Corporate Data Collection, Moral Panic, and Consumer Privacy

People use online services for shopping, learning, getting news, and keeping in touch. Every scroll and purchase is recorded by companies (Acquisti et al., 2015). These records are assembled into profiles for advertisement, recommendations, and personalization (Graeff & Harmon, 2002). There is considerable evidence, from studies of loyalty cards and direct marketing, of strong concerns about personal data collected by companies, especially when finances or location enter company databases. Work in economics has documented increasing resistance to providing income information in online surveys, suggesting an increasing privacy concern over time. A common pattern in public debate today is the view that corporate tracking is literally surveillance. Thus, the research question is to determine if fears of corporate data collection constitute a moral panic that is changing how consumers perceive privacy risks and consent. The answer to this question will be provided by analyzing two information literacy frames.

Information literacy frame 1: information has value

The Association of College & Research Libraries' (ACRL) frame "information has value" presents information as a commodity, a tool for influence, and an object subject to legal and ethical rules (Association of College & Research Libraries, 2015). Personal data gathered by corporations in online services fit this description. Marketing research indicates that companies use names, addresses, demographic profiles, and purchase histories to shape their offers and loyalty programs, while studies report a high level of concern about personal information, particularly about financial information and unique identifiers, and less about basic contact information (Phelps et al., 2000). Consumers associate different levels of sensitivity to different

kinds of information, then react with selective sharing, and requests for limits or redress when practices are perceived to be unfair.

A clear example of this value can be found in Timothy Greaff and Susan Harmon's study of grocery loyalty cards and tracking (Graeff & Harmon, 2002). By swiping their cards, shoppers receive discounts, but most have no idea how the stores connect these purchases to long-term profiles. According to the survey, there are concerns around privacy and weak understanding of data collection during ordinary shopping (Graeff & Harmon, 2002). This combination gives personal data a mixed status. Companies profit economically from it, while consumers feel some loss but do not have a clear understanding of what is going on in the background.

Beyond these marketing examples, behavioral privacy research helps extend this frame to a more general range of online services. Alessandro Acquisti and colleagues review studies indicating that there is a gap between what people say and what they disclose in specific situations (Acquiti et al., 2015). Disclosure choices are influenced by context, framing and system defaults. In this vein, Zhuo Sun and colleagues analyze more than one hundred privacy studies, and group influence on privacy decisions into factors related to individuals, types of information, organizational practice, interface design, and rules of interaction (Sun et al., 2024). The outcomes vary between trust and repeat use to resistance, fatigue, and retreat from digital spaces. Under the "information has value" frame, moral panic seems to appear when the debate treats personal data only as something corporations take advantage of, rather as a resource people value, trade, and protect through demands for transparency, consent, and accountability. This perspective reveals uneven bargaining over the usage of data.

Information literacy frame 2: authority is constructed and contextual

The ACRL frame “authority is constructed and contextual” views authority as something that is granted in very specific social communities and situations, rather than being a fixed badge across context (Association of College & Research Libraries, 2015). The debate about corporate collection of data in online services follows the same pattern. Technology companies, regulators, journalists and advocacy organizations all describe themselves as protecting users, but each of them has a different view of what is at risk. Corporate statements focus on personalization and internal programs; advocacy groups are concerned with opaque tracking, data brokerage and profiling; regulators put all the emphasis on privacy laws compliance and visible enforcement actions.

To see how these claims to authority work in practice, research on moral panic around technology shows how different voices influence public reaction. Alice Marwick examines the “MySpace moral panic,” and argues that news coverage and political speeches in the mid-2000s exaggerated the dangers of social networking sites and contributed to the justification of restrictive policies targeted at youth (Marwick, 2008). James Walsh goes through social media and outlines trends in which the headlines of addiction, misinformation, or even crime tend to shadow the normal use (Walsh, 2020). In these cycles, political actors claim authority as protectors, while blame is attributed to platform operators as careless or cynical.

A related pattern can be seen in Michael Levi and David Wall’s analysis following the September 11, 2001, attacks which is centered on security and surveillance (Levi & Wall, 2004). Governments and security services promoted databases and monitoring systems with language that stressed threats and urgency. Data protection rules and proportionality tests did, however, still put limits on many proposals and created legal obligations for oversight. The article reveals

anxiety and moral panic about surveillance tools as the institutional checks continue to operate in the background (Levi & Wall, 2004).

Finally, privacy concern and behavior research fits in this frame. In online surveys, Avi Goldfarb and Catherine Tucker (2012) report that refusal to share income has grown during the 2000s, especially among older adults, which indicates a changing in norms concerning disclosure (Goldfarb & Tucker, 2012). Alessandro Acquisti and colleagues describe the gaps between stated concern and action, as influenced by choice framing and default setting (Acquisti et al., 2015). Under conditions of low trust, audiences give alarmist accounts more authority, treat many tracking practices as one type of threat and pay less attention to legal and design protections.

Conclusion

Across both frames, research on corporate data collection in online services gives a mixed answer to the research question. Studies in marketing and behavioral privacy report a high degree of concern for personal data, and low awareness of tracking systems and trade-offs where people provide information in return for convenience, discount or social connection (Phelps et al., 2000; Graeff & Harmon, 2002; Acquisti et al., 2015; Sun et al., 2024). Economic research shows growing reluctance to report income in online surveys, which points to a general discomfort with long-term use of personal information (Goldfarb & Tuker, 2012). These highlight valid concerns about harm and fairness.

Research on moral panic and authority help to understand the extent to which fear is not limited to real, concrete risks. The “information has value” frame is used to present data as an asset for negotiation: one side in the market, especially firms, tries to monetize it, while the other, representing consumers, tries to gain benefits and protection. The “authority is constructed and contextual” frame exposes confrontation over the question of which actors should be trusted

in privacy debates, since stories of harm are promoted by firms, regulators, and advocates (Association of College & Research Libraries, 2015; Marwick, 2008; Levi & Wall, 2004; Walsh, 2020). Moral panic sets in when alarmist narratives reduce the difference between intensive surveillance and everyday use of data. Evidence from the different sources cited above suggests that the depiction of corporate data collection as overwhelmingly harmful is exaggerated, but also indicates gaps in transparency, consent, and oversight, which is a call for reform and better communication.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Association of College & Research Libraries. (2015). *Framework for information literacy for higher education*. Association of College & Research Libraries (ACRL). https://www.ala.org/acrl/standards/ilframework

Goldfar, A., & Tucker, C. (2012). Shift in privacy concerns. *American Economic Review, 102*(3), 349-353. https://doi.org/10.1257/aer.102.3.349

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4), 302-318. https://doi.org/10.1108/07363760210433627

Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post-9/11 European information society. *Journal of Law and Society, 31*(2), 194-220. https://doi.org/10.1111/j.1467-6478.2004.00287.x

Marwick, A. E. (2008). To catch a predator? The MySpace moral panic. *First Monday, 13*(6). https://doi.org/10.5210/fm.v13i6.2152

Phelps, J., Nowak, G., & Ferrel, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41. https://doi.org/10.1509/jppm.19.1.27.16941

Sun, Z., Pan, G., Yang, R., Zang, G., & Zhou, J. (2024). Consumer privacy decision-making in digital era" An integrative review and taxonomy. *Aslib Journal of Information Management. Advance online publication*. https://doi.org/10.1108/AJIM-12-2023-0526

Walsh, J. P. (2020). Social media and moral panics: Assessing the effects of technological change on societal reaction. *International Journal of Cultural Studies, 20*(6), 840-859. https://doi.org/10.1177/1367877920912257