Digital Identity: What Is It, and Why You Should Care.

Ed Zabar

[Ed Zabar](https://blog.verif-y.com/author/ed-zabar)



In this article, we will take an in-depth view into the significance of our digital identities and why it is vital to keep them secure. The last eighteen months have highlighted how the worlds of business and government are dependent on valid digital identity solutions. This is apparent in such areas as eCommerce, banking, government, healthcare, and media. However, there are many more areas and applications that require a trusted solution, some of which we will review below. This new necessity and awareness to the dependency businesses and governments have on the individual’s [validated digital information](https://www.verif-y.com/services/identity-verification/) creates compliance and data security issues that are far beyond the ability of most business to handle effectively.

**But what is *digital identity* and why should we care?**

Although there is no single, standard definition, it can be described as “[a combination of personally identifiable traits or attributes](https://learn.g2.com/digital-identity) that are stored in the digital sphere and can be used for interacting online with various individuals, companies and platforms”. Furthermore, a digital identity can be thought of as a digital portfolio of an individual’s personal and sensitive data. The building blocks that make up our digital identity are derived from usernames and passwords, identity cards, bank accounts, and so much more. Some of these pieces of data are given ***to*** the individual, and some are created ***by*** the individual, with both, creating a foundation for an individual’s identity in the digital sphere. These documents and information sources contain your [Personally Identifiable Information](https://www.miteksystems.com/blog/what-is-digital-identity-and-why-should-you-care) (PII). The term PII is defined as “any information that is unique to an individual or known as your ‘personal data’”. However, as opposed to an online repository such as Google Docs, Dropbox, etc., when dealing with sensitive information exchanges (regulatory, legal, health related and others) there is a clear need to ensure that the information shared is authentic and valid, which is not the case with data stored in digital repositories.

**Your Digital Identity Portfolio**

A digital identity portfolio of PII can be divided into five main categories: Government Credentials, Professional Credentials, Online Data and its subset: Social Data, and lastly, Personal Records.

|  |  |
| --- | --- |
| **Government Credentials** | This information can be found on government-issued documents such as passports, driver’s licenses, birth certificates, fishing licenses, military IDs, residency cards, national IDs, and various other official documents (e.g. criminal records, marriage licenses, etc.). |
| **Professional Credentials** | These documents include various records that are either publicly available or are held by various commercial and other entities. They include employment history, certificates, degrees, and diplomas, and more. |
| **Online Data** | This represents the data that online entities hold about individuals and organizations they interact with. These include online purchases histories, search histories, stored data (pictures, records and more), visits to specific websites, locations, email accounts, and much more. |
| **Social Data** | This data is an aggregation of how individuals present themselves online through social media platforms such as Facebook, Twitter, LinkedIn, TikTok, and others. This also includes information that is derived from how others interact with the individual online. |
| **Personal Records** | These include financial, health, legal and other personal records. Examples of these records include healthcare records, various legal records such as titles, claims and legal actions, and financial records such as bank accounts, credit scores, mortgage data and more. |

These documents, profiles, search data, and other online information are some of the building blocks that help create the individual’s digital identity. If properly constructed, validated, and stored, this multi-layered identity is very difficult to breach.

If these records become compromised or unavailable to the individual, as a result of loss or a breach, **the consequences can be severe, long lasting** and can include (but certainly not limited to): limited to no access to healthcare, hindrance to the ability interact with various government entities, limited to no access to banking and other financial information, and difficulties enrolling/interacting with various types of other organizations.

The use and sharing of these documents in our everyday lives creates a privacy and compliance issue for organizations that have, or require, access and storage of personal data to interact and transact with individuals. Given that identity theft is now more prevalent than ever, the need to strongly secure our digital identities is more paramount than ever.

**Compliance Issues and Personal Breaches**

In our increasingly digital-driven lives, more and more social media platforms, financial organizations, online platforms and other entities that requires signup and access to personal or proprietary information, rely on multi-factor authentication. These organizations authenticate users by combining the user’s unique combination of username and password with another item of unique user centric data, such as a photo extracted from a government ID, biometric data that the individual was required to provide in the sign-up process, a physical digital key, a text message, an app and more. As various organizations gather more and more data about us for their own purposes, they are also creating a problem by holding an increasing amount of PII that is out of our control.

In the past decade, and recent months, we have heard about the threat of global cyber-attacks, governments playing a bigger role in setting privacy regulations and standards, and corporate giants being fined millions and billions of dollars for selling, misusing, or not protecting their users’ personal data. Recent data breaches have started to sway consumer behavior, as users are more likely to leave a platform if a data breach has occurred where their data either has or could have been compromised. This continued loss and abuse of data over the past several decades has driven governments around the world to begin drafting, publishing and implementing strong privacy laws. The EU was the first to establish stringent and forward looking laws to protect individual privacy rights in May of 2018 with the establishment of the [General Data Protection Regulation (GDPR).](https://gdpr-info.eu/) This was the first large scale, government sponsored effort to address the inabilities of today’s laws to address the rapid changes in how our data is used/abused. However, the growing list of global regulations needs to keep up with the rapid changes in our digital world and ensure that they don’t stifle innovation, access and individual rights. To date, [over 123 countries](https://www.infosecurity-magazine.com/opinions/users-control-own-digital-identity/) have begun the process of passing new data privacy laws leveraging the relative success of the precedent set by GDPR.

With [legislation undoubtedly becoming more stringent](https://blog.verif-y.com/us-data-privacy-laws-explained), companies can no longer ignore the need to protect their users’ privacy and personal data. Digital centric companies and those with digital platforms are now spending more on digital privacy and will continue to increase their spending as new privacy acts become laws around the world. This creates a challenge for these companies, as well as an opportunity to continue to evolve business models. It is now necessary for users to feel safe when using digital platforms and make sure that they better understand how their data is used.

**So What Is The Solution?**

A strong digital identity is comprised of information such as government issued IDs professional credentials, health records, bank information, social media accounts, and more. Combined, and carefully used, these documents and information can be part of an individual’s online presence and identity. It is imperative that individuals can take back control of their own sensitive information and only use what they choose, with each platform they interact with.

**This is where our solution comes in.**

Verif-y’s digital identity solution creates a safe and easy to use platform in which individuals hold and control their personal data. Individuals can easily and safely monitor, transact, and share various parts of their identity wallet with individuals and organizations from around the world. At Verif-y, we give the user full control over their identity documents, without needing to see or store the user’s data. Verif-y’s digital identity solutions include [Identity Verification Services (IDV)](https://www.verif-y.com/services/identity-verification/), [Know Your Customer (KYC)](https://www.verif-y.com/services/identity-verification/), [Know Your Business (KYB)](https://www.verif-y.com/services/identity-verification/),[Background Checks,](https://www.verif-y.com/services/background-checks/) and [Credential and Employment Verification](https://www.verif-y.com/services/credential-and-employment-verification/). Verif-y provides [financial institutions](https://www.verif-y.com/industries/financial-institutions/), [healthcare](https://www.verif-y.com/industries/healthcare/), [education](https://www.verif-y.com/industries/education-2/), and [human resources](https://www.verif-y.com/industries/employers/) organizations the ability to better understand who the individuals they interact with really are. This is done while transferring the control to the individual whose data is sought by the organization. Our solutions transform the way individuals manage their data by creating a simple to use, secure platform that allows for safe and permissioned exchange of sensitive personal data.

[See Our Approach](https://blog.verif-y.com/cs/c/?cta_guid=c5a99eb8-a6f3-45e9-8958-c4169ce575fd&signature=AAH58kHh9UXqQlW_4sII_uXSgzNqFcVt6w&pageId=49897895329&placement_guid=4f53c0bf-1fe9-410f-9311-a8294ca0e001&click=ae773527-3b09-4b17-8157-2d9bbbc655ec&hsutk=9d11a544117a53686af606949393a9eb&canon=https%3A%2F%2Fblog.verif-y.com%2Fwhat-is-digital-identity&utm_referrer=https%3A%2F%2Fblog.verif-y.com%2F&portal_id=9009840&redirect_url=APefjpFLyuXdpWiVc-RfBsLru6GNTMX6WpluObY1A6LbEOxYCNvayBFU7mLl6gfDuNVOl9DSAdqYxaaqGjUN7Gy8RzULJMK9v_eNTRmrR8U2G1qbOeJxsudF3uhFqZ4i5mMMuGKhhGLRA04zuruvYTW8KtUtMb6k7zoD9m2xMKqCWM3yHyaVzyiC5VTLRdI38s3wnIm1Oq6zbCOXXPK6W4Tjflm6o-tOI1n4wwQHSeFPRMbu_KcX1scXu_3Y9DOIEca5HmxjcshM8vmaIRnQRc4HRdY2VQdML9z8ChsLp7jZOf5XhmsQyUc&__hstc=66120369.9d11a544117a53686af606949393a9eb.1649849487414.1657630774363.1657633078290.50&__hssc=66120369.12.1657633078290&__hsfp=980283150&contentType=blog-post" \o "See Our Approach" \t "_blank)