
PRIVACY & DIGITAL TRUST: 2010'S WERE ABOUT DATA COLLECTION; 2020'S WILL BE ABOUT DATA PROTECTION

Team8 – Global venture group
03 Mar 2021

On one hand, globalization and the growth of the digital economy are accelerating the need for safe and trustless means of digital collaboration to remain competitive. On the other, emerging privacy regulations and consumer preferences are driving more investments in privacy-enhancing technologies and providing users with more control over their data. The net result of these colliding forces will be new privacy- and zero trust-driven strategies that impact underlying architectural design and business processes.

Drivers

The recent history of high-profile data breaches is accelerating privacy regulations and eroding consumer trust in companies. Cisco's 2020 Consumer Privacy Survey¹ revealed that one-third of consumers are "Privacy Actives" who have stopped doing business with organizations over Data Privacy concerns. This trend is likely to continue as 65% of the world's population will have its personal data covered under modern privacy regulations in the next two years, up from 10% in 2020.² Yet, many organizations have a hard time keeping up with the growing and ever-changing regulations because they lack an effective Governance Risk and Compliance (GRC) program and regulations often conflict with one another, making it costly and complicated to comply. To satisfy regulations and earn consumer confidence, organizations need to take a proactive approach with tools, systems, and services that help them get ahead of business risk by identifying and managing personal information within their enterprises and throughout the supply chain, respecting regional variations in data regulations, and transparently supporting consumers' intentionality about data sharing.

Impact - In the future, personal data may be controlled by the consumer, which will drive changes in business models, regulations, and security. As consumers and companies become more scrupulous, technologies that enable doing business without sharing data will take centre stage and drive competitive advantage. Storing data that an enterprise doesn't need has become a liability not worth taking. Not knowing what data it has and who has access to it has become unconscionable.

Solutions - Data Discovery, Data Classification, Privacy Rights (DSAR), Data Protection and Compliance, Homomorphic Encryption, Anonymization & Synthetic Data, Distributed Machine Learning, Multi-Party Computation

Perspectives:

Defender's Perspective - *"In today's digital world, privacy sometimes, albeit superficially, seems at odds with business objectives. Businesses must reconcile a vigorous appetite to collect, leverage, and exchange data that could be monetized with a growing demand for enhanced privacy from consumers and regulators. In particular, businesses need to carefully consider reducing their liability as related to data loss or misuse. Privacy preserving technologies such as homomorphic encryption help businesses to achieve new and existing objectives by enabling the processing of data while keeping it encrypted, and outsourcing computation to untrusted servers and clouds without compromising on privacy. Such mathematical approaches may not only help to improve existing data sharing practices, but even more importantly can unlock hidden value, new business models, and unique approaches to collaboration for organizations who are willing to adopt a new privacy paradigm."* - Professor Shafi Goldwasser, Director of the Simons Institute for the Theory of Computing, UC Berkeley.

Team8's Attacker Perspective

The use of privacy-preserving technologies and a decreasing number of large hackable open datasets is pushing bad actors to attack the edges and collect data before it can be secured. Payment Card Industry (PCI) removal of credit card numbers from databases pushed attackers towards attacking the Point-Of-Sale system, where the card number was "in the clear". Similarly, privacy-preserving technologies will make the edge devices increasingly important to attackers who are after the raw data.

In our next blog, we will cover Resilience & Recovery.

Sources

¹ https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-infographic-2020.pdf

² <https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w>

Related blogs

- + [Introducing cybersecurity, the megatrend of the 2020s](#)
- + [Cloud security: A necessary component in digital transition planning](#)
- + [Security of Things: Dealing properly with the explosion of connected devices](#)
- + [Perimeterless world: Networks are becoming less tied to physical locations](#)

Related products

- + [WCBR - WisdomTree Cybersecurity UCITS ETF - USD Acc](#)

View the online version of this article [here](#).

Important Information

Marketing communications issued in the European Economic Area (“EEA”): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as “WisdomTree” (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.