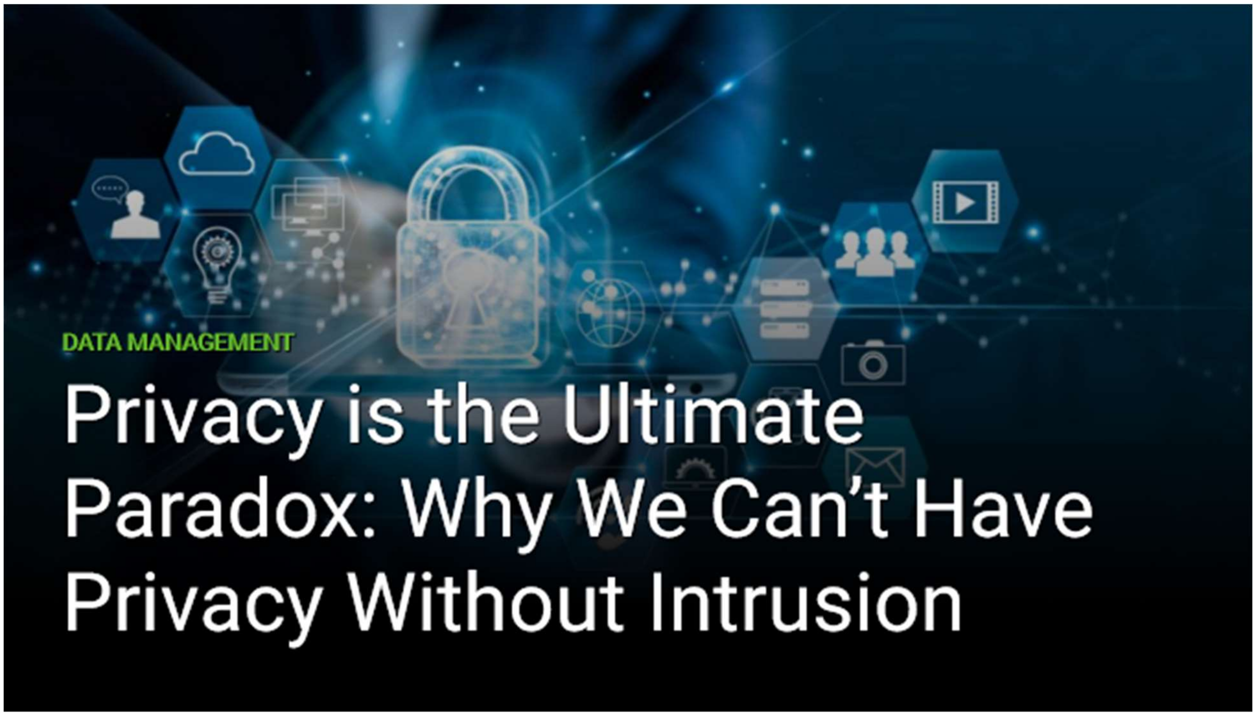

Privacy is the Ultimate Paradox: Why We Can’t Have Privacy Without Intrusion

This article explore the contradictions that arise with data regulations. It helps us consider how history is shaping attitudes toward privacy and is charting a path forward for businesses facing the demands of regulation today.

“Doublethink”, a concept defined by George Orwell as the simultaneous acceptance of two mutually contradictory beliefs. Now 70 years after 1984’s publication, new data regulations ask us to consider a premise that Orwell most of all could appreciate: Privacy equals control.

In April of 2016, The General Data Protection Regulation, otherwise known as GDPR, was passed by the European Union Parliament. Intended to put power over personal information back into the hands of the individual, GDPR also propels organizations to tighten their grip on enterprise data, personal and otherwise.

No business regulation in recent memory has loomed so large or appeared so daunting to multinational enterprises as GDPR’s four percent of global annual turnover penalty. One board member affectionately refer to it as the God Damn Privacy Regulation. The ramifications of this law may echo for years to come.

Now over two years after being passed and five months after going into effect last May, we’re finally starting to get a hint of potential sanctions, including an investigation into Facebook by the Irish Data Protection Commissioner for a recent data breach. European Data Protection Supervisor Giovanni recently alluded to potential fines by the end of the year as well.

While GDPR remains the most formidable, other countries have followed the EU's lead with their own flavors of privacy regulations, including Brazil, India, and several US states.

Challenging Requirements and Steep Sanctions

The challenging new requirements coupled with steep sanctions cast a shadow on a significant cross-section of functions at multinational corporations, requiring synchronization across IT, records management, legal, compliance, and information management. These requirements have compelled the implementation of new technologies and business processes designed to index, identify, analyze and control the use and retention of all enterprise data.

While the promise of better management and protections afforded to personal information is appealing, a key point is often missed: the technologies and processes necessary to compliance facilitate a degree of intrusion into personal data on a scale that is unprecedented.

This new wave of regulations requires corporations to identify and analyze personal data enterprise-wide, and then attribute it to the data subject. Therefore, as companies adapt to the new requirements, they necessarily increase the accessibility of knowledge available to them for each individual whose data they manage. Many leaders in the data privacy community have commented on this paradox privately, but it has yet to receive any meaningful media coverage.

To illustrate, now dragged into the regulatory spotlight are enormous repositories of "unstructured" data—data created by humans, for humans, comprising emails, instant messages, documents found in file shares, etc.—that until now have been undermanaged. Because this data is humanmade, aside from the common scenario of documents containing standard personal information such as address, social security, credit card number, etc., it can be extraordinarily revealing of individual behavior and intent and is therefore highly sensitive.

Intuitively, this data needs to be governed. However, as organizations undertake initiatives to analyze and manage unstructured data for regulatory purposes, it also becomes increasingly accessible to utilize for other purposes as well.

Existing use cases I've seen firsthand range from legal and security-driven to sales and HR.

For instance, identifying which employees are likely to quit (based on communication patterns), who are subject matter experts, and who are the go-to people in each department. This is just the beginning. It also has the power to reveal employee sentiment towards the company, political beliefs, or mental health.

GDPR May Increase the Protection of Nominal Data

There is a real danger to asking corporations to command every single document they own containing personal data. By complying with these regulations, organizations are only a step away from building out complete data profiles for each data subject and therefore uncovering more about us than ever before. As Tim Cook ironically noted in a recent speech, scraps of data can be harmless on their own but dangerous when assembled.

However, as has the public forum by and large, while praising GDPR he also failed to address the possibility that it may simply increase protection of "nominal data" while forcing powerful technologies into the hands of the world's largest corporations. Who cares what companies do with our personal address when technology will soon enable them to analyze every facet of what makes us, us?

It's important to note here that GDPR protects corporate use of data for particular purposes, including legal requirements and "legitimate interests." We are yet to see what will and won't qualify as a legitimate interest.

One thing is clear: As a civilization, we must determine what is an acceptable level of intrusion into our lives and into our character and stand by it.

Need for Safety Mechanisms

We must stay vigilant about the many privacy encroachments already endemic at home, ranging from corporate data processing to the Patriot Act and NSA surveillance to the scanning and tracking of citizens' car license plates with location data. Under the pretense of protection, we end up herded toward a surveillance society and ill-prepared for the consequences ahead.

With so much at stake, how then do we harness information technology for good while mitigating its side effects? As technology advances, it is incumbent on us to build in safety mechanisms whenever good intentions yield to temptation and oversight authority leads to abuse of power.

In 1948, perhaps even Orwell couldn't have imagined the power to be wielded through control of information. But he conveyed a fundamental truth of living in today's information age: "If you want to keep a secret, you must also hide it from yourself."

As we continue to plunge willfully into the digital maelstrom, perhaps the updated Orwellian perspective should replace "doublethink" with "think twice."