Core Principles of Information Privacy

IMMUNIZE YOUR SENSITIVE DATA©

Table of Contents

Intro

Following the breach of the United States' National Security Agency (NSA), a renowned bastion of security, and the subsequent auction of its cyber espionage tools on the Deep Web, the certainty of avoiding hacking incidents becomes elusive. The prevailing sentiment is that it's not a question of if one will be hacked, but rather when.

It becomes crucial to discern the distinction between information "Security" and "Privacy". Notably, privacy is not inherently encompassed within the realm of cybersecurity. The cybersecurity industry, true to its nomenclature, centers on providing security measures rather than addressing privacy concerns directly. Understanding this differentiation is pivotal in navigating the evolving landscape of digital threats and fortifying against potential cyber intrusions.

According to the United States' National Institute of Standards (NIST) newest Cybersecurity Framework 2.0: "*Cybersecurity and privacy are independent disciplines, but in certain circumstances their objectives overlap*".

Who truly values privacy? Consumers take the lead, where they face the reality that they often wield minimal, if any, influence over the storage practices of their Personal Identifiable Information (PII) by service providers in banking, telecommunications, insurance, and healthcare, just to name a few. Enterprises come second, but increasingly so, as corporations such as 23andMe begin to face class action lawsuits, putting many on the brink of survival.

Information Privacy vs Security

While closely intertwined, these two terms are not interchangeable, despite frequent misuse to convey a similar concept. The security of something deemed valuable primarily pertains to the constraints and controls placed on its access. On the other hand, privacy specifically addresses how the content is shielded from intrusive observation.

Consider a written document classified as top secret, where public disclosure or awareness by third parties poses a substantial threat. Safeguarding its security involves placing the document within a sealed box inside a maximum-security safe, situated in a fortified area bolstered by security measures and personnel, ensuring exclusive access for authorized individuals.

Preserving its privacy, however, requires a distinct approach—ensuring that only authorized individuals can comprehend the document's content. This objective is achieved through the indispensable application of cryptography, a practice that has proven successful for millennia in maintaining the confidentiality of sensitive information.

What sets privacy apart from security? Even if an unauthorized entity manages to overcome all the security measures safeguarding a document, gaining access alone doesn't equate to comprehension. The content remains protected by encryption, rendering the invested time and effort in breaching security futile.

When information privacy is prioritized alongside security, a noteworthy outcome emerges: in the unfortunate event of a security breach, the ensuing damage is minimized. This principle extends seamlessly to documents, information, and data in both physical and digital formats, affirming the importance of a comprehensive approach to safeguarding sensitive assets.

Private Information goes beyond PII

Personally Identifiable Information (PII) encompasses a spectrum of sensitive details—names, dates of birth, social security numbers, phone numbers, addresses, banking information, medical records, and an extensive array of other personal data. The gravity of safeguarding the privacy of such information cannot be overstated, as unauthorized disclosure can lead to severe consequences. Identity theft can inflict financial ruin upon individuals or families, while a data leak has the potential to bring down entire companies or organizations.

Expanding beyond PII, a myriad of other sensitive information demands vigilant protection from prying eyes. This spans from confidential attorney-client communications to proprietary commercial secrets, private negotiations, signed contracts, trade secrets, law enforcement investigations, merchandise transport details, and military communications. In essence, any information that, if leaked, could cause harm to individuals or organizations is deemed sensitive and private. Data leaks have evolved into existential threats for entities and individuals alike, especially for those ill-equipped to grapple with the repercussions of unauthorized access to such critical data.

Cybersecurity

Cybersecurity is essentially the practice of protecting systems, networks and programs from digital attacks (cyberattacks) and unauthorized access.

According to the United States' National Institute of Standards (NIST) newest Cybersecurity Framework 2.0: "*Cybersecurity risks are a fundamental type of risk for all organizations to manage. Potential impacts to organizations from cybersecurity risks include higher costs, lower revenue, reputational damage, and the impairment of innovation. Cybersecurity risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences. The NIST Cybersecurity Framework (Framework or CSF) 2.0 provides guidance for reducing cybersecurity risks by helping organizations to understand, assess, prioritize, and communicate about those risks and the actions that will reduce them. Those actions are intended to address cybersecurity outcomes described within the CSF Core. These high-level outcomes can be understood by a broad audience, including*

executives, government officials, and others who may not be cybersecurity professionals. The outcomes are sector- and technology-neutral, so they provide organizations with the flexibility needed to address their unique risk, technology, and mission considerations. These outcomes can be used to focus on and implement strategic decisions that improve cybersecurity postures (or state) while also considering organizational priorities and available resources".

Cybersecurity can be defined as the continual process of erecting, sustaining, and updating digital defenses to thwart unauthorized access to individuals' or organizations' digital assets. However, it's worth noting that within this conceptual framework, there is a conspicuous absence of specific references to encryption or cryptography.

Cyberprivacy

Cyber-Privacy revolves around safeguarding the privacy of digital assets and preempting the theft, abduction, or public disclosure of sensitive information in the event of a cybersecurity breach.

It may seem unusual, but the official publication from the United States National Institute of Standards and Technology (NIST) minimally addresses encryption or cryptography in its Privacy Framework paper titled. "NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0", from January 16, 2020.

The Privacy Framework states:

> "*For example, if an individual requests access to data, the organization may not be able to produce the data if the data have been distributed or encrypted in ways the organization cannot access*"

Subsequently, the document incorporates two additional quotes pertaining to the utilization of cryptography.

> "*Depending on its objectives, if an organization is trying to achieve privacy by limiting observation, this may lead to implementing measures such as distributed data architectures or privacy-enhancing cryptographic techniques that hide data even from the organization*", and "*CT.DP-P1: Data are processed to limit observability and linkability (e.g., data actions take place on local devices, privacy-preserving cryptography)*".