



© Photo Fotosphaere-AdobeStock

E. European Impact

Personal data breaches: why certain individuals are victims, while others act. The role of cultural preferences.

ESCP Impact Paper No.2023-17-EN

Christelle AUBERT HASSOUNI, Sandrine MACÉ & Béatrice PARGUEL
ESCP Business School

[Personal data breaches: why certain individuals are victims, while others act. The role of cultural preferences.

Christelle Aubert Hassouni*

Sandrine Macé**

Béatrice Parguel***

ESCP Business School

Abstract

Respect for privacy is a much-explored topic in recent studies on the impact of new technologies on consumers, employees and citizens. Most of these studies have taken an attitudinal rather than a behavioural approach, examining concerns as opposed to responses. This paper, a synthesis of thesis research by Christelle Aubert-Hassouni, presents the responses to personal data breaches, and explores the impact of cultural preferences. While the legal means for the protection of personal data (consent, complaint, withdrawal or deletion of data) are based on an individual interest in protecting one's privacy, this study demonstrates that there are cultural preferences influencing other actions, such as concern for others (values of tradition and social equality). It also highlights the limits to an over-individualisation of these means and the advantage of more collective actions led by regulatory authorities and companies.

Keywords: New technologies, Privacy concerns, Data breach, Culture

* Ph.D., ESCP Business School

** Professor, ESCP Business School

*** Research Director, CNRS, PSL, DRM

ESCP Impact Papers are in draft form. This paper is circulated for the purposes of comment and discussion only. Hence, it does not preclude simultaneous or subsequent publication elsewhere. ESCP Impact Papers are not refereed. The form and content of papers are the responsibility of individual authors. ESCP Business School does not bear any responsibility for views expressed in the articles. Copyright for the paper is held by the individual authors.

Personal data breaches: why certain individuals are victims, while others act. The role of cultural preferences.

The lack of trust in privacy protection is one of the main barriers to the adoption of connected objects or other services using personal data. The General Data Protection Regulation (GDPR), which came into effect in Europe in May 2018, provides a regulatory framework and strengthens the protection of individual rights. Companies strive to reinforce the security of their customers' and employees' personal data, and yet data breaches¹ are on the rise. Estimated at \$4.82 million on average (IBM, Cost of a Data Breach, 2022)², the financial cost of data breaches is growing. This cost includes loss of turnover and the time employees spend recovering data. It does not include the indirect cost linked to individuals' responses (customers or employees), owing most likely to a lack of understanding of these forms of behaviour and their consequences.

The aim of this paper is to present the various types of response to data breaches and their main antecedents. The role of cultural preferences is explored in depth.

This paper is based on thesis research by Christelle Aubert-Hassouni, defended on 13 April 2023, under the supervision of Professors Macé and Parguel. Three complementary studies were led, each exploring a level of observation: macro (institutional - national culture), meso (social - membership of a sub-group sharing the same values), and micro (psychological - individual cultural preferences).

Varied responses to data security breaches

In the event of a data breach, how do you personally respond? Are you among the majority of people who suffer in silence? Or, on the contrary, do you apply technical measures for security (e-mail encryption, use of a VPN)? More radically, do you decide to stop using certain online services? Or to transmit false information (Son and Kim, 2008)?

Perhaps you share your unfortunate experience with your family or friends and/or on social media, to tell your story, express your annoyance and warn of the shortcomings of an organisation or business? Are you even more involved, through your collective actions with organisations such as None of Your Business led by Marx Shrems?

Or are you among those who expect compensation and act alongside institutions by filing a complaint with administrative bodies (e.g. the CNIL in France), or initiating individual or collective (class action) legal proceedings?

There is a wide range of responses to personal data breaches. The intensity of these responses varies. They can take technical, social or institutional forms. Their common denominator is that they weaken the company/organisation in the medium-to-long term. Companies and organisations see institutional actions as the most costly and dangerous (fines and legal expenses). This is arguably an erroneous view. Social actions are insidious; starting with social networks, they spread customer / patient / user / employee dissatisfaction, and contribute to damaging a company's most precious asset, its image and reputation. As for technical responses to data breach, they result in a collection of erroneous

¹ Data breach is defined by the GDPR as security incidents, of malevolent origin or otherwise, which compromise the integrity, confidentiality or availability of personal data.

² <https://www.ibm.com/security/data-breach>

data, or the absence of the latter, which in turn compromises algorithmic quality and thus marketing efficiency in terms of recommendation or customisation.

The profile of individuals with the greatest tendency to respond to data breaches.

Why do certain victims of data breach take action? Why do others simply suffer the consequences? Previous studies in the field of associated research, i.e. consumer complaints (Sahli, 2021; Cri , 2003; Gr goire et al., 2009), or concerns for respect of privacy (Labrecque, 2021), outline the characteristics of an individual likely to respond in the event of a personal data breach.

They are young (student or worker under the age of 35), with a good level of education and a certain degree of proficiency in digital technology. The negative emotions triggered by the data breach, the stress, frustration or humiliation experienced because the moral contract between the company and this individual was not respected, incite the person to act. The greater the importance this person gives to their online privacy, the more they believe their complaint will benefit others by preventing further victims (societal benefits), and the more active they will be when the company is at fault.

Some of these characteristics were confirmed in the research led by Christelle Aubert-Hassouni. Others, such as cultural preferences, add to this profile.

Does belonging to a culture influence the type of response?

The variability between European countries in terms of both the number of complaints filed with the authorities and the amount of fines imposed (DLA Piper GDPR fines and data breach survey)³ may be explained by cultural effects which are specific to each country: attitude to the law, institutional trust, notion of individual responsibilities, perception of complaint, concern for one's privacy, and attitude to risk, security or vulnerability.

Hofstede's national culture models (Hofstede, 2001) and individual cultural preferences (Sharma, 2010) were used to study the impact of cultural preferences on responses to data breach. Three studies were led: the first collected macro data on the number of complaints per European country and Hofstede's cultural dimensions (<https://www.hofstede-insights.com>); the second analysed the content of 15 interviews with individuals actively engaged in privacy protection, and the third study consisted of an online survey of 452 respondents. The three studies confirm the impact of culture on the form and intensity of responses, with cultural preferences appearing to carry a predominant weight. This shall be discussed below.

Individualism: a key factor in the response to data breaches.

Further to other studies (e.g. Miltgen & Peyrat-Guillard, 2014), the aforementioned 3 led on macro, meso and micro levels confirm the role of a key variable, i.e. individualism.

The 2 meso and micro studies reveal that the more individualist the person, i.e. the more this person demonstrates a preference for autonomy, independence and individual freedom characterised by the protection of their own goals and interests (Hofstede, 2001),

³ <https://www.dlapiper.com/en-au/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023>

the greater their tendency to act individually and collectively in the event of a personal data breach.

Through adhesion to national culture, the inhabitants of so-called individualistic countries (e.g. UK, Denmark or Sweden) apparently believe that each person has the right to defend their privacy. They are more likely to understand the implicit norms of control, transparency and trust which form the basis of the social contract (Martin, 2016) regulating personal data use and sharing. The results of the macro study demonstrate that in countries promoting individualism, the number of complaints filed with local regulatory bodies is significantly higher.

How are these results to be built on? In more individualist countries, it is easier for local regulatory authorities to accomplish their task. Given the more fluid nature of expression and action, their task is thus to facilitate access for all to reporting and legal recourse, via information campaigns and support measures (on and offline, etc.). However, the companies at the origin of the data breach must be highly vigilant in this type of country, given the risk of social and collective actions where individuals share their criticisms with their physical circle and on social networks. The reputation of the firm is at stake. It is in the best interest of these companies, who are obliged to report any data breach to the regulator within 72 hours, to develop seamless, transparent communication by providing their customers with all necessary information to channel and coordinate their actions.

‘All for one and one for all’. Acting for the protection of privacy is also a social practice.

The protection of privacy is not only a matter of individualism, however. There are also petitions (such as that by the Quadrature du Net in May 2018), group actions (e.g. by None of Your Business, which led to the invalidation of the Privacy Shields in July 2020), and class actions (such as that led against Oracle in August 2022 by the Irish regulator in association with specialised lawyers and experts in privacy). These class actions demonstrate that implication in the protection of individual rights goes beyond personal interests. India, whose political model is less influenced by the individualism of 18th-century Western philosophy, notably challenged Meta twice: in 2016 by refusing the free internet offer Facebook Free Basics, and in 2020 when it summoned the firm's representatives before parliament to clarify the risks of Facebook's meddling in the 2019 legislative elections.

In fact, other ideals, such as the care and attention given to others, or the protection of social equality for all, irrespective of gender, origin and vulnerability, are key grounds for action to protect privacy. The protection of each person's freedom implies upholding the freedom of all.

In the macro study, we thus find that the number of individual complaints to regulatory authorities for data breach is higher in European countries promoting femininity (Hofstede, 2001), i.e. in countries such as Sweden or Norway where the principles of equality predominate (e.g. gender equality and community care). On a more micro and individual level, a preference for social and gender equality makes the risk of data breach more concrete, and thus encourages people to be more active in the event of a proven breach of personal data.

This result is corroborated and enhanced by the qualitative study on the meso level examining the motivational values of groups and communities acting for privacy protection. In considering the protection of privacy as a social rather than individual practice

(Bourdieu, 1972), the interviews reveal that the protection of social equity is a fundamental reason for action to protect personal data. 'All for one and one for all' to protect a common asset and thus the most vulnerable populations in terms of privacy (e.g. journalists, people suffering from illness, or abused women).

The notion of a social practice in the protection of privacy is particularly significant at a time when the entire sector is organising itself, when stakeholders are acting for the development of a digital civic and economic life which respects our societies, but also in a context where it is rarely in the interest of companies to highlight their vulnerability to highly frequent cyberattacks. These social practices enable each individual to develop and share a technical and IT culture, helping each citizen to become a responsible user of technologies and a counterforce to companies, in the hope that all people will soon be protected and no longer need to act.

Conclusion

By examining cultural preferences and their impacts on responses to personal data breach, we further our understanding of concerns for privacy protection. Therefore, concern for the protection of one's privacy does not mean simply controlling one's own data, but securing everyone's personal data. Like other researchers (Cardon, 2019), we call on all stakeholders, companies, regulatory authorities, consumers, employees, etc. to consider the protection of privacy as an 'advantage for the community' and not 'an advantage for oneself'.

References

- Aubert-Hassouni, C. (2023). Influence de la culture sur les réponses face à une violation de données personnelles. Thèse de doctorat, École doctorale de Management Panthéon-Sorbonne (Paris), en partenariat avec ESCP Business School.
- Bourdieu, P. (1972), « Esquisse d'une théorie de la pratique », Librairie Droz.
- Cardon, D. (2019), « Culture numérique ». SciencesPo les presses.
- Crié, D. (2003). Consumers' complaint behaviour. Taxonomy, typology and determinants: Towards a unified ontology. *Journal of Database Marketing & Customer Strategy Management*, 11(1), 60-79. <https://doi.org/10.1057/palgrave.dbm.3240206>
- Grégoire, Y., Tripp, T. M., & Legoux, R. (2009). When Customer Love Turns into Lasting Hate: The Effects of Relationship Strength and Time on Customer Revenge and Avoidance. *Journal of Marketing*, 73(6), 18-32.
- Hofstede, G. (2001). « Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations ». SAGE Publications.
- Labrecque, L. I. (2021). When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. *Journal of Business Research*, 135, 559-571.
- Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, 137(3), 551-569.
- Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103-125. O.I. <https://doi.org/10.1057/ejis.2013.17>

Sahli, A. B. (2021). When dissatisfied customers express revenge online: Who are they and how do you deal with their complaints? *Décisions Marketing*, 102(2), 247-264.

Sharma, P. (2010). Measuring personal cultural orientations: Scale development and validation. *Journal of the Academy of Marketing Science*, 38(6), 787-806.
<https://doi.org/10.1007/s11747-009-0184-7>

Son, J.-Y., & Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, 32, 503-529.
<https://doi.org/10.2307/25148854>