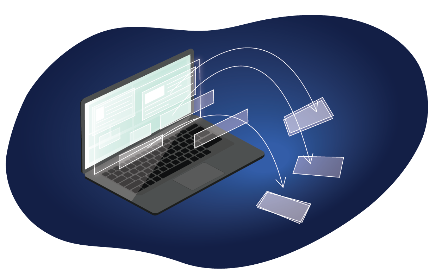
How Secure is your Personally Identifiable Information? (PII)

David Maberry

[David Maberry](https://blog.verif-y.com/author/david-maberry)



As part of Verif-y’s ongoing efforts to educate organizations and individuals about digital identity, we thought it might be useful to dedicate a post to the current challenges related to the protection of Personally Identifiable Information (PII), as well as provide suggestions on potential mitigation strategies.

One would assume that given all the kerfuffle surrounding constitutional rights, someone would already be loudly and passionately complaining about the continued violations of the following constitutional amendments:

* + **First Amendment:** Freedom of ***religious belief and to*** ***keep that choice private***.
  + **Third Amendment**: Protects the ***home as a zone of privacy***.
  + **Fourth Amendment:** The ***right of privacy against unreasonable searches and seizures by the government.***
  + **Ninth Amendment:** Protects ***citizens fundamental right to privacy covering areas that are not specifically addressed in the other amendments.***

The United States ranks in the middle of the global pack for privacy protection

Although I am not a lawyer nor a constitutional scholar, I still find this lack of attention odd, especially in the case of a country who espouses the constitutional rights of its citizens. In fact, the United States ranks in the middle of the global pack for privacy protections. According to the [United Nations Conference on Trade and Development](https://unctad.org/page/data-protection-and-privacy-legislation-worldwide) 66% of the 194 member countries have adopted some form of privacy related legislation for their citizens.

Adding to the complexity of the challenges faced by citizens of the United States, privacy protections can differ greatly based on state of residence, with citizens of California and Virginia benefiting from the strongest legal protections. Mississippi and Utah both tried, and failed, to pass privacy specific laws while the rest of the states consist of a mixed bag of legislation,[both proposed and in process](https://iapp.org/resources/article/state-comparison-table/). Currently, there are limited privacy protections in place at a Federal level (e.g. [Health Insurance Portability and Accountability Act [HIPAA]](https://www.cdc.gov/phlp/publications/topic/hipaa.html)) however a single, overarching Federal privacy standard, such as the [Global Data Privacy Requirement (GDPR](https://www.globaldata.com/privacy-policy/)) for citizens of the European Union, does not exist for all citizens of the United States of America.

The final *piece de resistance* is the age and condition of most state and federal government technology platforms, the use of which was never originally intended for mobile applications. This presents an obstacle that will be further amplified by 5G networks that will potentially transmit and share even more personal information via the Internet of Things (IoT) devices. This challenge is especially salient for government institutions that continue to manage their constituent’s data on mainframe-based platforms or, as a work around, have uploaded their mainframe data to a cloud solution. This is the behavioral equivalent of moving out of your apartment because it’s full of stuff, and renting another apartment to fill with the same stuff.

The pandemic has exposed these systems to further challenges

Ironically, investing billions of dollars and adding layers of technology to these aging technologies has actually *increased* Federal and State government’s risk and vulnerability for security breaches and data loss. In some cases, this issue is exacerbated due to the multitude of work-arounds required to make these aging systems more mobile and user friendly. The pandemic has exposed these systems to further challenges with maintaining the confidentiality, availability, and integrity of personal data security. See [Solarwinds, Microsoft, election/voter interference, etc.](https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time" \t "_blank) for further support of this position.

Rather than continuing to dedicate time and resources to shoring up aging technology, a novel approach would be to challenge the notion that technology is infinitely saleable. An architect would never build a 30-story building using an existing foundation for a 3-story building. That effort would require extensive re-engineering and most likely a completely new foundation on which to build the new structure. Why should technology be any different?

An architect would never build a 30-story building using an existing foundation for a 3-story building.

Verif-y utilizes a patented, machine learning and blockchain based process to secure data in a manner that meets or exceeds current regulatory requirements such as the Global Data Privacy Requirement (GDPR), Personal Information Protection Act (PIPA), California Consumer Privacy Act (CCPA) and other regulatory requirements governing the use of personally identifiable information. If your organization is currently overwhelmed with options for addressing these types of requirements, consider Verif-y as a simple, safe alternative to large scale, resource intensive efforts to meet compliance requirements. This approach empowers entities with the ability to offer a completely unique technology in order to shift privacy related data over to a platform that is equipped to scale with growth while meeting or exceeding global privacy requirements.

 David Maberry

David has over twenty-five years of experience in leading the application of emerging technologies while streamlining governance requirements and thereby creating sustainable, organizational change. Prior to joining Verif-y, David was a Managing Director for PwC where he was responsible for the risk assurance emerging technologies practice. He has also served as the Chief Risk Officer for a financial services organization and, finally he was a Principal at Deloitte where he focused on privacy and security initiatives. He is a frequent guest lecturer at national and local professional services conferences on subjects such as enterprise risk management, emerging technologies and organizational transformation.