Privacy, Privacy, Privacy

[Chad Peiper](https://blog.verif-y.com/author/chad-peiper)



When it comes to our personal information, privacy is usually something we all want, but aren’t actively thinking about.

Recent generations have witnessed great advancements in technology and the digital world, giving us unprecedented amounts of access to communication and information starting at a very young age.

This level of ease in communication is beneficial to many parties, often enhancing relationships between individuals, businesses, and other entities. However, there are downsides to having everything so readily available and easily accessible. The information that we as individuals put into these digital spaces are often susceptible to being taken out of our control. And nowadays a lot of what we’re feeding into this digital space is our valuable personal information.

Much of our personally identifiable information is already out of our control; large centralized data brokers manage our data in the background and reap the rewards. We are constantly offering out this information for free in our daily lives. You enter your address and credit card information for something as simple as ordering a pizza. Your birthday, phone number, and mother’s maiden name when opening an email account. Your social security number to apply for a credit card. We enter all these pieces of information so casually and nonchalantly because we are asked to so often. Sure, we want this information to be secure and believe privacy is important – but how often are we consciously thinking about that when entering all these data?

In recent years, it’s been entering our minds surprisingly often. But not for particularly good reasons. The intrusion into our minds comes from reports about identity theft, data breaches, and social media scandals. As more and more private information becomes available in the form of digital data, the more precious privacy becomes. The trading of personal information is a lucrative market in the digital age.

After the credit reporting agency Equifax was hacked in 2017, 148 million people had their personal data compromised, data which included: names, addresses, phone numbers, social security numbers, driver’s license numbers, credit card information and much more. This trend of major data losses and lax security has only continued and has not shown signs of slowing down. In the past year, industry leaders such as Marriott, Capital One and many others experienced data breaches that affected hundreds of millions of people worldwide.

In addition to seeing data breaches carried out by malicious hackers, there are entities that deliberately dole out your private information to third parties. Users of technology such as Apple’s Siri and Amazon’s Alexa have noticed specifically targeted ads for products that they have only ever spoken about. Some of the confusion regarding these situations has been elucidated by the wave of apologies coming from Apple, Amazon, and Google for listening in on users’ conversations without them being made aware. Facebook, who has been notorious in the past for privacy controversies, also recently made a statement saying they had been allowing external contractors to listen to private audio conversations.

Just last year the political consulting firm *Cambridge Analytica* closed after facilitating the exploitation of privacy to an extreme level by using private data (taken without consent) from over 80 million Facebook users in an to attempt to sway their opinions on political campaigns during the 2016 US election (as only one example). This private data (which included personally identifiable information, “likes”, and locations) allowed them to create extremely personalized and targeted political ads. Facebook’s relaxed privacy regulations allowed for drastic violations of personal information to be carried out by a third party for its own gain.

But we see a silver lining on these dark clouds. We’re becoming more aware of how our data is used and what privacy policies are in place. We no longer want to agree to all the Terms & Conditions without understanding them first. We’re more careful about what information we’re giving out and to whom. In addition, privacy regulations are becoming more stringent as privacy continues to seep into the minds of consumers.

More aggressive stances on privacy have been taken up by EU regulators as seen with the General Data Protection Regulation (GDPR), and in California with CCPA beginning January 1st of 2020. The goal of these regulations is to give users back power over their personally identifiable information; such as who can see it, where it is stored, and how it is used. For instance, the EU is leveraging the GDPR to target Facebook’s most recent privacy breaches involving *Cambridge Analytica*, and Facebook could face up to $2.23 billion in fines.

So what happens when there’s a data breach? What do you do when you feel as through your privacy may be threatened? You can’t just decide to stop providing your data in instances when it is required. Think about this: this is the first generation that handles almost everything digitally, including the job application process; from submitting job applications on indeed to posting resumes on LinkedIn. If we want to apply for a job, we must offer up control of our personal information in the form of our credentials – our employment history, educational history, licenses, certifications, etc. – to employers.

So how do we guarantee privacy of that personal data? The need for privacy and security has resulted in the creation of applications such as Verif-y, a user-managed digital identity platform. Verif-y allows users to enter those same situations requiring personal information, all while keeping that information within the individual’s control.

With Verif-y, individual users are able to control and manage their digital identity and credential information. Individuals send credential verification requests to the authoritative source through the Verif-y platform. Once these credentials are verified, individuals manage and share them from within the Verif-y credential wallet. The user controls who has access to their credentials, and has the power to remove access if and when they want.

On the flip side, the credential awarding organizations, and the employers also benefit. Organizations can address data privacy regulations and create a more efficient system for communication of their employees’ personal information. Companies can utilize Verif-y’s variety of Regulatory Compliance Screening services to help in the fight to maintain individual privacy and keep personal information secure (while saving themselves money and resources at the same time.) This includes maintaining compliance with new legislation such as GDPR and CCPA.

Verif-y leverages blockchain technology and multiple levels of encryption to ensure that the personal information entered by users does not fall victim to a data breach and is not used and abused by third parties without user permission. Both employers and users can feel at ease that their information is secure.

So back to the question – what happens if there is another data breach? What if this breach occurs at a company you work for? What does it mean for the company, and for you as an individual employee?

Under the Verif-y platform, the personal data that you have submitted was not retained in the company’s data storage; it’s owned by you and is backed by secure technology. This means the company can retain privacy for its employees’ credential information, and the users remain in control of their data.