COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2024

Camille Howard (camillehoward@humanisticpowerllc.com, linkedin.com/in/dr-camille-howard) is President & Co-Founder of Humanistic Power LLC in Charlotte, North Carolina, USA.

Redefining privacy in a digital world

By Camille Howard, DBA, CCEP, CCEP-I, CIPP

The Latin phrase *ius relinquendum est*, which translates to "the right to be left alone," encapsulates an ancient concept of privacy that has undergone a dramatic evolution in the digital age. This ancient notion—deeply rooted in the desire for personal space and autonomy—has evolved significantly, especially in the digital age where personal data becomes an extension of self.

As we navigate this era, data privacy and individual identity fusion present new challenges and opportunities for compliance professionals. This article explores how embracing this unique perspective of privacy as an integral part of self can transform compliance strategies, making them more effective and competitive in today's digital landscape.

The digital self: Understanding data as an extension of identity

Every digital interaction contributes to a rich mosaic that defines our digital identity in today's interconnected world. This goes beyond mere online presence; it's a comprehensive digital persona shaped by various online activities. From social media footprints to browsing habits, online purchases to location tracking, each data point we generate becomes a pixel in the broader picture of our digital selves. This interconnectedness of personal data and identity is profound, marking a shift in how we perceive privacy. It's no longer just about safeguarding information but protecting an integral part of who we are. Recent statistics underscore this reality: a report by DataReportal in 2023 indicated that the average person spends nearly seven hours online daily, generating enormous volumes of data contributing to their digital identity.[1]

The proliferation of smart devices and Internet of Things technology has further entrenched this concept. According to data by Parks Associated, there was an average of 17 connected devices per household in the U.S in 2023.[2] These devices, ranging from smartphones to smart home technologies, constantly gather, store, and transmit data, weaving an ever-expanding digital fabric of our personal lives. This relentless data generation is not just a passive occurrence but actively shapes how businesses, governments, and society perceive and interact with us. It underlines compliance professionals' importance in protecting this data and understanding its broader implications on individual autonomy and rights.

In this context, data privacy becomes more than a compliance requirement; it's fundamental to preserving the digital human condition in the 21st century.

The privacy paradox and the control dilemma

In this digital landscape, users frequently exchange their personal information for convenience or access to free

services. This transaction often occurs without a complete understanding of its implications, leading to a critical question: How much control do individuals have over their data and, consequently, their digital selves? In reality, individuals' control over their personal data could be better.

The complexity and opacity of data collection practices by various online platforms and services can obscure the extent to which personal information is harvested and used. Terms of service agreements—often lengthy and filled with legal jargon—are routinely accepted without thorough reading, inadvertently granting broad permissions to collect and use personal data. The rise of technologies like artificial intelligence and machine learning has deepened this paradox.

These technologies can analyze vast amounts of personal data, creating detailed profiles that can predict behavior and preferences. While this can lead to enhanced user experiences, it also raises concerns about privacy, autonomy, and the potential misuse of such profiles.

Additionally, the digital divide exacerbates this issue of control. Only some have equal access to resources, knowledge, or tools to protect online privacy. Those less digitally literate may find it challenging to navigate privacy settings or understand the implications of data sharing, resulting in a disproportionate impact on their privacy and autonomy.

As we consider the profound ways in which personal data has become an extension of our digital selves, it becomes increasingly clear that the impact of technology on privacy rights cannot be overstated. The advancement of technology has not only expanded the scope of data collection but has also introduced complex challenges in how this data is used, shared, and protected. The ensuing case studies offer a window into the real-world implications of these technological advancements, illustrating the potential risks to privacy and the crucial role that compliance professionals play in safeguarding these rights. These examples highlight the necessity for a proactive and informed approach to compliance, adaptable to the rapid pace of technological change and sensitive to the intricate relationship between personal data and individual privacy.

Navigating the challenges: Case studies and implications

Case study: The Strava heatmap incident

In 2018, Strava—a popular fitness-tracking app—released a global heatmap visualizing the activities of its users.[3] However, it inadvertently exposed sensitive information about military bases and personnel movements, as soldiers using the app were included in the data. This incident raised serious concerns about data sharing and user privacy, even in seemingly innocuous contexts. It highlighted the unintended consequences of mass data collection and the necessity for organizations to consider the privacy implications of publicly sharing user data.

Case study: GDPR and the Schrems II ruling

The EU's implementation of the General Data Protection Regulation (GDPR) significantly affected global data privacy practices. A pivotal moment in GDPR's enforcement was the Schrems II ruling in 2020, following privacy advocate Max Shrems' complaint against Facebook's data transfers from the EU to the U.S. The European Court of Justice invalidated the Privacy Shield agreement, which governed transatlantic data transfers, citing inadequate privacy protections in the U.S.[4] This ruling reinforced the importance of safeguarding EU citizens' data and the ripple effect on international data transfer agreements, compelling compliance professionals to reassess and strengthen data protection measures in line with GDPR standards.

Case study: Facial recognition technology and privacy concerns

The increasing deployment of facial recognition technology—particularly by law enforcement—has raised significant privacy and ethical concerns. A 2019 study by the National Institute of Standards and Technology revealed racial and gender biases in facial recognition algorithms.[5]

Additionally, using this technology without explicit consent has led to public backlash and legal challenges. This case study reflects the ethical challenges and potential privacy violations of advanced technologies. It underscores the importance of implementing compliance measures that respect individual privacy rights and prevent discriminatory practices. These case studies demonstrate the nuanced challenges at the intersection of technology and privacy rights. They emphasize the critical role of compliance professionals in navigating these complexities, advocating for ethical data practices, and adapting compliance strategies to protect individual privacy in an increasingly digital world.

Having explored the intricate dynamics of the privacy paradox and the varying degree of control individuals have over their personal data, the focus now shifts to the role of compliance professionals and discussing actionable tactics and forward-thinking approaches to implement in this complex landscape.

Empowering compliance professionals: Strategies and tactics

These strategies are designed to navigate the challenges of modern technology and data privacy concerns, ensuring that organizations comply with current regulations and proactively protect and empower their digital constituents.

Here, we delve into practical measures and innovative solutions to create robust, ethical, and competitive compliance frameworks in the digital age.

- **Embed privacy into organizational DNA**: Beyond fostering a culture of data ethics, compliance professionals should aim to embed privacy considerations into the very DNA of their organization. This means going beyond education and implementing a mindset where every employee, from top to bottom, acts as a custodian of data privacy, understanding the implications of their action on data security.
- **Advance data minimization principles**: Develop and enforce policies emphasizing data minimization—collecting only the data essential for the intended purpose. This strategy reduces the risk of data breaches and aligns with increasing consumer expectations for privacy.
- **Embrace ethical data analytics**: In an era where data analytics is vital for business insights, ensure these analytics are conducted ethically. This involves scrutinizing the sources of data, the methods of analysis, and the purposes for which data is being used, ensuring they all meet high ethical standards.
- **Facilitate cross-departmental privacy collaborations**: Encourage collaborations between different departments—such as IT, legal, and marketing—to foster a more holistic approach to data privacy. This can lead to more comprehensive strategies that address privacy from multiple angles.
- **Implement dynamic consent mechanisms**: Go beyond static consent forms and implement dynamic, user-friendly mechanisms that allow consumers to choose how their data is used and shared. This approach empowers users and builds trust.
- **Engage in privacy thought leadership:** Establish your organization as a thought leader in privacy. This can be achieved through publishing insightful content, participating in industry panels, and contributing to public discussions on privacy issues.

- **Develop a data breach response protocol**: While prevention is critical, having a robust response protocol for data breaches is essential. This includes the technical response and communication strategies to manage stakeholder relations and reputation in the aftermath.
- **Advocate for balanced privacy legislation**: Actively participate in shaping balanced privacy legislation that protects individual rights while considering the practicalities of implementation for organizations.
- **Use privacy-enhancing technologies (PETs)**: Invest in and use PETs that help anonymize and encrypt data, ensuring that personal data remains private and secure even during a breach.

Incorporating these less conventional yet effective strategies can provide compliance professionals and leaders with a comprehensive tool kit to navigate the evolving landscape of data privacy and protection, thus securing a competitive edge for their organizations.

Conclusion: A call to action

We've highlighted the profound transformation in our understanding of privacy in the digital age, where personal data has become a digital extension of the self. The intricate relationship between data privacy and individual identity presents challenges and opportunities for the compliance community. The case studies of Strava, GDPR, and facial recognition technology underscore the nuanced complexities at the intersection of technology and privacy rights. They emphasize the critical role of compliance professionals in advocating for ethical data practices, navigating legal landscapes, and adapting to rapid technological changes. The outlined strategies, from embedding privacy into organizational culture to employing PETs, offer a roadmap for compliance professionals to develop robust, ethical, and competitive frameworks.

This proactive and informed approach is vital for safeguarding the digital human condition and maintaining trust in an increasingly interconnected world. The call to action for compliance professionals is to protect our digital identities and ensure privacy remains a fundamental right in the digital era.

Takeaways

- Privacy has drastically evolved in the digital age, encapsulated by the Latin phrase *ius relinquendum est* (the right to be left alone). Privacy is all about protecting information and preserving an integral part of individual identity shaped by various online activities.
- Every digital interaction, from social media to browsing habits, contributes to a person's digital identity, a comprehensive digital persona comprising data points generated online. This practice highlights the deep connection between personal data and individuals' identities.
- The proliferation of smart devices and the Internet of Things technology has led to an increase in personal data collection, significantly impacting how businesses, governments, and society perceive and interact with individuals. This trend emphasizes the need for compliance professionals to understand and protect this data.
- There's a paradox in the digital landscape where users often exchange personal information for convenience. However, the complexity of data practices and the opacity of terms of service agreements can limit an individual's control over data. This issue is compounded by technologies like artificial intelligence, which can analyze vast amounts of personal data, raising concerns about privacy and autonomy.
- Compliance professionals are crucial to navigating the complexities of technology and privacy rights. They

must adapt their strategies and tactics to address these emerging challenges, including developing robust and ethical compliance frameworks, implementing data minimization principles, and using privacy-enhancing technologies.

1 Simon Kemp, "Digital 2023: Global Overview Report," DataReportal, January 26, 2023, https://datareportal.com/reports/digital-2023-global-overview-report.
2 Erik Gruenwedel, "Parks: Average U.S. Internet Home Had 17 Connected Devices in 2023," Media Play News, January 10, 2024, https://www.mediaplaynews.com/parks-average-internet-u-s-home-had-17-connected-devices-in-2023/.
3 Tara Copp, "Fitbits and fitness-tracking devices banned for deployed troops," *Associated Press*, August 6, 2018, https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/.
4 European Parliament, "At A Glance: The CJEU judgment in the *Schrems II* case," 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.
5 National Institute of Standards and Technology, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," December 19, 2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.