SecurityAwarenessNews

the security awareness newsletter for security aware people

The Privacy Issue

Erasing Your Digital Footprint

Compliance Regulations That Are Changing the World

How COVID-19 Challenges Privacy

Erasing Your Digital Footprint

Who hasn't Googled themselves? It's always interesting to find out what kind of information a search engine associates with our name.

Thinking about it from a malicious perspective: if a scammer were trying to build a profile on you, how much data could they get from a simple internet search? Most likely, they would identify which social media sites you've joined; they would know if you have a personal blog; they might even find pictures of your face. These are all part of your digital footprint—a trail of information associated with your internet activity.

The amount of harm this could lead to depends on how much information you allow to be public. If your social media accounts are set to private, scammers won't have access to your friends, family members, or anything you post. Private social media accounts are one way to cover some of your digital footprints. Here are a few others:

- Upgrade privacy settings in your browser so that it doesn't track your location or any web or app activity.
- Limit the amount of information you make public, even if your social media accounts are set to private.
- Where possible, deactivate any accounts you no longer use (looking at you, Myspace).
- Review and revise permissions granted to mobile apps, and delete any apps you no longer need.
- Consider getting a VPN (virtual private network), which drives your internet connection through an encrypted tunnel and prevents anyone from seeing your location or activity.

To completely remove your digital footprint, you will have to take aggressive steps, such as deactivating all accounts and maybe even hiring a firm that specializes in data deletion. The main idea: we all leave behind a trail of data that can easily be uncovered. It's essential to take measures to hide as much of that trail as possible, so it doesn't lead to security incidents like identity theft (where a scammer uses your personal information to open fraudulent accounts or apply for loans).

If you handle confidential data here at work, you become partially responsible for someone's digital trail and must ensure it never gets exposed. Use common sense. Stay alert for scams. Think before you click, and always follow our organization's policies.

Compliance Regulations That Are Changing the World

It's no secret that organizations all over the world collect our personal data. The real secret is knowing what type of personal data is being collected, who is collecting or sharing it, and why.

But that may be changing. Both the **California Consumer Privacy Act (CCPA)** and the **General Data Protection Regulation (GDPR)** improve consumer privacy by empowering individuals to track their data and even opt out of collection. If you live in California (CCPA) or the European Union (GDPR), here is a snapshot of the rights you have under these laws:

CCPA California Consumer Privacy Act

- Right to know what data is processed, by whom, and why.
- Right to opt out and prohibit organizations from sharing or selling your data.
- Right to file a complaint against organizations that misuse data.

GDPR General Data Protection Regulation

- Right to erasure (request that organizations delete the data they've collected).
- Right to know what data is processed, by whom, and why.
- Right to object to data being collected.

Given that privacy remains an ongoing concern, it may not be long until the rights established under the GDPR and CCPA spread to all consumers regardless of location. These regulations represent an important step in the balance of consumers' right to privacy and the need for organizations to collect information.

Even with modern regulations, one thing remains unchanged: protecting privacy is still—and will always be—the responsibility of individuals. Even the most strict, comprehensive law in the world means nothing if you don't prioritize security awareness and take your privacy into your own hands.

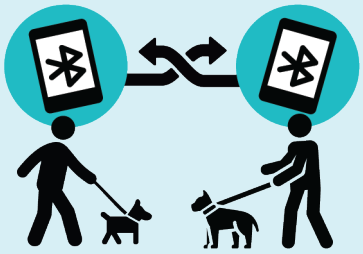
Here at work, it's your job to understand your role regarding these regulations. If you're unsure of your responsibilities, please don't hesitate to ask!

How COVID-19 Challenges Privacy

While almost all of us cherish some level of privacy, few of us would sign up for extended periods of social distancing. That, of course, has become the norm since COVID-19 spread worldwide, causing major closures and cancellations.

With that spread came new questions regarding privacy. ***Wouldn't you, for example, want to know if you encountered someone that has or has had the virus? Conversely, would you want others to know if you contracted the virus?*** It's a tricky balance that comes with no easy solutions.

One such solution, as proposed by Apple, Google, and other developers, is an app that notifies you if you came into contact with someone with COVID-19. The app would use *"Bluetooth low energy,"* a feature that allows smartphones to exchange and store anonymous identifier beacons that contain no personal information or location data. Per a white paper released by Google (who partnered with Apple on the project) it would work like this:



When two people come in close contact for a certain period of time, their phones will exchange anonymous identifier beacons.

If one of the two is positively diagnosed for COVID-19, that infected person can enter the test result into the app. The infected person can consent to upload the last 14 days of their broadcast beacons to the database.

Any other person who has been near the individual who tested positive will then be alerted. The app then provides the individual with information about what to do next.

The key to all of this is user consent. It would rely on individuals opting to upload their test results into a central database—a slope that immediately becomes slippery. Could it lead to overreach by data collectors or governments, considering this process essentially amounts to surveillance? How long does the data stay on the server, and when will it be deleted? Can users opt out and reverse consent? If you got sick, would you give consent for a third party to harvest this data?

Extraordinary situations call for extraordinary measures, to be sure. The COVID-19 pandemic illustrates the incredibly thin line that separates the right to privacy versus the need for data collection, especially where public health is concerned. When it's all said and done, COVID-19 may change the way we handle protected health information in the future.