THE GENERAL RELATIVITY OF PRIVACY

TREO Paper

Tawfiq Alashoor
Department of Operations, Information and Technology
IESE Business School
talashoor@iese.edu

Abstract

Einstein redefined our understanding of gravity with the theory of general relativity, illustrating it as a curvature of spacetime rather than a simple force. This research introduces the General Relativity of Privacy (GRP) to reconceptualize personal data through the lens of 'contextime' rather than spacetime. While space, such as geolocation, identifies us in the digital world, it is context that most significantly shapes our lifetime experiences. The GRP establishes that the meaning and value of privacy (e.g., personal data) is determined by contextime. With the foundation of two decades of theoretical and empirical research in information privacy, this macro viewpoint emphasizes how contextime shapes our digital identities and interactions, setting a foundation for addressing cybersecurity threats and enhancing economic freedom around privacy. The GRP offers a roadmap, presenting tangible recommendations for scholars, business leaders, policymakers, and especially consumers, all in a bid to protect a fundamental human right: information privacy.

Keywords: General Relativity of Privacy, Cybersecurity.

Toward a New Paradigm Shift in Privacy Research

In today's digital age, information privacy has emerged as a critical social and cultural issue spanning space, time, and technology (Acquisti et al., 2022). As a testament to its urgency, over 160 countries have now enacted regulations to address this pressing matter (Greenleaf, 2023). Privacy is a multidimensional concept and refers to an individual's ability to control when, how, and to what extent their personal information is used by others (Altman, 1977). Global statistics affirm that over 90% of data breaches are attributed to human error, particularly disclosures of sensitive data (e.g., passwords) (Kelly, 2017). This highlights that misguided privacy decisions are a significant root cause of the escalating cybersecurity crisis, imposing severe repercussions on consumers, organizations, and even entire societies and countries, which manifest as both tangible (e.g., identity theft, stock value dip, cyberwar) and non-tangible (e.g., feelings of insecurity and stress) costs. Despite more than two decades of rigorous privacy research examining the primary issues at both individual and organizational levels (Acquisti et al., 2015; 2020; Smith et al., 2011), we have only scratched the surface of the privacy iceberg. As we stand only 20 years into the actual digital era, a new paradigm shift in privacy research and practice is urgently needed to address future complexities and catastrophes.

The new paradigm should foster a synergistic approach, integrating insights from a myriad of fields — including but not limited to information systems, behavioral economics, computer science, marketing, law, communications, anthropology, and sociology, as well as hard sciences like physics and neuroscience — reflecting the pervasive nature of data privacy issues across all disciplines. The goal is to develop a theory that is both straightforward and nuanced to significantly advance future privacy science and enhance individual and organizational privacy practices through Privacy Education, Training, and Awareness (PETA) programs (Alashoor, 2024). This is particularly vital for upcoming generations, who, with their extensive digital footprints, can metaphorically "travel back in time" through their online histories. Indeed, the last two decades have seen a reality where, thanks to social

media, mobile phones, and smart devices, people can easily revisit past digital traces and interactions. However, this capability has also unveiled a puzzling scientific observation, often termed the 'privacy paradox' (Kokolakis, 2017).

The privacy paradox illustrates the discrepancy between individuals' stated privacy preferences and their actual online sharing behavior (Alashoor et al., 2023b). Building on the existing literature, the GRP posits that this divergence primarily stems from the nuanced interplay of context and time (Dinev et al., 2015; Nissenbaum, 2009; Tucker, 2018; Xu and Dinev, 2022). This is akin to the principles of general relativity where space and time are inseparably intertwined (Einstein, 2003); similarly, in privacy dynamics, context and time emerge as critical interwoven factors. Yet, this gives rise to a pressing concern: while Artificial Intelligence (AI) can analyze historical data at an unprecedented speed, effectively 'time traveling,' its capacity to comprehend the underlying context of the data remains highly dubious, undermining the validity of its predictive power and utility to humans. This limitation could spawn unforeseen socio-technical, economic, ethical, and political challenges, posing substantial threats to consumers, organizations, and nations. Such a development would be detrimental, especially given the existing biases evident in today's algorithms (Caliskan et al., 2017). This research aims to chart a new course in this space, advocating for a deeper, interdisciplinary exploration into what is coined the *general relativity of privacy*.

In essence, privacy revolves around the regulation of personal boundaries (Petronio, 1991), and the decision to share or protect personal information is pursued to derive meaning and value from private data (Alashoor 2024; Alashoor et al., 2023a). The perceived value - whether economic, social, or emotional - from any privacy decision is guided by a *privacy calculus* (Dinev and Hart, 2006). This socio-economic mental model posits that privacy decisions hinge on the expected benefits and costs of the behavioral outcome, such as sharing or protecting personal information. If not executed carefully, it can potentially lead to a cybersecurity crisis (e.g., sharing a password with an untrusted party) or significantly impede necessary operations (for instance, being overly cautious can result in missed opportunities for networking, collaboration, and innovation). The privacy calculus has propelled advancements in theory and practice but is susceptible to a myriad of biases and heuristics (Acquisti et al., 2020; Dinev et al., 2015). More importantly, it is limited in terms of highlighting the significant role of context and time, which together dictate the meaning and value of any privacy decision. This lays the foundation for the GRP, where the value and meaning of privacy (e.g., personal data) are shaped by contextime.

Just as Niels Bohr redefined the realm of physics by illustrating that light behaves as neither a particle nor a wave until observed (Bohr, 1928) - a metaphor illuminating how undisclosed information (e.g., personal data) can alter our perception of the world - the GRP posits that the true essence and value of privacy remain undefined until reconceptualized within the boundaries of 'contextime'. In the scientific realm, this theory could shed new light on the still unsolved questions within the behavioral economics of privacy, possibly paving the way for a new economic world order where personal data takes center stage as a form of 'tangible' digital currency.

References

Acquisti, A., Brandimarte, L., and Hancock, J. (2022). "How privacy's past may shape its future," *Science* 375 (6578), 270-272.

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). "Privacy and human behavior in the age of information," *Science* 347 (6221), 509-514.

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2020). "Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age," *Journal of Consumer Psychology* 30 (4), 736-758.

Alashoor, T. (2024). "It is seriously time for privacy education, training, and awareness (PETA) programs," in James, B. & Robles, M. (eds.) *Effective Methods for Teaching Business Related Topics During and Post Crisis*, National Business Education Association.

Alashoor, T., Aldawood, H., Alsulayyim, B., Almutairi, S., and Alotaibi, E. R. (2023a). An online randomized field experiment on the importance of privacy education, training, and awareness (PETA). In *Proceedings of the 3rd International Conference on Computing and Information Technology IEEE*, Tabuk, Saudi Arabia.

Alashoor, T., Keil, M., Smith, H. J., and McConnell, A. R. (2023b). "Too tired and in too good of a mood to worry about privacy: Explaining the privacy paradox through the lens of effort level in information processing," *Information Systems Research*, 34 (4), 1415-1436.

Altman, I. (1977). "Privacy regulation: Culturally universal or culturally specific?" *Journal of Social Issues* 33 (3), 66-84.

Caliskan, A., Bryson, J. J., and Narayanan, A. (2017). "Semantics derived automatically from language corpora contain human-like biases," *Science* 356 (6334), 183-186.

Dinev, T., and Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* 17 (1), 61-80.

Dinev, T., McConnell, A. R., and Smith, H. J. (2015). "Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research* 26 (4), 639–655.

Einstein, A. (2003). *The meaning of relativity, four lectures delivered at Princeton University, May 1921*. Routledge.

Greenleaf, G. (2023). "Global data privacy laws 2023: 162 national laws and 20 bills. *Privacy Laws and Business International Report* 181, 2-4.

Kelly, R. (2017). *Almost 90% of cyber attacks are caused by human error or behavior*. URL: https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security* 64, 122-134.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Petronio, S. (1991). "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples," *Communication Theory* 1 (4), 311-335.

Smith, H. J., Dinev, T., and Xu, H. (2011). "Information privacy research: An interdisciplinary review," *MIS Quarterly* 35 (4), 989-1015.

Tucker, C. (2018). *Privacy, algorithms, and artificial intelligence*. National Bureau of Economic Research, Inc., 423–437.

Xu, H., and Dinev, T. (2022). "Reflections on the 2021 impact award: Why privacy still matters," *MIS Quarterly* 46 (4), xx–xxxii.