THEME ARTICLE: GRAND CHALLENGES

Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety

Angelika Strohmayer, *Northumbria University, NE1 2SZ, Newcastle upon Tyne, U.K.*
Rosanna Bellini, *Cornell Tech, Manhattan, 10044, USA*
Julia Slupska, *University of Oxford, OX1 3JS, Oxford, U.K.*

Designers and developers of pervasive technologies have started to address privacy concerns. However, little work has been done to address the numerous safety concerns for specific social and population groups that fall outside conventional threat modeling based on network-based adversaries. If researchers, engineers, and designers are conscious about concerns for privacy, they must also be considerate of the safety of users of their systems. By using feminist and justice-orientated lenses to technology creation and testing, we present the concept of* safety as a challenge and a hopeful aspiration for pervasive computing. *We present a feminist vision for the future of pervasive technologies that engages with issues of technology-mediated harms to mitigate or aim to eradicate them entirely. By examining two concrete concepts of trust and abusability that will assist on this aspirational journey, we highlight ways to build safer technologies that are grounded in justice and safety for all.

Safety is a basic human need. For our basic rights to be met, we must be able to live in environments free of intolerable risk that is free from violence and the threat of harms, be this self-directed, interpersonal, or collective.[14] A safe digital technology or system, therefore, should work to ensure freedom from the dangers that are posed to its users. While rarely intended from the perspective of well-meaning designers and developers, some technologies generate different experiences of safety for different user groups. Although anyone can be vulnerable and subject to violence, some groups or individuals may face more adversity and vulnerability than others, threatening their wellbeing, their right to self-determination, and ability live a life free of coercion. Consider individuals who must perform "safety work"; mental and physical labor that is used to keep oneself safe, such as determining how to act in a social situation that may vary on the context, person, and time.[6]

With this article, we address these complexities and present the need for a paradigm shift in security research, one that begins to focus on peoples' safety holistically, which builds on current debates in security and privacy (see e.g.., Kaur *et al.*[11]). We demonstrate that the state or process of being safe is highly contextual and subject to many ethical and political dimensions. We seek to encourage critical questions around whose safety is prioritized, how this is achieved, and what means a group has to appeal to greater inclusion in this conversation. *We suggest a paradigm shift is needed; from a focus on security to safety in pervasive computing, which is necessary to meaningfully and proactively protect people who use technologies in our complex world.* To bolster our calls for this shift in focus, we first introduce literature on two types of harm that pervasive technology can cause, before decontextualizing our examples in postdigital ecologies, and proposing the concepts of *trust* and

1536-1268 © 2022 IEEE
Digital Object Identifier 10.1109/MPRV.2022.3182222

abusability as routes to developing safer technologies. We base our argument on extensive collaborative work with safety advocates, marginalized communities, survivors of technology-enabled abuse, and perpetrators of harm over multiple years. These interests converged into a series of two research engagements with safety experts across academia, industry, and the third-sector in the summer of 2021.

Shifting the Paradigm: From Security to Safety

Although often used interchangeably, there is a distinct difference between *safety* and *security*. Security is defined as the protection from deliberate threats (such as an adversary) while safety as the condition of being protected from situations that are likely to cause harm (such as toxic workplace environments). Working toward improved security for individuals may be noble, be this regarding a person's data, property, or identity, but it does not guarantee safety as deftly highlighted by *Our Data Bodies*.[a] Put another way, securing *known* harms may not produce the protection necessary to keep a person safe from bodily, emotional, and psychological harm. We demonstrate this by exploring two examples where the tension between security and safety surface for technology users: 1) the deliberate misuse of technologies to cause harm or "tech abuse"; and 2) use of technologies that causes harm to specific communities as the (un) intended consequences of harmful policy, design, or development practices.

Given the complicated nature of technology-enabled abuse and harm, we argue that traditional approaches to security may not be best equipped to resolve these challenges. Importantly, like all forms of abuse, technology-enabled abuse disproportionately affects those whose identities are marginalized, made vulnerable, or criminalized due to societal structures of oppression. By structures, the arrangement and relationships between complex social systems, we refer to racism, sexism, ableism, heterosexism, and classism; or as bell hooks[9] writes: *"the capitalist imperialist white supremacist patriarchy."* To combat these structures, we must center people's physical, emotional, and financial wellbeing as we move toward a postdigital world. To do so, it is imperative we adopt different ways of looking at the same issue for different communities. Through critical feminist and justice-orientated lenses, we can start from the margins (i.e., by focusing on people made marginal by discrimination or oppression) and take into consideration the unique needs of these communities, making technologies safer for them, and everyone else. Changes to systems to improve accessibility for instance have improved the usability for all users, or even completely changed the use of systems entirely.[7] Feminist security provides us the opportunity to build holistic pictures of understanding our realities that may not be represented solely in technical requirements. It attempts to accomplish a shift in focus to how social relationships (as opposed to external hackers or fraudsters) can be sources of (in)security, and how technology use can inform our understanding of how we relate to others.[10] Taking this feminist approach to focus on safety over security teaches us that technical solutions are only part of the answer for building safer environments for vulnerable groups. Instead, if we examine security in more complicated ways (shaped by our interpersonal relationships, our community experience, and our world), we might start to map and understand technology as one part of a postdigital ecology, a term we go into depth in later sections. Ultimately, looking toward *safety* is a shift from focusing on frequently static entities that require securing toward systems, assets, or ecologies that include or focus on peoples' states of wellbeing.

HARMS OF PERVASIVE TECHNOLOGIES

To illustrate our argument, we introduce two complementary topical examples of technology-enabled harm: technology-enabled abuse in the context of intimate partner violence, and harm caused by algorithmic decision-making processes. Our first case points directly to deliberate harm experienced at an interpersonal level, while our second case covers an institutionalized use of technology in the name of efficiency that may deeply engrain existing inequalities. While we scrutinize these examples in depth, the issue of safety applies to all pervasive technologies and has multiple additional axes of unsafety for people beyond these two cases.

Technology-Enabled Abuse

Intimate partner violence or domestic abuse, refers to behavior used to harass, threaten, intimidate, scare, or otherwise harm someone in a current or former intimate relationship. Despite often being treated as an edge case for developers, in the United Kingdom more

[a]A four-person team working on projects related to how digital information from marginalised communities is collected, stored, and shared by government and corporations in the United States of America. https://www.odbproject.org/2019/01/18/safety-vs-security-are-you-safe-or-are-you-secure/

than one in three women and one in five men will be subject to it in their lifetime.[4] This is in accordance with global estimates that one in three women have experienced physical and/or sexual violence by an intimate partner, and an estimated 38% of femicide committed by former or current intimate partners.[b]

There is a wealth of evidence that demonstrates digital technologies increasingly play a significant role in the harms experienced by victim-survivors: for example, abusers are leveraging the location-tracking capabilities of digital devices for stalking their partners and/or children, using named or anonymous accounts for online harassment, and threatening to disclose private information, such as HIV status or sexual identity.[5] Such actions are made possible through the existence of *dual-use* systems—software that has a legitimate purpose but can be used abusively; such as mapping tools. All of these instances manifest from behaviors that seek to influence the behavior of the person(s) on the receiving end of such attacks. Commonly, experiencing these can make someone feel helpless, isolated, scared, and confused due to the pervasive role of technology in modern life. Importantly, focusing only on resolving the security threats inherent to technology-facilitated abuse may not be effective in ensuring that the victim-survivor feels safe to live their life freely.

In recent years, researchers have explored how interventions can be designed and evaluated that respond to such harms holistically, such as the Technology-Enabled Coercive Control Clinic[c] or the Clinic to End Tech Abuse.[d] Such interventions are time intensive with considerably more initiatives required to meet the demands of technology-facilitated abuse that is set to increase with the further integration of digital systems, particularly pervasive technologies, with the human experience. How we respond to harm perpetrated through digital systems is vital for further investigation. This should include reflections on the role researchers, designers, and developers could play in mitigating or preventing digital risks and harms.

Algorithmic Harms

Algorithms are a sequence of instructions that take one set of inputs to produce a set of outputs—they are cornerstones of digital and computing infrastructures, including pervasive computing. When used to solve complex statistical problems at scale, sometimes they are referred to as machine learning. However, algorithmic decision-making consistently produces negative outcomes for marginalized groups due to incorrect assumptions or inferences regarding data gaps, and hard coded biases about specific populations. As many algorithms are built into proprietary software a black box effect is produced where accountability for bad or even unsafe decision-making is masked and the resource for challenging this is either challenging or implausible.

While making decisions on others' behalf is far from novel, the scale and ubiquity that algorithms now operate at generate novel dangers and risks; amplifying the intensity and capacity for harm. Digital harms thrive in areas that are hard to measure and combat, so introducing a decision-making system that is opaque can work in antithetical ways to ensuring safety for marginalized groups. This is a complex area of study, so we offer this discrete area of focus: YouTube determines the majority of its moderation algorithmically to ensure that videos depicting controversial issues, harmful acts, or sexually suggestive content remain off the platform. As Alkhatib and Bernstein[1] point out, their algorithm was unable to detect seemingly innocuous videos of children's cartoons (e.g., Peppa Pig) spliced with disturbing animated content of torture and death—which can cause harm to viewers. This same algorithm also demonetized LGBT-driven channels due to incorrectly inferencing sex and gender, including strategies for peer support and combating stigma, with sexually suggestive content—which again, can have direct impact on peoples' livelihood. Such strategies that aimed to secure young persons' wellbeing directly impacted on other users' state of safety by having to pivot to other spaces. This link between bias and safety shows that we must consider *power* and its relation to *bias* when designing, developing, and deploying new technologies: this allows us to ask questions not only on what *safety is*, but also *who is involved and has the resources to challenge this state of unsafety?*

If You Care About Security, You Should Care About Safety

As these two examples show, the grand challenge of *safety* that we propose with this article is particularly important for the pervasive community because of the potentially huge impacts that the technologies built in this community have in ensuring or undoing people's postdigital safety. This term was introduced by Coles-Kemp *et al.*,[2] to highlight the importance of realizing the "digital by default" fabric of contemporary society; where a postdigital understanding presents an environment that interweaves digital systems with our everyday realities in a way where they become

[b]https://www.who.int/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence
[c]https://newbegin.org/find-help/staying-safe/technology-safety/
[d]https://www.ceta.tech.cornell.edu/

inseparable and enmeshed. For tech abuse and algorithmic harms, this entails that violence and harm can easily spill into away-from-keyboard contexts; any trauma experienced digitally has physical impacts on our person in a multitude of ways. As such, we must see safety as a postdigital phenomenon and as responsible pervasive computing and security researchers who work in such an environment, it is imperative we: 1) take on a people-centered approach to security in a postdigital world; and 2) that we need to start these approaches from working with people at the margins.

Returning to framing safety in a postdigital ecology, we see it as an aspiration that must be considered when designing novel or adapting existing technologies. Not only does the ecology approach allow us to see connections beyond technologies, it also allows us to look beyond techno-solutionism; as we wrote in a recent toolkit that helps us center peoples' safety in data-intensive technologies[e]:

> *"We want to very strongly refute the thought that if only we are able to design the right kind of technology or the right kind of feature in our data-intensive systems that we are able to make people entirely safe. Rather, we would argue that this technology-centered approach to the abuse of data and data-intensive systems to perpetrate violence against individuals is in itself harmful."*

When we take social, and human, aspects of *safety rather than security* into consideration, it is impossible to "design out" all forms of harm in our digital systems and create perfectly safe systems. Instead, appreciating the difficulties of building safer technologies, and to build in mechanisms to allow for conscious development and adaptation for *when* (rather than *if*) harm is caused by or through our platforms. To help researchers put into practice this genuine appreciation for the potential (rather than erasure) of harm, we present three tenets that we have produced through our research. These represent what a feminist orientation to safety in technology development could be before presenting two useful concepts that pull together our thoughts more precisely: trust and abusability.

FEMINIST ORIENTATION TO SAFETY

Our feminist orientation to safety is grounded in the centering of experiences that are usually written about or dismissed as "edge cases." These are the experiences of people who are marginalized, victimized, criminalized, or folded into traditional categories of the user without critical thought about their unique needs and requirements: women of color, sex workers, incarcerated individuals, and victim survivors of intimate partner violence among others. The orientation is also grounded in our centering of safety throughout the design, development, and deployment of pervasive technologies: how can we center safety in the development of new and the improvement of existing pervasive technologies? Ultimately, the centering of these edge cases and safety must engage with detailed contexts of use and other sociotechnical aspects of pervasive technologies—throughout the product life-cycle from conception to disposal.

We propose the following three assertions that can put into practice our feminist orientation to safety.[f]

1) We must acknowledge and address existing power structures.
2) We must see and understand wider ecologies in which technologies, harm, and support sit, rather than focusing only on the immediate incident.
3) We must be more process-oriented and less outcome-oriented.

If we put these three assertions into practice, we must adapt our processes as we find out more ways in which the technology can be abused—which will ultimately be a continuous cycle of updating. We should to release any technology that is known to be unsafe, but rather restate that it is impossible to design out harms that are caused by pervasive technologies. We can instead put measures in place that reduce the likelihood of this event, and that provide direct avenues for support and change *when* this happens. Questions that then arise are: Who are we responsive to in our adaptation of technologies throughout the design cycle? What measures can we put in place to ensure we are able to respond to issues as they arise? When they arise, how can we make decisions that center the safety of those who are made most vulnerable in society? At the same time, we should also appreciate that sociotechnical pervasive systems become even more complex than they already are when we start to take the safety of people seriously. Yet, sitting

[e]see the Trust and Abusability Toolkit produced by the authors and additional collaborators, which is available at https://nrl.northumbria.ac.uk/id/eprint/47508/

[f]We provide further detail on these in the *Trust and Abusability Toolkit* we produced with additional collaborators, which is available at https://nrl.northumbria.ac.uk/id/eprint/47508/

with this discomfort and appreciating the process of making mistakes is also vital to move forward.

What our feminist orientation teaches us, is that the process of designing new systems or features, and adapting our systems after they are in-the-world can help us be more careful about what we design and the harmful (unsafe) consequences our work can have. In the following, we present two pragmatic concepts, each including several implications for the design of pervasive technologies, that allow us to put into practice this feminist orientation – both integral to understanding how people relate to technologies through the corporations that create them (trust) and peoples' knack to using them as novel tools to cause harm (abusability). The first: *Designing genuinely trust-worthy technologies* presents trust as a dynamic process and how technologies can encourage us to examine new questions about ourselves and our connections with others around this topic. The second: *Designing with abusability* draws on usability research to examine the notion of abusability, or the ability for technologies to be abused. We must consider this throughout design and deployment processes, and should negotiate this with people who use our systems prior to and after it has been deployed.

Designing Genuinely Trustworthy Technologies

Trust, in simple terms, is the exposure of oneself to a situation where the outcome is uncertain.[3] As one of the only certainties in life is further uncertainty, there are few actions that might be performed where there is not some element of trust to consider and examine. This dynamic, contextual interpretation of trust, makes it highly compatible for our investigation into wider scrutiny around states of safety and unsafety as it is highly contextual and impacted by things which are *unknown* (unlike security that requires insight into known threats). The harms that are caused by technologies, such as in our cases of intimate partner violence and algorithmic harms, necessitate some form of rupture of trust between persons, institutions, and/or systems.[13] For instance, intimate partner violence is so traumatizing because relationships necessitate the risk of being exposed to negative consequences in some way, frequently via technology, such as sharing intimate details or images. Abuse is the taking advantage of this trust, complicating the relationship of the victim-survivor to their own data, devices, and digital practices. While the concept of trust is volatile, it may be hard to achieve a positive result from a complete absence of it,[15] such as disengaging from genuinely supportive and caring systems due to the impact of system trauma. Care, however, must be made in ensuring that the reasons for increasing trust are out of *genuine* concern for those harmed, rather than surreptitious rationales, such as improving public image, platform growth, or harvesting user data. This critical perspective toward trust is important so that our attempts to resolve harm caused to vulnerable groups are not harmful in themselves. As such, we offer the following three considerations for how we may design genuinely trustworthy technologies, or, to put it another way, systems that are genuinely *worthy* of our trust.

Designing for design friction: We recommend developers consider *enforcing design friction* into important interactions with technologies. While this is not an entirely new concept, we see it as particularly important in how it relates to responding to harms and violence. Technologies can appear to reduce the amount of unhelpful friction in our lives, yet this reduction reduces the time for "trust pause" that can happen in-person encounters and actions.[g] Helpful questions, such as "Do I really trust this company to resolve this concern?" are important to consider over a longer period. In many ways, this may work counter to the instantaneous response of technology; services may demand an immediate response for them to work, such as submitting a form or agreeing to the terms and conditions of a site. However, digital technologies should be upfront about offering information around uncertainties that users may have; such as how their information should be used or how they may respond to violence perpetrated on or via their system.

Consider the dynamism of trust: Designers and developers may need to appreciate the dynamism of trust, particularly when someone has lost trust in digital technologies or systems that they expected to mitigate harm. Individuals who have been harmed by or through technologies may be reluctant to re-engage or use similar technologies in future. For instance, someone who has experienced financial inequality due to being discriminated against via an algorithm may be reluctant to reach out to credit services after seeing these services as part of the problem.[23] Trust is dynamic and contextual, therefore depending on a wide range of factors that may not be initially obvious to the developers of a system. As such, trust in systems may necessitate structuring a gradual build up

[g]https://www.i-cio.com/big-thinkers/rachel-botsman/item/the-dynamic-nature-of-trust-in-the-digital-age

over time; asking for a minimal amount of information from the user until gradually building up a picture as to how to best provide help. Systems that ask for too much too soon, like human relationships, may be subject to the withdrawal of engagement by users.

Question the methods of trust: Finally, we recommend that developers question *how* someone may be expected to trust in a digital system or service and whether this is a reasonable request. While many services expect and even demand trust from its users through use alone, under the assumption that it would not be used if someone did not trust it, we posit this as an incorrect assumption. It is important to acknowledge in digital service design that many users may have no choice other than to use a digital technology or service to resolve their concerns. For instance, submitting a complaint of harassing behavior through a social media channel can communicate that the user, to some level trusts the process to deliver a satisfactory response.[19] However, the same social media platform (or the reporting process itself) can be a source of trauma. Developers and designers may be encouraged to find ways of innovating to provide alternative means of providing help, and may consider ways to do this outside branded spaces.

We offer these suggestions to surface tensions surrounding digital technologies that cause users to be unsafe and to critique the potential "solutions" offered for mitigating these harms. These are by no means the only matters to consider when designing or deploying pervasive technologies that are worthy of trust, particularly for technologies offered to those who have experienced harm and may approach such systems with a deep mistrust. Our postdigital world has dramatically reduced the amount of time it takes between thought and action; for positive results if the matter is urgent, and negative where individuals may be taken advantage of in a manner unlike in-person situations. By taking pause to consider the facets of trust in digital systems and services we stand a better chance of offering technologies that succeed via careful consideration for the wellbeing of vulnerabilized or at-risk users.

Designing With Abusability

Where product developers often focus on the positive impact new technologies might have on the world, information security practitioners often focus on the negative: how a product or system might be compromised. However, as we have outlined earlier in this article, information security places an intense focus on how an external, malicious actor (or actors) may penetrate a system for sabotage or financial gain, over examining the complex privacy and security practices inherent to social relationships. The concept of "abusability" offers a way expand the focus of traditional approaches to security: abusability plays on the concept of usability to ask what kinds of uses should be restricted rather than enabled in design.[h] Abusability is defined as the possibility that malicious actors might hijack or weaponize a system for harmful activity; and we argue developers and designers have a responsibility to anticipate and mitigate this.[i] The following section develops three implications for incorporating abusability at various stages of the product development lifecycle.

Consider power dynamics: Rather than depicting users of a system as interchangeable and well-meaning actors, designers must consider the inherent power dynamics in societies structured by gender, race, ability, age, and other hierarchies of difference (Hill[8]). For example, smart home devices, such as locks or cameras which have different account types for "Owners" and "Guests" create a hierarchy of affordances, which can reinforce abusive dynamics in the context of family violence or coercive control.[12,20] Although such hierarchies might be useful or desirable for many users or potential consumers, designers should consider the implications of implementing hierarchy into design, and endeavor to make such hierarchies clear and understandable to all users of a potential device or system. Abusability is a reminder that power will often be abused, or as the old feminist slogan puts it "abuse of power comes as no surprise."

Include safety concerns in threat modeling and testing: One practical way designers can incorporate abusability is by reconfiguring design practices, such as threat modeling and usability testing to include interpersonal harms such coercive control, bullying, or stalking.[5] Threat modeling both in research and in industry practices should ask how might this product be abused for harm?[18,22] By drawing on existing social science and human–computer interaction research on interpersonal abuse, researchers can develop threat models that can be used in industry product development. This is true not just for the problems related to coercive control or domestic violence, but also more broadly for other forms of abuse or discrimination that are exacerbated by technology, such as racism or xenophobia. Further research on new forms of technology-enabled abuse, as

[h]https://www.wired.com/story/abusability-testing-ashkan-soltani/
[i]https://aiblindspot.media.mit.edu/

well as forms of abuse that have received less attention (such as abuse of marginalized groups like migrants or domestic workers, or intersectional abuse that combines racism and sexism or other forms of discrimination) is also critical. Researchers and practitioners conducting usability testing can also develop abusability tests that include abuse scenarios akin to penetration testing, in which a malicious actor attempts to use the product for harm.[17] Results from such tests should be fed back into product documentation or policies, or in more serious cases, researcher and practitioners should advocate for "refusal"[j]: products with a high likelihood for abusability should be withdrawn or sent back for rethinking and redesigning.

Develop responsive systems: Although abusability is critical at the design stage (where it is preventative), it is also important to address abuse once it has happened by developing responsive systems. At the most basic level, this entails including blocking and abuse reporting features on any platform or product, which allows for interpersonal interaction. Abuse often occurs on platforms where it is unexpected, as is demonstrated by the case of abusers sending $1 bank transfers to send abusive messages.[k] Bank developers (understandably) did not consider a use case in which users may need to block others from sending them money; while this may have been flagged by incorporating abusability into threat modeling, it is also important to have prominent and accessible abuse reporting features so problems can be flagged as they arise. Advocates we called for a *relational dynamic* between technologists and support services, such as domestic violence shelters and sexual violence counseling, in which advocates are taken seriously and compensated fairly in efforts to flag problems and develop support systems for those who have experienced technology-mediated abuse.

Such initiatives must also be careful of the pitfalls of *ethics-washing*, i.e., a performative display of interest in countering abuse without meaningful action and *tokenism* or seeking approval on an already developed project from advocates or survivors without meaningfully consulting them. For example, a rising criticism against technology companies has resulted in a spate of *Trust and Safety* or *Responsible Innovation* positions without

[j]https://blogs.lse.ac.uk/businessreview/2019/06/22/technologies-of-control-we-have-to-defend-our-right-of-refusal/

[k]https://www.sbs.com.au/news/people-are-using-1-australian-bank-transfers-to-send-someone-an-abusive-message/eab4d533-ac85-4f9f-8a6f-8cd71928070d

TABLE 1. Abusability maturity model. Originally published in Strohmayer *et al.*'s trust and abusability toolkit: https://nrl.northumbria.ac.uk/id/eprint/47508/

Maturity level	Description
−2: Actively facilitating abuse[1]	Company designs and sells spyware or covert monitoring devices, which are easily used for abuse
−1: Willful ignorance	Company either ignores the problem of technology abuse or addresses it superficially through: • *Ethics-washing:* a performative display of interest in countering abuse without meaningful action • *Tokenism:* seeking approval or a "green stamp" on an already developed project from advocates or survivors without meaningfully consulting them
0: Organisational awareness	Key decision-makers in company demonstrate an awareness of technology abuse broadly (through reading key resources) and how technology abuse occurs in their products and platforms specifically. This includes research and active reflection on questions like: • What kinds of abuse occur on our platforms, products, or devices? • Who is disproportionately affected by this kind of abuse? • How does this abuse relate to specific product features?
1: Taking action	Company has taken action to mitigate and redress abuse on its platform or using its products, for example through: • Including tech abuse in threat modeling or abusability testing • Understanding how measures implemented to prevent abuse—such as reporting features or content moderation—can themselves be abuse • Incorporating abuse into content moderation policies and features (such as automated detection) linked to abuse reporting function • Offering options to survivors, such as blocking perpetrators
2: Meaningful engagement	Company actions to address abuse incorporate abusability using principles of "trauma-informed" or "coercive control resistant" design. Tech abuse survivors and advocates are consulted at different stages of product development, their input is fairly compensated and their feedback is taken seriously (in contrast with level −1 where advocates are only consulted after product is developed).

sufficient mechanisms for those teams to have enough power to actually shift design decisions. Both researchers and practitioners can draw on the principles of participatory action research and co-design to ensure meaningful and respectful engagement with both survivors and advocates (see e.g., Kaur *et al.*[21]).

By considering power dynamics, incorporating safety concerns into design and testing, and building responsive systems, both security researchers and practitioners can reconfigure cybersecurity practices to center people's safety in technology design. Cybersecurity concerns have fleshed out frameworks and industry standards for verification, monitoring, and certification, such as the US Department of Defense's Cybersecurity Maturity Model Certification (CMMC).[l] There is ample work remaining to develop frameworks and industry standards for evaluating the abusability of existing systems and the extent to which developers account for abusability in design, but in our trust and abusability toolkit, we start some of this work. We propose a basic rubric for evaluating the maturity of abusability practices (see Table 1); this is a high-level overview and not a full maturity model that would be used in industry; however, such details should be fleshed out in the future.

CONCLUSION

In this article, we use a feminist and justice-oriented lens of our world as postdigital ecologies; where we highlight and unpick the topic of safety as both a challenge and vision for pervasive computing. We do this based on the assumption that researchers, engineers, and designers want to be, and to a degree already are, conscious about privacy concerns of their users. We put forward that if individuals are conscious about privacy concerns, they should also care about the postdigital safety of those who use their systems. We argue this by drawing on interdisciplinary literatures, specifically using examples related to technology-facilitated abuse in intimate partner violence contexts and algorithmic harms as prescient examples of why notions of safety are so important. Using these examples, we present our understanding of safety as a postdigital ecology before providing two suggestions of how we can use a feminist orientation to safety to design, develop, and adapt pervasive technologies: 1) designing genuinely trustworthy technologies; and 2) designing with abusability. Our challenge and vision for pervasive computing is grounded in three core tenets of a feminist safety lens as outlined previously: 1) centering the experiences of those who are usually ignored as "edge cases"; 2) centering safety and unsafety throughout the design, development, and deployment lifecycles of pervasive technologies by engaging deeply with "abusability" and "trust"; and 3) engaging deeply with sociotechnical aspects that relate to pervasive technologies. In working through these three aspects, we argue that technologists are able to fully take into consideration holistic safety of people. What we argue herein is not that we should "design out" unsafety, but that we should actively engage with the very real risk that the technologies we build can and will be used for harm instead.

[l]https://crest-approved.org/the-cybersecurity-maturity-model-certification-cmmc/index.html

REFERENCES

1. A. Alkhatib and M. Bernstein, "Street–level algorithms: A theory at the gaps between policy and decisions," in *Proc. Conf. Hum. Factors Comput. Syst.*, 2019, Art. no. 13, doi: 10.1145/3290605.3300760.
2. L. Coles-Kemp, R. B. Jensen, and C. P. R. Heath, "Too much information: Questioning security in a post-digital society," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2020, pp. 1–14, doi: 10.1145/3313831.3376214.
3. T. K. Das and B. - S. Teng, "The risk-based view of trust: A conceptual framework," *J. Bus. Psychol.*, vol. 19, no. 1, pp. 85–116, 2004. [Online]. Available: https://www.jstor.org/stable/25092888
4. M. Elkin, *Domestic Abuse Prevalence and Trends, England and Wales: Year Ending*. San Francisco, CA, USA: Nick Stripe, 2021.
5. D. Freed *et al.*, ""A stalker's paradise": How intimate partner abusers exploit technology," in *Proc. Conf. Hum. Factors Comput. Syst.*, 2018, pp. 1–13, doi: 10.1145/3173574.3174241.
6. B. A. Harris and D. Woodlock, "Digital coercive control: Insights from two landmark domestic violence studies," *Brit. J. Criminol.*, vol. 59, no. 3, pp. 530–550, 2019, doi: 10.1093/bjc/azy052.
7. S. L. Henry, S. Abou-Zahra, and J. Brewer, "The role of accessibility in a universal web," in *Proc. W4A 2014 - 11th Web Conf.*, 2014, pp. 1–4, doi: 10.1145/2596695.2596719.
8. H. Collins, *Black Feminist Thought*. England, U.K.: Routledge, 2002, doi: 10.4324/9780203900055.
9. B. Hooks, *Teaching Community: A Pedagogy of Hope*. England, U.K.: Routledge, 2003.
10. K. Hörschelmann and E. Reich, "Entangled (In) Securities: Sketching the scope of geosocial approaches for understanding 'Webs of (In)Security' 1," *Geopolitics*, vol. 22, no. 1, pp. 73–90, 2017, doi: 10.1080/14650045.2016.1214821.

11. M. Kaur *et al.*, "Human factors in security research: Lessons learned from 2008-2018," 2021. Accessed: Apr. 22, 2022. [Online]. Available: http://arxiv.org/abs/2103.13287
12. R. Leitão, "Anticipating smart home security and privacy threats with survivors of intimate partner abuse," in *Proc. DIS ACM Designing Interactive Syst. Conf.*, 2019, pp. 527–539, doi: 10.1145/3322276.3322366.
13. K. Levy and B. Schneier, "Privacy threats in intimate relationships," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–13, 2021, doi: 10.1093/CYBSEC/TYAA006.
14. R. Lewis *et al.*, ""Safe spaces": Experiences of feminist women-only space," *Sociol. Res. Online*, vol. 20, no. 4, pp. 105–118, 2015, doi: 10.5153/sro.3781.
15. S. Marsh and M. R. Dibben, "The role of trust in information science and technology," *Annu. Rev. Inf. Sci. Technol.*, vol. 37, no. 1, pp. 465–498, 2005, doi: 10.1002/aris.1440370111.
16. R. Mortier *et al.*, "Human-Data interaction: The human face of the data-driven society," *SSRN Electron. J.*, 2014, *arXiv:1412.6159*.
17. S. Parkin *et al.*, "Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse," in *Proc. ACM Int. Conf. Proceeding Ser.*, 2019, pp. 1–15, doi: 10.1145/3368860.3368861.
18. E. PenzeyMoog, *Design For Safety. A Book Apart*. New York, NY, USA: A Book Apart, LLC, 2021.
19. S. Schoenebeck, O. L. Haimson, and L. Nakamura, "Drawing from justice theories to support targets of online harassment," *New Media Soc.*, vol. 23, no. 5, pp. 1278–1300, 2021, doi: 10.1177/1461444820913122.
20. J. Slupska, "Safe at home: Towards a feminist critique of cybersecurity," *St. Anthony's Int. Rev.*, vol. 15, 2019.
21. J. Slupska *et al.*, "Participatory threat modelling: Exploring paths to reconfigure cybersecurity," in *Proc. Conf. Hum. Factors Comput. Syst.*, 2021, pp. 1–6, doi: 10.1145/3411763.3451731.
22. J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the Internet of Things," in *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Bingley, U.K.: Emerald Publishing Limited, 2021, pp. 663–688, doi: 10.1108/978-1-83982-848-520211049.
23. S. Tonkin, *Restoring Financial Safety: Collaborating On Responses To Economic Abuse*. Fitchburg , MA, USA: WEstjustice, 2018.

ANGELIKA STROHMAYER is a senior lecturer at Northumbria University's School of Design, NE1 2SZ, Newcastle upon Tyne, U.K., and co-director of the Design Feminisms Research Group. Her research focuses on feminist, in-the-world research that sits at various intersections of safety, technologies, textiles, and other craft practices, theory development, and methodology. She is the corresponding author of this article. Contact her at angelika.strohmayer@northumbria.ac.uk.

ROSANNA BELLINI is a postdoctoral associate in information science at Cornell Tech, New York, NY 10044, USA. Her research focuses on how digital technologies can be used to exacerbate and facilitate new methods of harms for vulnerable and marginalized populations including survivors of intimate partner violence, and the role of feminisms in design, digital rehabilitation for abusive behaviors, and restorative justice-orientated approaches with sensitive data. Contact her at rbellini@cornell.edu.

JULIA SLUPSKA is a doctoral student at the Centre for Doctoral Training in Cybersecurity and the Oxford Internet Institute, University of Oxford, OX1 3JS, Oxford, U.K. Her research focuses on technologically mediated abuse, such as image-based sexual abuse ('revenge porn') and stalking, as well as emotion, care, and metaphors in cybersecurity, and how feminist theory and methodology can critique and reconfigure online safety and security practices. Contact her at Julia.slupska@cybersecurity.ox.ac.uk.