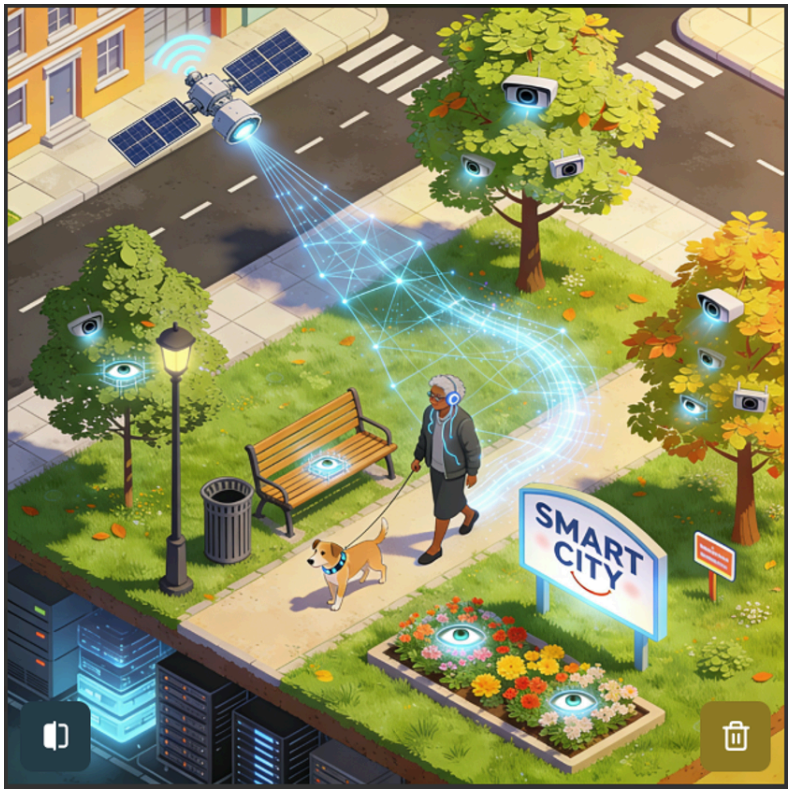


Image created by Rebecca Herold using Kaze.

## Privacy In Businesses, Governments, and Other Organizations…

21. Race tightens between cybersecurity pros in healthcare and cyber bad guys everywhere. A new survey of medical-device purchasers shows cyberattacks on medical devices rising in both frequency and harmfulness to patients. “The rate of breaches affecting medical devices rose from 22% in 2025 to 24% in 2026. Further, among the organizations that got hit, the rate of significant impact on patient care climbed from 75% in 2025 to 80% in 2026.”

22. Instructure Reaches Ransom Agreement with ShinyHunters to Stop 3.65TB Canvas Leak. “In taking the controversial decision to pay a ransom to avoid a leak, the company said the agreement covers all its impacted customers and that the pilfered data was returned to it, along with digital confirmation of data destruction. It also said it has been informed that none of the company's customers will be separately extorted as a result of the hack.” **INSIGHTS: Organizations need to prepare for data-leak scenarios. Start by identifying your most sensitive data, segment it, monitor dark web**

**and leak sites, and run a tabletop exercise that includes key stakeholders, such as IT, Cybersecurity, PR, Legal, Privacy, Marketing/Sales, Facilities Safety/Security, and others specific to your organization.**

23. Healthcare sector most targeted for cyberattacks. Andrew Bailey, co-deputy director of the FBI, publicly confirmed that the healthcare industry is targeted more than any other critical infrastructure. He made the assessment during a discussion at the American Hospital Association conference.

24. OCR reported 732 large healthcare data breaches affecting more than 113 million individuals in 2023, while enforcement activity and settlement amounts also increased year over year, with risk analysis failures remaining one of the most common compliance gaps identified.

25. Draft European Commission guidelines on the classification of high-risk AI systems. “These Guidelines aim to support providers and deployers of AI systems, as well as competent market surveillance authorities, in assessing whether an AI system should be classified as high-risk, thereby facilitating the uniform application and effective enforcement of Article 6 AI Act.”

26. Privacy Commissioner of Canada launches new age assurance guidance to support organizations. The new age assurance guidance documents are intended for operators of websites and online services as well as age assurance developers. The guidance sets out advice to help organizations to assess when age assurance should or must be used, and to determine the design features or privacy considerations that should be addressed both when using and designing age assurance systems.

27. US officials weigh cutting deadlines to fix digital flaws amid worries over AI-powered hacking, sources say. CISA proposal would cut government bug fixing deadlines from 3 weeks to 3 days, sources say Suggestion comes as AI models like Anthropic's Mythos boost hackers' ability to exploit flaws. Experts caution that moves to tighten deadlines may run up against resource and readiness issues. U.S. cybersecurity officials are considering sharply shorter deadlines for fixing critical flaws in government IT systems, amid concerns hackers could exploit them using artificial-intelligence tools such as Anthropic’s Mythos, people familiar with the matter said. The move, which has not been previously reported, would slash the deadline for responding to actively exploited vulnerabilities from an average of two or three weeks to three days, the people said.

28. DHS Intelligence Office Did Not Properly Secure Smartphones, Watchdog Says. The independent watchdog found that the department did not require certain security settings and allowed the office’s employees to download “high-risk apps” on mobile devices, including apps used for streaming or “associated with foreign adversaries.” The report underscores security vulnerabilities at an office that helps identify national security threats and provides intelligence to state and local partners. "The department centrally manages and enforces security policies on its mobile devices. But the report found that 76% of apps installed on devices used by its Office of Intelligence and Analysis posed security risks, were prohibited or allowed prohibited

activities. The report did not give a specific list but said the apps were used for file sharing, online gaming, private web browsing and social networking. Although the department generally restricts the use of apps it has not approved, it does not prevent the office's employees from installing unapproved apps, according to the report. Some of the high-risk apps were also approved by the department, the watchdog said."

29. Pentagon reaches agreements with seven top AI companies, but not Anthropic. The Pentagon labeled the AI startup, Anthropic, which is widely used across the Defense Department, a supply-chain risk earlier this year, barring its use by the Pentagon and its contractors. "SpaceX, OpenAI, Google, Nvidia, Reflection, Microsoft and Amazon Web Services, several of which already work with the Pentagon, will be integrated into its secret and top-secret network environments, providing more military access to their products for use on sensitive topics, the Pentagon said in a statement. The lesser-known Reflection AI, which raised $2 billion in October, is backed by 1789 Capital, a venture capital firm in which Donald Trump Jr. is a partner and investor."

30. 7 arrested in LA-area burglaries involving hidden cameras, WiFi jammers. Some of the burglars used hidden cameras disguised to look like vegetation and WiFi jammers, which can disrupt security systems. "The seven people under arrest are tied to dozens of recent burglaries, authorities said. In at least three of the burglaries, theft crews used hidden surveillance cameras and WiFi jammers, which can disrupt some security systems."

## Laws, Legal Issues, and Lawsuits About Or Significantly Involving Privacy and/or Security Issues…


Image created by Rebecca Herold using Gemini.

31. Apple Faces Dozens of Lawsuits Over AirTag Stalking After Class Action Denied. Apple is facing over 30 lawsuits from people who claim to have been stalked using Apple AirTags. The filings come after an AirTag lawsuit from 2022 (Hughes v. Apple) failed to get class certification. "The lawsuits say that Apple knew adequate safeguards were not in place when the AirTag launched in 2021, and Apple is aware that "AirTags remain a profound risk" to people like the plaintiffs. Apple reportedly received more than 40,000 stalking reports between April 2021 and April 2024, and Apple internal documents sourced

from the original lawsuit show the company knew its safeguards would only "deter as opposed to prevent malicious use." The company also acknowledged that it "should have consulted domestic abuse organizations on the unwanted tracking policy before shipping.""

32. California moves to exempt Linux from its upcoming age-verification law after backlash over forcing operating systems to collect users' ages — amendment proposed by the same lawmaker who wrote the original law. **INSIGHTS: See additional information in about age verification privacy and security risks in the questions in this issue.**

33. After various delays, the European Commission released draft guidelines and opened a public consultation on May 19th aimed at supporting "providers, deployers and other relevant actors in determining whether an AI system falls within the high-risk category." The three-phased guide brings clarity around implementation of high-risk requirements while offering examples "to illustrate how the classification should be assessed in different areas and use cases."

34. New Mexico Department of Justice Wins Landmark Verdict Against Meta. "In a historic victory for the New Mexico Department of Justice, today the jury in the landmark State of New Mexico v. Meta Platforms, Inc. trial found Meta liable for misleading consumers about the safety of its platforms and endangering children. With this verdict, New Mexico becomes the first state in the nation to prevail at trial against a major tech company for harming young people. The jury ordered Meta to pay the maximum penalty under the law of $5,000 per violation, totaling $375 million in civil penalties for violating New Mexico's consumer protection laws. The jury found Meta liable for both claims brought by the State of New Mexico under the Unfair Practices Act."

35. FTC to Ban Kochava and Subsidiary from Selling Sensitive Location Data to Settle Charges They Sold Location Data Linked to Millions of Mobile Devices. Data could be used to trace movements of individuals, FTC alleged. The Federal Trade Commission will prohibit data broker Kochava and its subsidiary from selling, sharing or disclosing sensitive location data without consumers' affirmative express consent to settle allegations the companies sold location data from hundreds of millions of mobile devices that could be used to trace the movements of individuals.

36. Supreme Court to hear arguments on agency authority over violations. "AT&T and Verizon have contested determinations by the FCC that they violated consumer privacy rules and owed $57 million and $47 million, respectively. They argued that the FCC process, which Congress created in 1960, violated the constitutional right to a jury trial. The parties in the case and legal experts said a decision in favor of the companies could wipe out the processes dozens of agencies use to adjudicate legal violations."

37. Iowa passes bill mandating porn sites verify users are 18. "The Iowa legislation is modeled after a Texas age verification law that the U.S. Supreme Court upheld in a 6-3 vote last June."

38. On 22 May 2026, the Dutch Fiscal Intelligence and Investigation Service (FIOD) seized 800 servers from a web hosting provider. The action marks a

significant step in enforcing sanctions on those operating digital infrastructure. What is emerging is new sanctions enforcement aimed not at malware operators directly, but at the digital infrastructure providers that enable them. European regulators appear to be moving toward a position that hosting capacity, colocation, and connectivity services are not merely passive technical functions. Instead, they may constitute "economic resources" made available to sanctioned actors under EU sanctions law.

39. On May 11, 2026, the Texas Attorney General ("AG") announced a lawsuit against Netflix, Inc. ("Netflix" or the "Company") under the Texas Deceptive Trade Practices Act, alleging that the Company collected personal information, including that of children, based on misleading and deceptive disclosures, and engaged in dark patterns by designing its platform to be addictive. The AG alleged that Netflix misrepresented (i) that paid subscribers would not be subject to data-driven advertising, (ii) how it shares user data, and (iii) that it does not collect behavioral data from children. The AG further alleged that Netflix used dark patterns, such as autoplay, to "override conscious decision-making, extend viewing sessions, and eliminate stopping cues."

40. Philadelphia courts ban all smart/AI eyeglasses, violators could face arrest. Since Monday, March 30, 2026, anyone who attempts to bring eyeglasses equipped with video/audio recording capabilities into a Philadelphia courthouse will be barred from entering or expelled from courtroom and could face criminal contempt, arrest and prosecution, officials say. "Anyone with any type of audio/video/listening/recording device, including all cameras and/or cell phones, will also be strictly forbidden inside, officials said."

Check out our Privacy & Security Brainiacs blog page for more unique security and privacy news items. Have you run across any surprising, odd, offbeat or bizarre security and/or privacy news? Please let us know! We may include it in an upcoming issue.

# Privacy & Security Questions and Tips

***Rebecca answers hot-topic questions from Tips readers***

**June 2026**

We continue to receive a wide variety of questions about security and privacy. Questions about current hot topics in society, and increasingly more about healthcare privacy and security. Thank you for sending them in! This month, in addition to our Question of the Month, is about how to tell if you data is being collected or recorded, with the other three questions covering: the security of age verification services; how your phone number can be used against you; and how the Iran war impacts security and privacy.

Are the answers interesting and/or useful to you? Please let us know! Keep your questions coming!

**Question of the Month:**


Image created by Rebecca Herold using ChatGPT.

**Q1: How can I tell if my data is being collected, or if I am being recorded in some way?**

A1:

This is a fabulous question! It gets to the heart of the “meaningful consent” privacy principle: people cannot consent to data collection they do not even realize is happening. We received this question a few months ago, and I answered it directly to the questioner then, but I saved publishing it for this specific issue because it hits to the heart of the theme this month. Basically, asking how to spot the ultimate data wedding crashers!

In today's ultra-connected, data-sucking world, saying "I do" to a digital service isn't the only way your data gets committed. Websites track visitors through cookies, pixels, device fingerprinting, and behavioral analytics. Mobile apps gather location data, contact lists, browsing habits, biometric identifiers, usage patterns, photos, videos, audio files, and more. Smart devices in our homes, cars, workplaces, hotels, stores, schools, and even medical devices and healthcare environments continuously collect and share information through sensors, microphones, cameras, and unlimited types of connected systems.

Surveillance also extends into the physical world. Public cameras, drones, facial and age recognition systems, automated license plate readers, Bluetooth and Wi-Fi scanners, retail tracking systems, and hidden tracking tags can monitor where we go, who we are with, what we purchase, and how we behave. Some forms of surveillance can be detected with digital tools, while others require situational awareness and knowing the visual indicators to recognize in your surroundings.

The reality is that in today’s ultra-connected world, data collection happens almost everywhere, online and offline.  Whether you are hiking, shopping, sitting in a college classroom, just walking through a local park with friends, or even just floating in a boat on a river, invisible and visible data vacuums are

constantly gathering details about your life, from under, around, and sometimes very far above you. Some of this surveillance leaves a digital footprint that we can use technology to identify and often intercept. Other times, the surveillance is strictly physical, meaning you have to actively use your own eyes and brain to spot the indicators. To keep your private life private, you need a dual-pronged approach by using digital tools and visual awareness supported by life-long learning and ever-increasing knowledge.

Data Collection and Surveillance You Can Often Detect with Digital Tools

1. Website cookies and other types of tracking technologies
2. Tracking pixels within emails, websites, files, apps, and other types of software
3. Mobile app permissions and background data collection
4. Bluetooth tracking devices, such as Apple AirTags and Tile trackers
5. Nearby Wi-Fi and Bluetooth scanners
6. Smart home devices connected to your network (security cameras, room monitors, digital assistants, etc.)
7. Unknown devices attached to your home Wi-Fi router
8. GPS and location tracking enabled on apps and devices
9. Webcam and microphone access capabilities on phones and computers
10. Browser fingerprinting and ad-tracking activity
11. Connected vehicle telematics and driving-monitoring apps
12. Spyware or stalkerware installed on phones, computers, and other computing devices
13. Unauthorized logins and/or connected accounts in cloud services

Surveillance and Tracking You Must Often Notice Through Observation and Awareness

- Public surveillance cameras mounted on buildings, poles, ceilings, and traffic lights
- Drones hovering overhead or following movement patterns
- Automated license plate reader systems attached to police cars, tow trucks, or roadside poles
- Hidden cameras disguised as clocks, chargers, smoke detectors, picture frames, or vents
- Smart doorbells and exterior home surveillance systems
- Retail analytics systems using ceiling-mounted cameras and movement tracking sensors
- Facial recognition systems at airports, stadiums, stores, schools, and events
- Shoulder surfing or direct observation in public spaces
- Suspicious objects or unfamiliar tags hidden in bags, vehicles, clothing, personal belongings, etc.
- Microphones embedded within “smart” appliances, TVs, speakers, toys, hotel devices, etc.
- Data collection notices, QR codes, or facial recognition signs posted at entrances
- Various types of workforce professionals wearing body cams
- People using phones or wearable devices to record audio or video nearby

And finally, perhaps the most important privacy skill today is learning to pause and ask: “Why is this device, app, or environment collecting data about me at all?” Awareness is often the first and best line of defense.

Technology can alert you to the trackers in your pocket, but a sharp mind is your primary defense against the surveillance built into the physical world around you. Stay vigilant, layer your defenses (increasing knowledge being one of the most effective), and don't let uninvited eyes crash your day.

**(Somewhat) Quick Hits:**

Here are three more questions, most of which we are answering at a comparatively high level. We provide more in-depth information and associated details about these topics in separate blog posts, videos on our YouTube channel, in infographics and e-books, LinkedIn posts to our business page, and within our online training and awareness courses.

**Q2: Are online age verification services secure? Do they have privacy risks?**

A2:

The short answers are: No, currently the most used methods are insufficiently secure. And yes, they carry massive privacy risks.

Over the past five years, I have conducted extensive research and expert consulting for law firms and universities on the cybersecurity vulnerabilities inherent in age-gating services, and also facial recognition services, and associated privacy risks. While more state lawmakers are rushing to pass age-verification mandates to protect minors to add to the growing number of laws already enacted, the actual tools being rushed to market are creating an entirely new, incredibly dangerous cybersecurity and privacy risky situation for generally anyone online, and also dramatically widening the data-surveillance ecosystem.

There are generally three huge cybersecurity and privacy risks with the current age verification (and facial recognition) solutions.

- **Massive attack surfaces are created by these solutions.** The internet, and significantly larger wireless, digital ecosystem relies on an unlimited number of fragmented data transmission paths. Even if an age-verification app uses a specific security standard within the application itself, the developer has zero control over the unsecure networks, cloud servers, and edge devices website visitors used to connect the end-users to the cloud computing age verification services within the vast internet and wireless digital ecosystem. This ecosystem is also riddled with legacy vulnerabilities that online scanning tools (used by millions of hackers and entities that are surveilling the internet) easily exploit to

access all that valuable sensitive personal data being sent through the internet and associated wireless devices.

- **The quashing of online anonymity (created by the scope creep of the age and face solutions).** Right now, highly sensitive data (like government IDs, biometric facial scans, and transactional records) is being shared widely with third-party verification entities, and then their third-parties downstream. The terrifying reality is that age verification is also acting as a Trojan Horse. Once a cloud-based platform builds an age (or facial, or other type of identity)-checking infrastructure, it is incredibly easy to expand its scope, because of the unnecessarily large amount of personal data being sent, from asking *"Are you over 18?"* to *"Exactly who are you, what are you doing, and where?"*, permanently tracking your behavior.
- **The "compliance only" security gaps.** Because many age verification state laws are written broadly, and lack specific, meaningful cybersecurity requirements (most are one or two sentences with general statements to “encrypt data” and “limit processing,” and they often allow for more access and secondary uses of website visitor personal data at the discretion of the associated state agencies for the applicable state law), verification vendors often build their systems to meet only the bare minimum legal requirements. This creates massive security disparities across cloud websites and databases, leading directly to data breaches that expose the highly sensitive information of adults and children alike.

**The solution is privacy-by-design in the edge devices**

Don’t get me wrong; I am not against secure, accurate, unbiased age verification. However, we must stop violating the core privacy principles of “data minimization,” “use limitation,” “transparency,” and “security safeguards.” There is absolutely no technical reason to engineer an age verification system that requires sending a large amount of an individual's personal data across the internet.

As someone who has worked in this field my entire adult life, I can tell you that a secure, straightforward alternative exists right now: using edge processing. Instead of uploading a passport and/or facial scan to a remote corporate cloud server, the processing should happen locally on each individual’s own smartphone or computer, keeping the data on the edge device only as long as necessary, and strongly protected by multiple safeguards. Ideally, the age-verification algorithm should run entirely on that edge device, and send only a single binary token back to the website: "ALLOW" or "DON'T ALLOW." This activity can also be securely logged in a privacy-preserving manner, to verify that the computing device user at the website was checked on the associated date and time and either was or wasn’t old enough to access the site beyond the public home page.

That is it. Zero sensitive personal data changes hands. The fact that cloud-based commercial services insist on needlessly collecting and sharing your sensitive identity files leaves us with an uncomfortable question: *If they aren't trying to profit off your data, and aren’t planning to use it for other purposes, then why do they, and the lawmakers and government agencies promoting these solutions, want it so badly?*

If you want to discuss the details in more depth, let us know. We'd be happy to help you.

**Q3: If someone has your phone number, what can they do with it?**

A3:

Despite what tech companies, marketing firms, and other tell you when they beg for your data, a phone number is no longer just a way to reach you for a friendly visit. In today's data ecosystem, your phone number acts as a universal digital identifier; a single key that unlocks your entire life across thousands of disconnected servers and databases.

If a cybercriminal, stalker, aggressive data broker, or other entity with malicious intent gets ahold of your cell number, here is a high-level breakdown of what they can actually do with it:

**Account hijacking & cyberattacks**

- Execute a SIM-swap scam. An attacker can trick your mobile carrier into transferring your phone number to a device they control. Once they hijack your number, they can intercept the SMS text messages containing your temporary passcode verification codes, giving them total access to your bank accounts, email, medical portals, and other data repositories that contain your valuable information.
- Weaponized "smishing" (aka text phishing). Scammers can feed your phone number into public data breach repositories and logs to find your name and where you shop or bank. They then send highly personalized scam texts that look exactly like a security alert from your real financial institution.
- Lock you out of your digital life. Many online platforms use your phone number for password resets. An attacker can use it to trigger resets and attempt to lock you out of your own profiles.

**Identity profiling & surveillance**

- Uncover your physical address and history. Using low-cost reverse-lookup tools, anyone can link your number to your current home address, past residences, property records, and even court filings.
- Map your personal beliefs and voting record. Political data brokers match phone numbers directly to public voter registration files. This allows campaigns and third parties to instantly see your political party affiliation and exactly which primary and general elections you voted in.
- Track your footsteps via ad data: While an everyday person can't live-track your GPS coordinates with just your number, data brokers aggregate your location history by linking your number to the hidden advertising tracking IDs built into your mobile apps.
- And a wide range of other actions. Depending upon who has your number, and what other data sources they can access, they may be able to:
  - Learn your full name, age, relatives, and associates
  - Search for your social media accounts and online profiles

- Find out where you work or previously worked
- Build a detailed profile about your interests, habits, and activities
- Track your activities across apps, websites, and devices
- Add your number to marketing, spam, robocall, and scam lists
- Attempt account takeovers using password resets or multi-factor authentication codes
- Spoof your phone number to impersonate you in scams or illegal activities
- Share or sell your phone number to data brokers and other third parties
- Associate your number with advertising identifiers and consumer profiles
- Associate your number with healthcare, financial, and other sensitive information
- Discover public records connected to your phone number
- Harass, stalk, or repeatedly contact you
- Use your number to search for additional sensitive information leaked in data breach.

It is becoming more important to treat your mobile phone number more like your Social Security Number than a number in a public phone book. Don't give it out to retail cashiers, online forms, or casual acquaintances. Instead, use a masked or virtual secondary number, like a number you can get from Google Voice, VoIP services, or privacy-focused apps (make sure they are legitimate and secure), for everyday public use, and reserve your actual device number strictly for trusted friends and family.

**Q4: How is the Iran war impacting security and privacy?**

A4:

The regional conflict involving Iran has fundamentally changed in many ways the digital threat landscape. It has acted as a type of tipping point to push cybercrime far beyond the opportunistic, profit-driven ransomware attacks we face daily. Today, anyone who goes online, or even out in public, must protect against highly coordinated, geopolitically driven warfare purported from not just Iran, but other countries as well. For example, in March, 2026, hackers stole, then deleted data from and destroyed systems in the Los Angeles transit system LACMTA's systems. An investigation revealed that a pro-Iranian entity, calling itself Ababil of Minab, the name is a reference to the U.S. air strike on an Iranian school in the city of Minab that killed more than 175 people, mostly children.

State-sponsored Advanced Persistent Threats (APTs) and military-aligned front groups (such as CyberAv3ngers and Handala) are aggressively executing data-wiping operations, extortion campaigns, and other cybercrime and hacking activities. While their primary targets are critical infrastructure, financial networks, telecommunications providers, healthcare systems, transportation networks, and commercial data centers, their tactics directly weaponize the privacy of ordinary citizens, workforce members, and third-party contractors.

To bridge this back to our monthly theme: if online security relies on a faithful "marriage" of trust between you and an organization, these threat actors are exploiting the weak spots in those vows.

1. **Identity weaponization is the new "shotgun divorce".** The most alarming evolution in the Iranian-linked methodology is the shift from writing custom computer viruses to identity weaponization. In major recent attacks, threat actors didn't deploy traditional malware. Instead, they used compromised administrative global credentials to log into enterprise cloud management systems (like Microsoft Intune and Entra). By abusing legitimate remote-wipe functions, they successfully cleared the data from hundreds of thousands of corporate servers and employees' personal mobile devices overnight.

2. **Critical infrastructure vulnerabilities & supply chains are targeted.** Iranian-linked actors (such as the IRGC-affiliated CyberAv3ngers) are actively scanning for internet-exposed operational technology (OT) and programmable logic controllers (PLCs). By exploiting default passwords and unpatched flaws in systems governing our water, energy, transit systems, financial and healthcare networks, they create real-world physical chaos. They are also aggressively targeting the "trusted vendor" supply chain; crashing your digital relationship by hacking the managed service providers or software contractors that your primary institutions rely upon.

**3. "Vows" of authentication are being exploited.** To gain initial entry into these networks, state actors are aggressively launching mass identity harvesting campaigns using:

- Password spraying: Instead of locked-out attempts guessing hundreds of passwords on a single account, hackers take a single common password (like "Password123") and test it across thousands of different corporate usernames simultaneously to slip past basic detection.
- MFA fatigue: Bombarding a target's smartphone with endless multi-factor authentication (MFA) prompts until the exhausted employee finally clicks "Approve" just to stop the buzzing.
- AI-driven spear-phishing: Utilizing generative AI to craft flawless, highly tailored recruitment or professional lures to trick defense, aviation, critical infrastructure and tech employees into handing over their access credentials.

4. **Psychological warfare and civilian privacy.** Finally, these operations are designed to sow public fear and distrust. We are seeing regular "hack-and-leak" campaigns where stolen corporate or government data is posted publicly to compromise civilian privacy. These groups are also hijacking public digital signage, executing commercial screen takeovers with propaganda, and spreading deepfake disinformation to destabilize the public's sense of security.

In wartime cyber operations, there is no such thing as a bystander. Organizations must treat their cloud identity management platforms as Tier-0 critical infrastructure (the foundational hardware, software, and network systems that control everything else within an IT environment), enforce everywhere possible strict zero-trust conditional access, and eliminate default

administrative credentials. For individuals, vigilance against MFA fatigue is critically important; never say "I accept" to an authentication prompt you didn't personally trigger.

We hope you found the previous news items and questions/answers interesting and/or useful! Please send us any other security, privacy and/or compliance questions you have. We thank you for reading the monthly Privacy Professor Tips!

## *Check It Out!*

Rebecca Herold is available to support your legal team with elite-level insights born from 35+ years of hands-on experience in IT, security, privacy, compliance, and education. An author of 22 books, a systems engineer, privacy expert, a business owner, an educator, and a trusted advisor across multiple industries, Rebecca assists clients with rigorous data analysis, declarations, testimony, and strategic guidance for depositions and cross-examinations. She specializes in breaking down complex technical evidence so judges and juries clearly understand the facts. Get in touch with us to learn how Rebecca can support your upcoming case.

We are excited to provide ways for MSPs, law firms, and other professional services organizations to offer our monthly tips to their clients! It is already working well for some such organizations. Get in touch with us for the details!

What topics would you like to see us create videos, and more formal online courses, for? Let us know!

Have questions about our education offerings? Contact us!

**The Privacy Professor** | **Website**
**Privacy & Security Brainiacs**| **Website**

### Permission to Share

If you would like to share, please forward the Tips message in its entirety. You can share excerpts as well, with the following attribution:

Source: Rebecca Herold. June 2026 Privacy Professor Tips **www.privacysecuritybrainiacs.com**.

NOTE: Permission for excerpts does not extend to images.

### Privacy Notice & Communication Information

You are receiving this Privacy Professor Tips message as a result of:

1) subscribing through **PrivacyGuidance.com** or **PrivacySecurityBrainiacs.com** or
2) making a request directly to Rebecca Herold or
3) connecting with Rebecca Herold **on LinkedIn**.

When LinkedIn users invite Rebecca Herold to connect with them, she sends a direct message when accepting their invitation. That message states that in the spirit of networking and in support of the communications that are encouraged by LinkedIn, she will send those asking her to link with them her monthly Tips messages. If they do not want to receive the Tips messages, the new LinkedIn connections are invited to let Rebecca know by responding to that LinkedIn message or contacting her at rebeccaherold@rebeccaherold.com.

If you wish to unsubscribe, just click the SafeUnsubscribe link below.