



Information Research – Vol. 31 No. ISIC (2026)

Information is a gun: recognising information facilitated interpersonal harms

Yimin Chen and Dana McKay

DOI: <https://doi.org/10.47989/ir31ISIC65256>

Abstract

Introduction. With the growing popularity of smart technologies, sensitive and personal information has never been more abundant or accessible, but this information can be readily abused to perpetrate interpersonal harms. However, discussion of the role of information in these harms is largely absent from the Library and Information Science (LIS) literature. We argue that a disciplinary belief that ‘*information wants to be free*’ has created a gap in LIS research about the ways in which information can be weaponised to facilitate interpersonal harm.

Method and analysis. We summarise research from privacy, cybersecurity, and other computing disciplines that examine cases of information facilitated interpersonal harm and demonstrate that access to information was an enabling factor in each case. We also performed keyword searches in the LISA database for terms relating to interpersonal harm and found few results relating to the role of information collection and access in interpersonal violence and abuses.

Conclusion. The LIS community could contribute vital expertise to the study of information facilitated interpersonal harms if we reconsider our assumption that greater access to information is a social and public good.

Introduction

'oh, better to be anything than America as a gun.'

~ Brian Bilston

In February of 2016, the pseudonymous British poet Brian Bilston posted a poem entitled *America is a gun* to Twitter (Bilston, 2016). In it, Bilston lists symbols of various countries in simple rhyming quatrains, starting with *'England is a cup of tea,'* but always ending with the rhyme-breaking refrain: *'America is a gun.'* The inspiration for the poem, according to Bilston, was a tweet by then-Florida governor Jeb Bush—a photo of a handgun engraved with his name and the caption: *'America'* (McKernan, 2016). Just days later, there was a mass shooting in Kansas. Just months later, the Pulse nightclub shooting in Florida became the deadliest mass shooting in US history.

In the years since, Bilston's poem has been shared countless times on social media to mark the occurrence of mass shootings in the United States and as commentary on that nation's firearm obsession. Some have criticised the poem for being overly simplistic, pointing out the many positive symbols that could also represent America and the fact that other countries have shameful aspects of their cultures, too. But, of course, the purpose of Bilston's poem is not to make a comprehensive representation of all a country's virtues and vices, but to forcefully draw our focus to one urgent problem: the danger of gun violence in the United States. Similarly, our purpose in this paper is not to claim that information is literally a gun, but to draw focus to an urgent problem that has, thus far, received little attention in Library and Information Science (LIS): how information systems, specifically the unprecedented access to information they provide, can be used to enact interpersonal harms.

The second amendment to the United States constitution has been interpreted by many American firearms advocates as codifying a nigh-unlimited natural right to gun ownership (Barr, 2021). To draw a parallel, the *second amendment* of LIS may as well be Stewart Brand's aphorism that *'information wants to be free'* (Levy, 2014). In much the same way that many Americans feel entitled to their guns because they consider themselves responsible users, people often feel that they are entitled to access and use information because they consider themselves to be responsible users. The LIS discipline tends to implicitly consider the free access to information as an unalloyed good; our intent, in comparing information to firearms, is to argue that it is not.

What does it mean for information to be a gun?

Advocates for the National Rifle Association and gun rights activists hold that guns are tools; that *'guns don't kill people; people kill people'*. This is, of course, a banal truism, but its purpose is to obscure the fact that it is the interaction between guns and people that causes harm. Furthermore, certain design features of firearms, including semi-automatic firing and high-capacity magazines, enable faster delivery of more bullets and therefore amplify the capacity for serious harm (Koper, 2020). Similarly, we argue that the design of consumer information technology, including social media platforms, mobile apps, and smart home devices, enables greater collection and delivery of data, which then facilitates and even encourages abuse. We detail some of these information abuse cases below, demonstrating that interpersonal harm is perpetrated through information access and misuse.

Information facilitated interpersonal harm

In their review of sociotechnical harms in the Human Computer Interaction literature, Shelby et al. defined *interpersonal harms* in this context as those which *'adversely shape relations between people or communities'* (2023), such as instances of technology facilitated violence and invasions of privacy. Indeed, technology facilitated violence and abuse has increasingly been recognised as a growing social problem (Gupta et al., 2024), but we contend that it is the information collected, processed, and surfaced through these technologies that facilitates the ability for one person to

enact harm upon another. It is this direct, intentional, and often individualised nature of information facilitated interpersonal harms that distinguish them from other types of informational harms, which may be unintentional, such as misinformation, or broadly directed, such as mass media propaganda and malinformation.

Privacy experts have noted that instances of interpersonal harm are often situated in a narrative of care (Levy & Schneier, 2020) and feminist cybersecurity scholars raised similar concerns about intimate threats (Slupska, 2019). Justice scholars have looked at the normalization of extensive information sharing practices (Butler et al., 2024) and health scholars have examined the harm caused by abuse of these technologies (Brown & Hegarty, 2024; Brown et al., 2021). Human computer interaction and design scholars have also suggested *safety by design* as a potential remedy (McKay & Miller, 2021; Sambasivan et al., 2019). Numerous interpersonal informational threats have been identified through this research; we focus here on three: stalkerware, parental monitoring technologies, and weaponization of internet of things.

Stalkerware

A comprehensive 2019 report by Parsons et al. (2019) examined the capabilities and marketing of so-called ‘stalkerware’ apps, which have become incredibly prevalent tools in the perpetration of intimate partner violence. Notably, this report found that many of the companies involved in this industry actively promoted their software as covert surveillance tools but failed to make clear what recourse might be available to victims of their products. More recent research has unfortunately confirmed that these products remain readily available and abusable (Bonam et al., 2025). Literature on social media also shows that even software not specifically marketed as stalkerware is regularly leveraged for stalking (Fiolet et al., 2021; Zuboff, 2019).

Parental monitoring technologies

Parents are increasingly using location-tracking apps like Life360 to monitor their children’s activities. While this practice is usually borne out of genuine concern for their children’s safety, studies have raised serious concerns about privacy and security, as well as tensions in the parent-child relationship arising from the availability of tracking data (Mavoa et al., 2023). On the one hand, parents may be anxious about their children moving toward independence, and on the other hand, the mere existence of location information imposes social obligations on parents to know more about their children’s lives (Lupton, 2020).

Weaponization of internet of things

The potential for information available from smart homes built from consumer electronics to facilitate coercive control has previously been raised by McKay and Miller (2021). Work by Stephenson et al. (2023) identified common abuse vectors for internet of things and more recently, Brown et al. (2025), analysed the abusability of 13 consumer internet of things devices available in Australia, including smart doorbells, fitness trackers, and an air conditioner. The authors identified seven types of internet of things design features that could facilitate misuse, including weak user profile protections, limited recording of access logs, and lack of clear activity indicators, and noted that a *safety by design* approach could significantly curb potential abusability.

In each of these examples, access to and exploitation of information provided by devices and apps was the enabling factor that facilitated the perpetration of interpersonal harms. However, much of this work has focused solely on technology and technological solutions to this problem, rather than on the information itself.

A blind spot within LIS

The LIS literature has traditionally paid significant attention to information needs, with some authors even arguing that information needs should be included as a primary need in Maslow’s hierarchy—on the same level as food and shelter (Cole, 2025). However, there has been little

discussion about when information should be withheld, except in the context of privacy. Even so, this discourse is generally framed around preventing the misuse of sensitive data by institutions (Cervone, 2016), rather than on interpersonal harm. This oversight may be because feminist conceptions of interpersonal privacy are considered niche, rather than normative (Slupska, 2019). By contrast, computing disciplines like cybersecurity and human-computer interaction have been concerned with the use of information technology in perpetrating intimate threats or domestic and family violence for over a decade (Dimond et al., 2011). There is also the concept variously known as *safety by design* or *prevention through design*, which emphasises anticipating and proactively mitigating potential technological threats during development, rather than as an afterthought (Brown et al., 2025).

Searches conducted in the LIS database *Library & Information Science Abstracts* (LISA) for peer-reviewed articles using the keywords ‘intimate threats’ (0 hits), ‘safety by design’ (1 hit), and ‘interpersonal violence’ (9 hits) in their abstract and summary text reveal that these terms are all but non-existent in the LIS literature. While related terms like ‘intimate partner violence’ (44 hits) do appear, much of this literature is focused on supporting the information needs of survivors of violence and technology-based interventions rather than on investigating the role of information in facilitating interpersonal violence. Despite the demonstrable role that information access plays in the perpetration of interpersonal harms, LIS researchers do not seem to have substantively engaged with this topic yet. Perhaps, like second amendment gun rights advocates, could the discipline’s preoccupation with information access have led us to turn a blind eye to legitimate reasons why information needs ought to be denied?

Conclusion

LIS has long concerned itself with how people gain access to information and, as a discipline, we have predominantly considered greater access to information a social and public good. In this paper, we demonstrate that information ought to be treated with more care, showing it to be strongly implicated in digital interpersonal harms. Previous attempts to address such harms in other disciplines have predominantly focused on perpetrators or technologies, rather than examining the information flows as a possible mechanism for intervention. Surprisingly, information science has largely been absent from these discussions. The understanding of information flows, uses, and impacts that LIS could bring might be key to solving this problem, but we will need to reconsider our position that more access to information is necessarily better. It is time for us, as a field, to recognise the myriad ways in which information in the wrong hands is, indeed, a gun, and work towards a solution.

About the authors

Yimin Chen is a Lecturer (Assistant Professor) in Interaction Technology and Information at RMIT University. His research focuses on the prevention of online gender-based violence through technological and social interventions. Yimin can be contacted at yimin.chen@rmit.edu.au

Dana McKay is an Associate Professor and Inaugural Associate Dean at RMIT University, Australia, leading the Interaction, Technology and Information Discipline of the School of Computing Technologies. Dana has been studying information interaction for twenty-five years in both professional and academic contexts; she was jointly awarded the Association of Information Science and Technology 2024 Lois Lunin Award. Dana can be contacted at dana.mckay@rmit.edu.au

References

- Barr, B. (2021, February 1). *Conservative defense of the Second Amendment falls short: Needs-based defense no longer sufficient to preserve citizens' right to self-defense*. The Heritage Foundation. <https://www.heritage.org/firearms/report/conservative-defense-the-second-amendment-falls-short-needs-based-defense-no-longer>
- Bilston, B. (2016, February 18). *America is a gun*. Facebook. <https://www.facebook.com/photo.php?fbid=1267219516628496&set=a.410535654447489&id=100064731724463>
- Bonam, M., Rayavaram, P., Abbasalizadeh, M., Lee, C. S., Pattavina, A., & Narain, S. (2025). Current research, challenges, and future directions in stalkerware detection techniques for mobile ecosystems. In *The 11th International Conference on Information Systems Security and Privacy*. <https://doi.org/10.5220/0013371700003899>
- Brown, A., Harkin, D., & Tanczer, L. M. (2025). Safeguarding the “internet of things” for victim-survivors of domestic and family violence: Anticipating exploitative use and encouraging safety-by-design. *Violence Against Women*, 31(5), 1039-1062. <https://doi.org/10.1177/10778012231222486>
- Brown, C., & Hegarty, K. (2024). Fear and distress: how can we measure the impact of technology-facilitated abuse in relationships? *Social Sciences*, 13(1), 71. <https://doi.org/10.3390/socsci13010071>
- Brown, C., Sanci, L., & Hegarty, K. (2021). Technology-facilitated abuse in relationships: Victimization patterns and impact in young people. *Computers in Human Behavior*, 124, 106897. <https://doi.org/10.1016/j.chb.2021.106897>
- Butler, L. C., Fissel, E. R., Graham, A., & Fisher, B. S. (2024). “If you have nothing to hide it shouldn't be a problem”: The social construction of cyber abuse and normalized cyber behaviors in intimate relationships. *Victims & Offenders*, 1-26. <https://doi.org/10.1080/15564886.2024.2410991>
- Cervone, H. F. (2016). Information doesn't always want to be free: An overview of regulations affecting information security. *Digital Library Perspectives*, 32(2), 68-72. <https://doi.org/10.1108/DLP-02-2016-0009>
- Cole, C. (2025). An examination of Wilson's concept of information need: Implications. *Information Research*, 30(2), 65-71. <https://doi.org/10.47989/ir30253987>
- Dimond, J. P., Fiesler, C., & Bruckman, A. S. (2011). Domestic violence and information communication technologies. *Interacting with computers*, 23(5), 413-421. <https://doi.org/10.1016/j.intcom.2011.04.006>
- Fiolet, R., Brown, C., Wellington, M., Bentley, K., & Hegarty, K. (2021). Exploring the impact of technology-facilitated abuse and its relationship with domestic violence: A qualitative study on experts' perceptions. *Global qualitative nursing research*, 8, 23333936211028176. <https://doi.org/10.1177/23333936211028176>
- Gupta, N., Das, S., Walsh, K., & Chatterjee, R. (2024, May). A critical analysis of the prevalence of technology-facilitated abuse in us college students. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (pp. 1-12). <https://doi.org/10.1145/3613905.3652036>

- Koper, C. S. (2020). Assessing the potential to reduce deaths and injuries from mass shootings through restrictions on assault weapons and other high-capacity semiautomatic firearms. *Criminology & Public Policy*, 19(1), 147-170. <https://doi.org/10.1111/1745-9133.12485>
- Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1), tyaa006. <https://doi.org/10.1093/cybsec/tyaa006>
- Levy, S. (2014, November 22). "Hackers" and "Information Wants to Be Free". Medium. <https://medium.com/backchannel/the-definitive-story-of-information-wants-to-be-free-a8d95427641c#.y7d0amvr3>
- Lupton, D. (2020). Caring dataveillance: Women's use of apps to monitor pregnancy and children. In L. Green, D. Holloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.) *The Routledge companion to digital media and children* (pp. 393-402). Routledge.
- Mavoa, J., Coghlan, S., & Nansen, B. (2023). "It's about safety not snooping": Parental attitudes to child tracking technologies and geolocation data. *Surveillance & Society*, 21(1), 45-60. <https://doi.org/10.24908/ss.v21i1.15719>
- McKay, D., & Miller, C. (2021, May). Standing in the way of control: A call to action to prevent abuse through better design of smart technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-14). <https://doi.org/10.1145/3411764.3445114>
- McKernan, B. (2016, June 14). This poem about America has taken on new meaning after the Orlando shooting. *Indy100*. <https://www.indy100.com/news/this-poem-has-taken-on-new-meaning-after-the-orlando-shooting-7299716>
- Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., Khoo, C., & Deibert, R. (2019). The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry. <http://hdl.handle.net/1807/96320>
- Sambasivan, N., Batool, A., Ahmed, N., Matthews, T., Thomas, K., Gaytán-Lugo, L. S., Nemer, D., Bursztein, E., Churchill, E., & Consolvo, S. (2019, May). "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In *proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14). <https://doi.org/10.1145/3290605.3300232>
- Shelby, R., Rismani, S., Henne, K., Moon, A., Rostamzadeh, N., Nicholas, P., Yilla-Akbari, N., Gallegos, J., Smart, A., Garcia, E., & Virk, G. (2023, August). Sociotechnical harms of algorithmic systems: Scoping a taxonomy for harm reduction. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 723-741). <https://doi.org/10.1145/3600211.3604673>
- Slupska, J. (2019). Safe at home: Towards a feminist critique of cybersecurity. *St Antony's International Review*, 15(1), 83-100. <https://www.jstor.org/stable/10.2307/27027755>
- Stephenson, S., Almansoori, M., Emami-Naeini, P., Huang, D. Y., & Chatterjee, R. (2023). Abuse vectors: A framework for conceptualizing IoT-enabled interpersonal abuse. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 69-86). <https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-vectors>
- Zuboff, S. (2019). *The age of surveillance capitalism: the fight for the future at the new frontier of power*. Profile Books.

© [CC-BY-NC 4.0](#) The Author(s). For more information, see our [Open Access Policy](#).