Towards Anti-Imperialist Security, Privacy, and Safety Research in HCI

Miranda Wei
University of Washington
Seattle, USA
weimf@uw.edu

Matthias Fassl
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
matthias.fassl@cispa.de

Figure 1: Even after an empire is long gone, imperialism continues to manifest around us. Inside a building in a popular Viennese park, symbols of the Austro-Hungarian empire overlook a cafe where people grab their weekend coffees.

Abstract

Usable security and privacy is an interdisciplinary research field at the intersection of computer security, privacy, and HCI founded over 20 years ago. Since then, the field has expanded its domain to claim a wider range of human-centered security and privacy issues. Our field's increasing breadth warrants both celebration of scientific exploration as well as careful consideration of the process itself. The expansionary process of a scientific domain to study a different societies, particularly those that have less global privilege, shares some characteristics with imperialism: the development and maintenance of power of one country over another through various forms of domination. In this work, we take a first step towards anti-imperialist research by identifying how imperialist tendencies manifest in security, privacy, and safety research in HCI and characterizing systemic trends. To aid the development of a critical eye for imperialism in our field, we offer reflection questions for individual researchers.

Keywords

Anti-Imperialism, Security, Privacy, Sociotechnical Safety, Scientific Imperialism, Decolonial

ACM Reference Format:
Miranda Wei and Matthias Fassl. 2025. Towards Anti-Imperialist Security, Privacy, and Safety Research in HCI. In *New Security Paradigms Workshop (NSPW '25), August 24–27, 2025, Aerzen, Germany.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3774761.3774772

ACM ISBN 979-8-4007-1875-5/25/08
https://doi.org/10.1145/3774761.3774772

1 Introduction

Lazy. Stupid. Naive. For a long time, this has been security and privacy experts' prevailing assessment of any non-expert user who did not adequately choose unique long passwords, painstakingly configure privacy settings on dozens of websites, and stay abreast of every new tech gizmo. This assessment, sometimes turned into jokes such as the ID10T error or PEBKAC (problem exists between keyboard and chair), can obscure harmful underlying beliefs that justify intolerance. Negative assessments of other populations have been used to justify vast injustices in history, such as the forced labor of "lazy natives" in colonies during the 19th century European imperialist project [8, p. 2].

Dismissing valid reasons that people might have for choosing unencrypted channels, sharing personal information, or trusting default settings, researchers coined a term for their confusion: the privacy paradox. From the security and privacy expert perspective, users' non-compliance with expert advice is an absurd contradiction. If users stated that they believed privacy to be important, but rarely took actions to protect their data, this was evidence of users' irrationality and naïveté. Research has explored many factors that might explain this perceived mismatch of attitude and behavior [41]. However, this mismatch can also be attributed to faulty assumptions of perfectly rational behavior predicted by economic theories [87] and underestimating the importance of context to privacy attitudes [82]. Even if no expert ever called a user stupid, the implicit focus on user deficit positions experts as an authority with the paternalistic responsibility to 'fix' users. This fix often takes the form of additional education: mandatory cybersecurity trainings, personalized trainings, and endless resources for users to self-educate what experts think they should know. This approach contrasts growing efforts in other HCI subcommunities that regard users as knowledgeable and resourceful and focus on communities' existing strengths [90].

The so-called privacy paradox is an illustrative example of what we explore in this work: imperialist tendencies in security, privacy, and safety research in HCI. These tendencies are unlikely to be the intended outcome of individual researchers, but rather the consequence of the research process itself being situated in specific periods of time and space. Research, including the people and ideas therein, are then influenced by broader social, political, and cultural forces of those times and places. Imperialism has been one such force, where imperialism is defined as:

> "the development and maintenance of power of one country over another through economic, diplomatic, and cultural domination even in the absence of direct colonial occupation" [92].

As the vast scale of imperialism's impact on economies and societies is beyond the scope of this work, we instead focus our attention to a realm closer to home: our own research area.

Our self-reflection and critique come at a critical moment. Since at least 1999 [5, 89], the interdisciplinary research field of usable security and privacy has focused on usability and other human factors related to computer security and privacy. Research in this field began with a US-focused lens on issues such as authentication or online privacy controls, which especially affected privileged Western users in corporate settings. The field has since expanded its domain to claim a wider range of human-centered security and privacy issues. In the process, the study of "other" user populations and their distinct threat models has become a place for discovery. In recent years, research on marginalized and vulnerable populations in computer security and privacy has exploded in popularity. While we should strive to have more globally representative research, we should also carefully consider how and why we undertake such efforts. For example, the uncritical export of security and privacy concerns from one area of the world to another risks perpetuating harmful assumptions and epistemic injustices [6] that prop up the broader forces of imperialism.

As sociotechnical safety researchers, we seek to avoid perpetuating imperialism through our research. The first step towards anti-imperialism is awareness, through building our capacity to identify and characterize imperialism. We strive to take a nuanced approach, avoiding absolute classifications of 'imperialist' or 'not imperialist' research, in recognition of the fact that research is rarely unequivocally judged. Yet, as this field continues to consider social justice issues on a global scale, we advocate for an expressly anti-imperialist approach to human-centered security, privacy, and safety research.

In this critique paper, we trial our anti-imperialist lens. We first summarize relevant prior work on scientific imperialism, colonialism, and decolonial HCI, to provide readers with the necessary context to ground our future discussion. Next, we present examples of how imperialism manifests in security and privacy research, without blaming individual researchers for these systemic trends. These examples do not constitute an exhaustive list and we invite readers to build on this work with additional examples and discussion. Finally, we conclude by proposing anti-imperialist reflection questions to assist researchers in contemplating their own work and navigating the complex legacies of imperialism in research.

2 Motivation

To aid readers in understanding our motivations for this work as individual researchers, we describe our intention to enact critical generosity and our positionality as authors.

2.1 Enacting Critical Generosity

We write in the spirit of critical generosity, to embrace "the critical and the generous in our work with texts, the authors, the readers, and ourselves" [48]. This spirit requires that we remain attentive to the social world from which the people who write research papers come from and the social world that the research then shapes. Receiving criticism is rarely pleasant, even for researchers hardened by years of adversarial peer review. With this critique paper, we do not aim to attack individuals or specific research projects. Instead, we reflect on repeating patterns of work in the research community.

We embrace epistemic generosity, listening and waiting to see what we can learn from papers and discussions rather than relying on suspicion and vigilance [22]. Following the example set by bell hooks [15], we seek to avoid dominator thinking that casts blame and divides research work into a binary of good or bad. Hence, we do not cite specific papers as negative examples. Instead, we invest our energy in creating discussion about transformative practices, hoping readers will apply equal critical generosity to our critiques.

We are also still learning about postcolonialism, anti-imperialism, and relevant ongoing discussions. Therefore, we write from a perspective that reflects our ongoing efforts to question our own assumptions that have been informed by imperialism. We take inspiration from the postcolonial field of the 1980s, where academics from former British colonies began the process of reflecting on the imperialism embedded in themselves and their academic disciplines [93].

Criticism is an act of care that can be supportive of all. A feminist conceptualization of critique [22] is heterogeneous, multidimensional, and not easily reducible to pointing out unfavorable facts. Aligned with this conceptualization, the reflection practice proposed in Section 5 aims to cultivate an "ability to shift our sense of antagonism into a creative response" [65]. Our goals are to map broader trends and determine new research directions, learn from what has worked and what has not worked, and begin the work of translating and applying principles from postcolonial theories to human-centered security and privacy research.

2.2 Author Positionality

Both authors are early career researchers with over eight years of experience each in usable security and privacy. Our educational background includes computer science and engineering, political science, and cultural and social anthropology. While the legacies of imperialism and colonialism have material impacts on our daily lives and political orientations, neither of us have had formal education in these subjects.

Our personal experiences drive us towards this topic. We come from places in the world that have either tried to or are in the process of colonizing and exerting imperial power on other parts of the world. Our families' history additionally influenced our concerns about imperialism. Imperialism is ingrained in our past, through the migration histories of our ancestors. We also observe the present wealth that colonialism produced in European cities, e.g., as expressed in pompous architecture like the crowned double eagle in Figure 1 representing the Austro-Hungarian empire, and how people innocently admire the outcomes of exploitative practices.

The geopolitical status of the countries we live and work in, as well as their imperialist and colonialist practices, concern us. We reject providing tacit support for exploitative practices in computer science and security research, and instead endeavor to deconstruct such practices. We have also been politically active in student representation, works councils, labor unions, and student councils, and we encourage solidarity with peers and colleagues. We extend this solidarity to our fellow researchers, the people they research and work with, and anyone impacted by academic research.

Drawing on Black feminist critiques of technology [16, 73], we recognize that technologies can unintentionally replicate the logics of oppression. Our goals in highlighting imperialism in computer security and privacy are to dismantle imperialist beliefs and practices that are at odds with our critical and feminist values.

3 Background

To inform our analysis of imperialist security research in future sections, we begin by reviewing relevant prior work about imperialism. We first present key ideas from colonialism and imperialism, and then describe how such ideological systems can also be enacted in science, for example, as neo-colonial science and scientific imperialism. As this scholarship has largely evolved outside of the discipline of computer science, we next summarize the growing body of HCI research that has learned from and engaged with postcolonial and decolonial scholarship. Finally, we trace the history of computer security research to the origins of the values spread by imperialist security research.

3.1 Colonialism and Imperialism

Colonialism and imperialism are sometimes used interchangeably, reflecting the two concepts' similarity and mutually beneficial relationship. They can both describe the subjugation of the people of a particular land for the benefit of another group, such as during the European empires of the nineteenth and twentieth centuries. Colonialism mainly refers to practices of settlement or occupation, and especially "to describe the colonial system that was put into operation in the colony itself" [92]. European empires often used imperialism as a political justification for this colonialism, as an ideology that "openly advocated and practiced domination over the territories of other peoples of a different race." The modern conception of imperialism also describes "the development or maintenance of power ('hegemony') of one country over another through economic, diplomatic, and cultural domination even in the absence of direct colonial occupation" [92].

We emphasize the distinction between colonialism and imperialism not to provide a complete account of their scope but to understand them as complementary systems that create and maintain global power dynamics of inequality. Though some believe these concepts are relegated to history textbooks, the legacies of nineteenth and twentieth-century colonialism are still evident in our modern world. Colonization continues to shape contemporary scientific knowledge in many ways: the languages, political and economic systems, and sociocultural norms of colonial powers often still play an outsized role in postcolonial countries.

Cultural imperialism. Cultural imperialism describes a variety of ways for establishing imperialist control through exporting culture [85]. While imperialism's cultural and economic impacts are closely intertwined [79], cultural imperialism emphasizes the spread of imperialist control even outside of political and economic spheres of life [85]. Classic examples of cultural imperialism are through the production of TV series and big-budget movies that become global phenomena. For example, MTV helped spread US American youth culture abroad in the 80s and 90s, and more recently, US-dominated social media companies have impose US-based values on users globally through content moderation policies.

Postcolonial and decolonial approaches. Postcolonial scholarship focuses on the active, ongoing, or recent processes of colonization. Early postcolonial scholars like Franz Fanon [35] and Edward Said [77] were primarily concerned with contesting the "previous dominant Western ways of seeing things [...] to change the way people think, the way they behave, to produce a more just and equitable relation between the different peoples of the world" [93].

Emerging distinct from postcolonial thought, decolonial thinking was developed initially by Latin American activists and scholars and has broadly come to signify attempts to not only contest and change perspectives but also to re-situate knowledge and practice outside of dominant power [17, 93]. By centering the everyday experiences of people marginalized by dominant Western power, the practices of decolonizing have been applied broadly to essentially all aspects of life, from social and political systems to daily practices of culture, work, and play; from relationships, education, and health to computing.

Neo-colonial science. One manifestation of colonialism in science may be familiar to researchers under the name of *helicopter research* or *parachute science*: the practice of researchers from a wealthier country going to a less wealthy country to collect data and publish about that other country, without meaningfully contributing back in some way to the latter country. This practice has also been termed neo-colonial science, reflecting the similarities of scientific knowledge, rather than material resources and labor, being extracted from colonized places.

3.2 Scientific Imperialism

Scientific disciplines come with their own history, values, established knowledge, and investigation methods. Researchers may fear that more powerful and prestigious scientific disciplines could grow to encroach on other disciplines, displacing their knowledge, methods, and values in the process. For example, Dupré strongly criticized how economic styles of thought were pushed onto other disciplines of human behavior [33], sometimes far beyond the origins of the initial idea. In his view, transferring the core assumptions of one concept to another could often be inappropriate, stripping away the necessary context from scientific ideas. Transferring the methods typically used to investigate one set of phenomena to another could have the same ill-advised effect. Dupré identified scientific imperialism as when one science imposed acceptable ways of doing research onto another science, *"dominating other scientific disciplines and sub-disciplines"* [25]. The economist Mäki evoked the poem, "The White Man's Burden"[1], to caricaturize the definition of scientific imperialism as:

> "the superior discipline's burden to bring scientific enlightenment to other disciplines, or at least to the study of other domains." [71]

However, applying existing methods and ideas to new research challenges is common, or even expected in interdisciplinary fields. Most scientists regard this process positively. In this book, *Against Methods*, Feyerabend envisioned that allowing and encouraging epistemological pluralism would enable new forms of inquiry and insights into long-standing problems [38]. Therefore in practice, distinguishing between legitimate cases of epistemological pluralism and instances of scientific imperialism may be difficult, which is why other scholars have argued for an improved definition of scientific imperialism [25, 71].

To reconcile these two positions, Mäki defined three (more specific) kinds of scientific imperialism: imperialism of scope, style, and standing [71]. Imperialism of scope does not merely push styles of thought far away from the origins of the initial idea (as defined by Dupré), but occupies the territories of investigation or knowledge of other disciplines. Imperialism of style imposes research strategies and quality standards onto other disciplines. Imperialism of standing increases the prestige and resources of more powerful disciplines at the expense of other disciplines.

Dupré saw the danger of scientific imperialism in the limited insights provided by applying theories and methods far from the originating discipline. However, limited insights are not that dangerous – they are still insights. Clarke and Walsh were more specific, saying that the danger was overlooking how approaching a subject matter in a particular way can simultaneously shed light on some aspects while obscuring others [25]. This could lead to accepting inferior explanations and disregarding better explanatory alternatives. In the worst case, as Mäki pointed out, this may result in losing the knowledge available before introducing another discipline's values, theories, and methods [71]. This effect, also known as *Kuhn-loss*, is a feature of Thomas Kuhn's concept of scientific revolutions [62]. In contrast, successful instances of scientific unification and epistemological pluralism do not obscure these aspects.

While Dupré [33] mainly was concerned with the spread of Rational Choice Theory from economics to the social sciences, scientific imperialism also affects other interdisciplinary research. The interdisciplinary research area of security, privacy, and sociotechnical safety takes cues from disciplines such as computer science, information science, psychology, economics, and sociology. For example, behavioral economics maintains a strong presence in usable privacy research, aiming to quantify the "value" of personal data [3, 28, 54]. This centers the quantity of the value of data as an economic and individual trade-off between giving up privacy and receiving free services, rather than taking a broader systemic perspective that analyzes surveillance capitalism. Sociology and other disciplines that theorize about social systems invite us to make systems of power (economic, social, or otherwise) for critique. Researchers from different research disciplines are in an ongoing – often highly localized – discussion about what constitutes acceptable, rigorous, and "proper" ways of doing research. These discussions are often shaped by scientific imperialism of scope, style, and standing that this community grapples with. Reflecting on the effects of applying theories and methods from other fields and which kind of knowledge may be obscured will better facilitate such discussions.

3.3 Decolonizing HCI

Broadly influenced by postcolonial and decolonial scholarship outside of computer science, HCI scholars have explored efforts to work for social justice in HCI and against colonization and imperialism, resulting in at least 115 papers from 2004 to 2022 [30]. Scholars view such efforts as both a theoretical and methods-driven applied orientation.

As a theoretical orientation. Initially, postcolonial computing was a label Irani et al. started to use in 2010 as an analytical lens to grapple with Western technologies being exported to "new cultural contexts" (in other words, "out there") [56]. In a subsequent publication, they explored how postcolonial computing could be generative, to pose different ways of looking at the world, develop new research questions, and move beyond "regretful contemplations of past biases" [76]. This approach might be seen as an improvement over prior perspectives on computing that ignored "out there", i.e., non-Western contexts, entirely. In identifying the existence of an other, these authors demonstrated how differences " are not simply a source of undesirable unevenness and aberration, but also sites of creativity and possibility" [76]. However, postcolonial computing may not go far enough in interrogating *who* does the computing and *where* they do it. Though Dourish and Mainwaring outline the colonial impulse of ubiquitous computing (Ubicomp) in its universalizing (to the neglect of the periphery's knowledge) and its quantifying (for the purposes of hegemonic control) tendencies [32], decolonial thinkers argue that this still obscures the ways that Ubicomp itself is part of and perpetuates a racialized world system [9]. Ali points out that practitioners of postcolonial computing still benefit from the systems of power they exist in, and therefore, postcolonial computing needs to be decolonized by decolonial computing [10].

Later HCI researchers have expanded on decolonial computing approaches, outlining a decolonizing agenda for HCI research and design [11], reflecting on the establishment of AfriCHI and ArabHCI to create space for decolonial HCI and pursuing decolonization thinking [66], Afro-Postmodernism for decolonial praxis [14], and decolonizing technology design in Asia [42].

For methods and applications. Decolonial methodologies have been conceptualized for technology design [13, 18] and design practices [58, 81], with particular focus on participatory design (PD) as a method well-suited to decolonial research efforts [24, 81]. Most notably, Smith's "Decolonizing Methodologies" thoroughly critiques

[1] Written by imperialist and racist poet Rudyard Kipling in 1899, "The White Man's Burden" called for the United States to impose colonial control over the Filipino people.

how imperialism and colonization created an imperial view of research *on* indigenous peoples, and articulates the development of indigenous methodologies for research as well as approaches for decolonizing knowledge production [80].

Zong and Matias emphasize that data refusal can also be an act of design. In particular, when done from below, it could be seen as aligned with decolonial efforts [95]. Finally, citational justice in the practice of research itself is another part of rejecting cultural imperialism [63].

Decolonial approaches and thought, popularized in HCI research, are also beginning to reach the usable privacy and security research community. For example, Hasegawa, Inoue, and Akiyama [51] identified a skew in usable privacy and security studies. More so than in HCI, participants came from WEIRD countries. The authors suggested ways to address the geographic and linguistic issues and facilitate research on topics for non-WEIRD countries. For the design of privacy-enhancing technologies (PETS), Chowdhury et al. [23] proposed using Amartya Sen's *capability approach* to move from primarily considering tools' utility focusing on users' capabilities. The increased diversity of methods and measures of success help in recognizing human agency, assessing power dynamics, and paying attention to context when developing inclusive PETS.

3.4 Computer Security's Contradictory Origins

The origins of computer security research reflect two opposing perspectives on power and authority. On one hand, many early security efforts (e.g., tools, organizations, and institutions) were in support of military purposes and thus have been closely aligned with imperialism. On the other hand, early hackers and other counterculture users of technology were staunchly anti-authority, in some cases explicitly extending this to anti-imperialist efforts.

Military origins. Encryption for military purposes has a long history that can be traced back to the Roman Empire. Kerckhoff formulated six design rules for encrypted military communication [59], and encryption played a significant strategic role in the outcome of the Second World War. Increasing digital communication has empowered governments, reduced costs of surveillance, and enabled the mass surveillance of citizens – which cypherpunks (an anti-establishment group from the 1990s) oppose by providing citizens with access to encryption [57]. For example, Zimmermann developed PGP, a (for the time) easy-to-use system to encrypt emails, with the specific mission to counteract government surveillance [94]. The initiatives of the cypherpunks conflicted with US government policies, a conflict that became known as the "crypto wars." This conflict, questioning whether the government should accept that there is communication they cannot read, is still ongoing with ever-changing encryption tools, crimes, and threat actors.

After the Second World War, international intelligence sharing between the US and the UK continued countering global threats like the Soviet Union. Together with Canada, Australia, and New Zealand, they formed the Five Eyes alliance [75] – which influences international surveillance capabilities and discussions on the availability of encryption to this day. In line with Mearsheimer's theory of *offensive realism* [70], other countries align themselves with the Five Eyes alliance when it serves their geopolitical interest.

Counterculture origins. As the military purposes of computer security developed into one set of professionals, institutions, and beliefs, institutions, and professionals, so too did another set: counterculture hackers who often reacted in direct opposition to the former group. Such hackers tended to have an anti-authoritarian bent, as The Hacker Manifesto, written in 1986 and now regarded as a seminal text for grassroots self-identified hackers, illustrates:

> "We seek after knowledge... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals... I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike." [84]

Among other observations, The Mentor (the handle of the Hacker Manifesto's author) explicitly denounces tools developed for military security, such as atomic bombs, and the wars waged by imperial powers. Hackers adopted the term "white hat" (akin to the heroes in Wild Western movies) to distinguish themselves from "black hat" hackers (the villains) to be considered trustworthy enough for salaried industry positions.

While the anti-establishment hacker manifesto aspirationally proclaimed that online everyone is free from discrimination, online discussions were dominated by white men. In *Hacker Culture*, Douglas Thomas described hacker culture as "boy culture."

Starting in 1988, the security community – consisting of a motley mix of vendors, government agencies, hackers, academic security researchers, and the military – used the fallout from the Morris Worm incident to center around the Computer Emergency Response Team (CERT) [43]. Since then, computer security has continued to reflect a spectrum of perspectives on power and authority. Some cybersecurity communities operate in explicit support of military or neo-imperial authority, while other grassroots hacker subcommunities operate in complete opposition.

4 Sketching out how imperialism manifests in security and privacy

Imperialism functions by imposing and maintaining social, political, and economic power over others while serving the interests of a few. Since imperialism is expansionist, it has developed mechanisms to bring others into that system of power, subjugating them to live and serve the interests of those with more power. The hegemonic nature of imperialism can obscure its very presence, making it difficult to critically question and recruiting others to unknowingly aid its expansion.

Depending on the research field, different powers are imposed and maintained. This section examines imperial power's expansion to and maintenance in usable security and privacy research, i.e., the study of user behavior and attitudes related to security and privacy. This subfield began with ground-breaking work on the human aspects of security in the 1980s and 1990s. In 1999, Adams and Sasse critiqued the authoritarian approach to organizational security, calling for more user-centered security [5]. In subsequent years, academics have gathered at a venue dedicated solely to this topic, the Symposium on Usable Privacy and Security (SOUPS).

SOUPS grew from a workshop organized by Professor Lorrie Cranor in 2004 at Carnegie Mellon University in the US.

Initially, usable security and privacy research was conducted where people most commonly interacted with computers: corporate office jobs. Primary research topics included authentication, privacy controls, and phishing [39]. With the proliferation of computing devices and an increasing technology-mediated everyday social life, topics rapidly expanded to include online hate and harassment, interpersonal digital safety, and mis- and disinformation, among others. The expansion of usable security and privacy to contexts beyond corporate contexts is critical to broaden the study of people's perceptions and needs in security. When examining new contexts, researchers unintentionally export their values and assumptions.

Many of the prominent scholars in this community are based in the US or in other Western countries [27]. A review of 485 usable privacy and security research found that 79% papers were conducted with Western participant samples [51], an even higher skew than the 73% of HCI papers with Western participants [68]. This overrepresentation of Western researchers and participants suggests that we must stay attentive to the ways that imperialist tendencies can manifest in usable security and privacy research. Building on Adams and Sasse's initial critique, even when security practice is not outright authoritarian, soft paternalism can be entrenched in how security and privacy mechanisms are designed, e.g., through nudging [4], which implies experts know the "right" behaviors.

Developing an anti-imperialist approach, we aim to counteract the uncritical export of Western ways of doing usable security and privacy. To propose a more sustainable approach for transforming future research practice, we focus on incorporating anti-imperialist considerations by identifying hegemonic dynamics. In this section, we highlight examples of how imperialism manifests in our work, and we invite all the readers to reflect on and extend this list.

4.1 The Language We Use When Conducting and Describing Research

Linguistic relativity suggests that culture, communicated through language, influences our thoughts and decisions [45]. So the language that researchers use to discuss research plans and potential outcomes may affect their research approach to security and privacy issues. Hence, it deserves critical reflection on where these terms and the language come from, how their meaning adapts, and which new areas we apply them to.s

The origins of security research (and computer science in general) are traceable to military and intelligence. This is noticeable in some of the key concepts that are still regularly used in computer security. For example, the "need to know" principle [74, p.167] is used in the military to restrict information access. There, it serves as a principle to discourage browsing for unrelated information and uphold power hierarchies. In computer security, the term has transferred to permissions and authentication research, specifically mandatory access control. It has also found its way into HCI to discuss which information should be displayed on restricted screen sizes. Adams and Sasse [5] argued that the need-to-know principle in computer security leads to a lack of user awareness and security departments' lack of knowledge about users.

Computer security and privacy research is often interlinked with other fields, such as cryptography. Cryptography has developed the term "ceremony" to discuss and formalize interactions with people [34]. It extends the notion of network protocols, a formalized communication between machines in which people follow a security ritual. For example, "key ceremonies" describe the key generation, use, or verification process involving one or more people to build trust in the security. While the concept enabled cryptographers to reason about human interaction, it also ignores social and cultural aspects that matter when these ceremonies are used in everyday life [36].

Frequently used terms like "user" impact research ideas and approaches. Research that only cares about users ignores security and privacy mechanisms affecting non-users [78]. For example, people who use smart glasses or voice assistants may infringe on bystanders' or visitors' privacy. As Satchell and Dourish [78] warned, focusing on users alone is at risk of becoming an unquestioned hegemonic paradigm in HCI research. Heeding their warning in the security and privacy field means refocusing research from an individualized perspective, i.e., the person interacting with a mechanism, to a systemic and community-oriented view on security, privacy, and safety.

Other terms, such as the "standard operating procedure" (SOP), have an unclear origin. While it is used in the military, it is equally if not more common in health and safety to give people step-by-step instructions to conduct critical routine operations. In information security, they are now used to manage incident response.

As an interdisciplinary area of research, usable security and privacy is especially prone to transferring embedded values. Not only does the research derive language and embedded values from associated disciplines, but it also forces them onto other applications and research fields. Hence, researchers should reflect on established terms and consider developing more appropriate terms and language.

4.2 In the Selection of User Populations

Most commonly, security and privacy research studied people at Western universities, security and privacy professionals and practitioners, developers, and crowdworkers. Non-Western populations often remained invisible, ignored, or "othered" in future work sections. While it is a welcome development that US-based study populations are no longer the unquestioned default in the review process, it seems to have led to a rush to "discover" and make visible "novel" study populations. This bears resemblence to the first step of imperialism that "could be tied to a chronology of events related to 'discovery', conquest, exploitation, distribution and appropriation" [80].

Othering of global majority populations. Prior HCI research demonstrated imperialism's legacy by measuring where the research is conducted. Many WEIRD (Western, Educated, Industrialized, Rich, Democratic) countries were imperial powers, providing a partial explanation for why 73% of CHI papers [68] and 79% of usable privacy and security papers [51] focus on Western participant samples that represent less than 12% of the world's population.

Many fields other than computer science have already identified that studying populations in less developed countries from an outside perspective is both a method and an outcome of neocolonialism [29]. Anthropology, for example, has a long history in the othering and "objective" study of indigenous peoples. As such, "the ways in which scientific research is implicated in the worst excesses of colonialism remains a powerful remembered history for many of the world's colonized peoples" [80]. At the turn of the twentieth century, eugenics, as a pseudo-scientific field, popularized scientific racism. The legitimacy and methods of science were used to study racial or ethnic minorities, evaluate their "quality", and justify imperialism, colonialism, slavery, and genocide. Quite understandably, indigenous people have become wary of researchers who want to study them. As a result, "many Indigenous intellectuals actively resist participating in any discussion within the discourses of post-coloniality. This is because post-colonialism is viewed as the convenient invention of Western intellectuals which reinscribes their power to define the world." [80]

Studying non-WEIRD populations can be valuable by making them visible in the research discourse and enabling discussion of specific security, privacy, and safety needs. However, given the history of power imbalances and misuse of scientific legitimacy, approaches and methods must be chosen carefully [51, 68]. The relationship between the researcher and the research subject differs when a researcher from a WEIRD place studies research subjects in a non-WEIRD, more marginalized place. This power imbalance based on imperialist history is even noticeable within the research field itself. The English language has become so widespread through imperialism that it has become the unquestioned default language for scientific communication. This privileges native speakers from dominant countries (e.g., one of the authors) and makes it harder to communicate knowledge for non-native speakers. Most research also takes for granted that widely available computing technologies were developed for Western populations based on certain assumptions about potential problems and their need for solutions – that may not apply in communities and regions now made visible.

So, adapting pre-existing methods and approaches to non-WEIRD populations may require extra care. However, seeing the repeated studies of how email encryption or privacy controls do not work for various populations, Western researchers should also be honest about what they hope to learn. Are there indicators to suggest that the results could be different, or is there pressure to make a novel contribution – recognizing that studying a new population is sufficient for getting accepted? Such an approach might reflect an imperialist urge to discover new populations to apply a demographic lens to, claiming new scientific territory and research novelty.

Valuing novelty over helpfulness leads to academic conquest. Academic venues, including top security conferences, value novelty. The USENIX Security 2024 Call for Papers specifies that "[a]ll researchers are encouraged to submit papers covering *novel* and scientifically significant practical works" [2] and similarly, the IEEE Symposium on Security and Privacy 2024 "solicit[s] previously unpublished papers offering *novel* research contributions in any aspect of security and privacy" (emphasis added in both quotes). [3] Particularly when conducting user research, the pressure for novelty can lead researchers to use well-known research setups and "branch out" toward user populations that are underrepresented in academic literature.

This is already happening: a growing body of usable security and privacy research focuses on marginalized, vulnerable, or at-risk populations. To handle this growing body, researchers developed a framework for unifying such research through contextual risk factors such as "oppression" or "stigmatization." Research papers in this vein describe their novel contribution to the literature as documenting the threat models, needs, or protective strategies of an essential but underrepresented populations in academic research.

Using the lens of novelty in academic security and privacy research, it is then possible to *see* populations that are visible, as opposed to those that are not [88]. Populations that are less visible are broadly the global majority and include people of Indigenous, African, Asian, or Latin American descent who represent approximately 80% of the world's population [21]. Often, papers about security and privacy research engaging with user populations do not even disclose that the recruitment occurred in the U.S.; it is the silently understood hegemonic assumption. At the same time, papers that are located outside tend to highlight the non-U.S. country of origin in the title. In this way, security researchers figuratively engage in the dynamics of "conquering" new populations for security and privacy when they write about the "novel" threat models and considerations of previously invisible populations in academic security research. Valuing this kind of novelty regardless of helpfulness is a "valorization of territorial and militaristic rhetoric as a hallmark of intellectual rigor [that] is deeply problematic and entangled with imperialist and androcentric approaches to knowledge production" [22].

In contrast, focusing on access to digital services instead of security and threat models moves the research lens from the novelty of the user population towards digital participation for everyone. For example, Coles-Kemp and Jensen [26] studied how refugees and migrants struggled to access necessary digitalized government services. They were primarily concerned with the benefits of these services that they required, foregrounding their helpfulness. Protecting assets and controlling access to these services remained a secondary concern.

4.3 In the Objective of Systematization

Systematization is a process and a tool. As a process, systematization includes delineating categories, defining what falls within, and excluding what falls outside. Systematization usually depends on some form of abstraction, a fundamental skill vital computer science and science in general. Abstraction is an act that withdraws or removes properties from consideration, so as to be able to attend to others [60]. The act of removal comes with power over how the abstraction can or should be used. Hence, systematization not only organizes knowledge or things but also bestows power upon entity doing the systematizing. History is littered with social constructs — systematization efforts led by various groups of people — that embedded and perpetuated systems of power. For example,

[2] https://www.usenix.org/conference/usenixsecurity24/call-for-papers

[3] https://sp2024.ieee-security.org/cfpapers.html

systematizing biological gender sustains the cisheteropatriarchy, systematizing labor sustains capitalism, and systematizing people into races sustains colonialism and imperialism. These systematization efforts, whether small or large, have served to benefit the entity with the authoritative viewpoint to define the categories of the system.

One example of systematization for usable security and privacy research is Westin's privacy index, which categorized people into high ("fundamentalist"), medium ("pragmatist") or low ("unconcerned") levels of privacy concerns [64]. Though these categorizations were largely used for industry and policy research, not academic, they were nevertheless influential for decades, broadly informing the notice-and-consent privacy model [86]. However, legal scholars have later critiqued this systematization, calling into question the validity and reliability of the survey questions [53]. While intended to improve the privacy of individuals in the US, these categories of privacy concern demonstrate the power afforded to entities that deployed them.

Survey scales are often intended to be used across disciplinary boundaries and geographical borders. As they can expand their influence for comparisons across boundaries, in some cases they can also be a tool for imperial influence. When security and privacy researchers systematize and categorize knowledge, they unintentionally imprint their view of the world on the categories and all of the people that consume that categorization and sorting; proclaiming their knowledge is most important [49]. In short, they impose their hegemonic views onto the categories. This is unavoidable, as research is not objective. But researchers need to be aware of this, openly communicate about this, and leave space for alternative categorizations.

Today, Westin's privacy index is not as relevant to privacy research anymore. Instead, we have global privacy standards based on European notions of what privacy is and how it should be enforced (GDPR). Globally effective regulations are important to uphold legal expectations of data protection and privacy, requiring organisation and uniformity. However, the uniformity comes with the cost of making other, alternative, conceptions of privacy, e.g., on a group level than on an individualized level, invisible and less legitimate.

Systematization of any kind also always requires a simplification and reduction of complexity and nuances [19]. However, it ends up giving a false sense of completeness which can be deceiving to researchers and end users alike. So, researchers have to continuously ask themselves who is or what kind of knowledge are further marginalized because they are not even mentioned?

4.4 In the Fundamental Embedded Values

The computer security research field comes with some fundamental embedded values. First and foremost, there is a common attacker for everyone, and security experts have the authority to say who that is and how to protect users from them.

Assuming that there is a correct path to increasing security. Education and training are governance tools used in colonization and imperialist efforts, e.g., in the British Empire [47] or the American Indian boarding schools in the US [31]. In security and privacy, education often comes in the shape of hierarchical 'advice' that appears as a form of enlightenment, telling users what they *should* be doing, sometimes with minimal explanation, threat model, or other context. From the first human-centered security studies, users' non-compliance implied a lack of knowledge and understanding of security issues. The security community saw it as their burden to enlighten end users to save them. Hence, many usable security and privacy research projects focused on designing and evaluating educational materials in different forms (posters, games, quizzes, and more). The widespread adoption of information security management in companies also led to the inclusion of security awareness training and campaigns. As a result, an entire ecosystem of awareness training and user education for companies has been developed.

This ecosystem privileges security experts' opinions of the correct path to achieving security, privacy, and safety, dismissing the idea that non-expert people are capable of reasonably managing their own security and privacy. They learn from scams and fraud, learn from their friends' and family's experiences, are able to recover, and also teach their friends about what they learned. To unlearn this particular embedded value, we have to accept that different ways of achieving security exist and allow end users to set their own priorities based on their lived experience, which they alone are the real expert.

Lack of participation (or exclusion) as an accepted outcome. The values embedded into security and privacy research also determine acceptable outcomes and side effects of security protections. For example, the safety of online users from harassment is not as important as the privacy of the perpetrators' communication. Prioritizing privacy in all cases leads to accepting the outcome of marginalized groups leaving online platforms and forgoing technology-mediated social interactions. This is not just. With more social interaction being moved online, it can create an experience of deprivation and dehumanization of "othered" populations:

> "To lose everything and to be forced to move to another country as a refugee, your only property, your own body and the knowledge that you carry within you, must be one of the most extreme human experiences of deprivation and dehumanization, the more so since one effect seems to be that you immediately begin to lose your humanity in the sight of others, reduced as the Italian philosopher Giorgio Agamben has put it, to 'bare life', an unrelenting minimal existence in which you are no longer the subject of rights but a supplicant who at best has become an object of compassion" [93].

Independence and self-governance. It is also useful to remind us that not all approaches to security and privacy have to embody neocolonialist values. The anarchist hacker community has brought liberal ideas to the open-source community as well as the security and privacy research community [43]. The values built into free (and open source) software projects can endure for a long time since these projects became popular enough to achieve the stage of an Internet infrastructure. The fediverse, a collection of social networking sites that communicate with each other, is one recent example of that. Its decentralized but federated nature is the antithesis of common centralized Internet services that surveillance capitalism encourages. Cory Doctorow identifies decentralization and independent operators as the way to fight surveillance capitalism [20]. The decentralization and self-governance also allow local communities to be self-sufficient and regulate their own communication style and levels of acceptable privacy protections.

4.5 In the Extraction of Value from Othered Populations

In an economic sense, imperialism "could be tied to a chronology of events related to 'discovery,' conquest, exploitation, distribution and appropriation" [80]. After discovery and conquest, imperialist research may exploit communities and participants to extract value. Extracted value comes in different forms, e.g., the added knowledge that can be applied elsewhere, monetary value, and the increased social capital of the researchers themselves. Following ethical research practices, researchers should, in any study, compensate participants and give back to the community to avoid exploitation and ensure friendly relationships with future researchers. Dedicated security and privacy clinics [52] are an example of establishing strong ties with an affected community to tailor practice and research to community needs. While the research output is welcome, it is not the primary factor for establishing these clinics. An anti-imperialist lens can help researchers consider in more detail the kinds of extracted values, think about ways of mutual learning, and empower the participants as well as their communities.

Extracting research value. Gaining knowledge that we did not have before is the entire point of doing research. However, extracting research value may become imperialist if the participants are (without a good reason apart from their availability) marginalized and they and their communities are not compensated appropriately. Worldcoin, co-founded by OpenAI CEO Sam Altman, is a cryptocurrency project that wants to provide a universal basic income (UBI) based on its cryptocurrency [2, 46]. Central to this mission is a high-tech orb that recruiters use to collect biometric iris data about everyone, ostensibly to avoid defrauding this imagined UBI system. Enrolling required personal data in the form of email addresses, phone numbers, and biometric iris data without meaningful consent. Collecting biometric data is an ethical concern because risks exposing all the participants to harms from misuse, which is on the rise according to the FTC [37]. The project focused on countries of the global south – Indonesia, Kenya, Sudan, Ghana, Chile, and Norway [46]. Participants were given "free money" in the form of the Worldcoin cryptocurrency, promising future wealth increase. In Kenya, the government ended up suspending enrollment to the project over data privacy concerns [72].

Extracting monetary value. The security and privacy industry also creates financial gains for itself. They do so first by individualizing the responsibility for security and privacy to end users (guilt-shaming them into compliance), thereby creating a market and then offering them software to combat the problem. This has been a pattern with anti-virus software before (now mostly obsolete) and is now more noticeable with commercial VPN software. VPNs have become widely known because of the 2016 FCC decision to allow analyzing ISP traffic for marketing purposes [61]. VPN providers used this decision to scale their operations up and employ large-scale advertisement campaigns to convince users worldwide that they need a VPN [7], essentially exporting a US-based privacy concern to the world. However, many security, privacy, and safety problems are either not easily reducible to individuals' behaviors because they are systemic or platform issues. Most commonly, people end up employing VPNs to circumvent censorship, an issue of digital participation and freedom. In authoritarian countries these can be helpful to access information and services from abroad, in democratic countries they are useful to access media that has been blocked because of intellectual property rights. In any case, asking money from individuals for security software limits access to security and privacy and can seriously impede adoption and, consequently, security gains.

5 Where do we go from here?

As explored in the previous sections, academic research and industry projects in security, privacy, and safety are grappling with the legacies of imperial systems. So what should be done? We do not believe there to be a single correct answer, but we see value in aligning our approach with other political questions that tackle systemic change.

Ben Green's action-oriented suggestion on grounding data science in a politics of justice [44] is relevant for developing an anti-imperialist approach. Green proposed a stage model of transformation that starts with cultivating *interest* (in social-good applications of data science), continues with *reflection* (about current ways of doing things in data science), and then next to changing *applications* of data science and finally *practice* based on the collective reflection. This section suggests a reflective practice [12] during the planning phase of research projects to understand how imperialism may manifest in the underlying ideas and research practice.

Reflection questions. Towards supporting security, privacy, and safety researchers to do anti-imperialist research, we now outline three reflection questions. These questions do not give binary verdicts about whether research is or is not perpetuating imperialism. Instead, their purpose is to generate discussion about how a research project may relate to imperialist tendencies. Only then can researchers detect systematic patterns and respond appropriately. This list is therefore not intended to be conclusive but instead, a practical starting point.

RFQ1: In what ways might we be perpetuating an imperialist past?

When beginning a research project, invest time and resources to learn about the planned research topic's history. Consider the assumptions that the original technology or sociotechnical system may have embedded in its composition. For example, is the "discovery" (e.g., of a novel population) being framed as the key contribution? In this way, the academic scholarship reflects normative assumptions of who is an expected user and who is not.

It is critical to consider the positionality of the researchers relative to the study population. Especially if researchers hold different positions than the population of interest, research should be a collaboration between researchers and the population. The slogan "nothing about us, without us" has been used by advocates to describe how populations such as youth [91] or people with disabilities [83] must be included in the development of policies or research about them. Additional scholarship on positionality is related to reflections on reflexivity [69], community-based research [50, 67], and more.

RFQ2: What forms of existing knowledge and practice might be hidden?

Imperialism, in its quest for implementing a new regime, can obscure and erase existing knowledge and practice, perpetuating epistemic injustice [6]. A key consideration for researchers must be to evaluate whether the researchers' assumptions about security, privacy, and safety – including threat models and appropriate responses to risks – match communities or research participants' expectations and goals. As discussed in Section 4.4, education can be a form of imperialistic governance. For example, forcing users to undergo mandatory security training is one way of enforcing the "right" behaviors - even if such training is poorly defined or misaligned to the goals of the user.

RFQ3: Are we as researchers benefiting more from the research than the participants?

Finally, researchers must carefully consider the long-term outcomes of the research project after publication. Applied research often makes arguing how the results benefit participants easier, but participants might contribute to fundamental research without clear outcomes. Even though direct monetary compensation for study participation has become more common, it is by no means the only way participants benefit from research. For example, researchers can offer to be a security and privacy consultant, donate their time to fix issues with tech, or try to create lasting community impact by setting up locally-hosted infrastructure and teaching community members how to maintain it.

Individual and collective reflective practice. These questions and principles for reflection can be operationalized individually, collectively, or both. The lowest barrier to entry is individual reflection: the lead researcher confronts these questions, checks how related work handled these questions, asks for other researchers' feedback, and documents the results in a research diary or the final paper. As Amulya [12] pointed out, individual and collective reflective practices are not mutually exclusive. Collaborations between three to eight researchers are relatively typical in security research. Structured collective reflection meetings could start with individual-focused breakout sessions, which then inform a round-table discussion, enabling mutual learning and "exploring the connections across those multiple perspectives" [12]. In the context of collective discussions among research team members, there is no need to stay within the scope of the reflection questions. We encourage following up on other aspects of imperialism related to the research project that arise in the discussion.

Institutioning anti-imperialist reflective practice. Ideally, investigating potential imperialist tendencies of a research project happens before its start and during the write-up stage to double-check the framing of the paper's intent and results. Reflective practice is about "building a habit, structure, or routine" [12] in the work of researchers. One way of making reflective practice a structure or routine is *institutioning* [55], making or adapting an institution. The internal or ethical review board is typically an existing university institution with an established application and review process. We want to avoid adding additional burden to these existing institutions that often lack resources. However, that particular moment in a research project is already a moment of reflection that can invite a broader view of the research project and its relation to imperialism. As an initial step, adding a paragraph in the paper about what the researchers thought about that and how they plan to mitigate the potential impact of imperialist tendencies would be helpful.

Effecting change. With this critique paper, we hope to contribute to a change in knowledge and facilitate a change in practice. As a community of researchers and scholars, we have the power to impact change in research culture and the policies associated with our publication venues and research institutions. In this work, we reflected on imperialist tendencies we have observed in usable security and privacy research specifically. Similar to the Missouri model for trauma-informed schools [1], success in advancing anti-imperialist research is a process, not a destination.

To continue this process, future work can work to identify the roots of imperialist ideologies that underlie ongoing research projects. As an instructive case, Gebru and Torres traced the common roots of effective altruism and longtermism, both part of the TESCREAL bundle, to first-wave eugenics [40]. For usable security and privacy research, much more reflection is needed from additional vantage points to build a communal practice of anti-imperialist research.

Acknowledgments

We acknowledge the Coast Salish peoples of the land that University of Washington occupies, the land which touches the shared waters of all tribes and bands within the Duwamish, Puyallup, Suquamish, Tulalip and Muckleshoot nations.

We acknowledge that European imperialism and colonialism has shaped power and wealth disparities in Europe and globally. The CISPA Helmholtz Center for Information Security is on land that was contested between Germany and France. These Europeans, in contrast to the people they colonized, were allowed to choose in democratic elections what should happen with the land they live on.

CRediT author statement

Miranda Wei: Conceptualization (formulation and evolution of research goals), Methodology, Investigation, Resources, Writing (original draft, review, & editing), Project administration. **Matthias Fassl:** Conceptualization (evolution of research goals), Methodology, Investigation, Resources, Writing (original draft, review, & editing), Project administration.

References

[1] 2019. *The Missouri Model for Trauma-Informed Schools.* Technical Report. Missouri Department of Mental Health. 25 pages. Retrieved 2024-09-08 from https://dmh.mo.gov/sites/dmh/files/media/pdf/2019/05/missouri-model-trauma-informed-schools.pdf

[2] 2023. Understanding the Orb and why Worldcoin uses biometrics. Retrieved 2024-09-08 from https://worldcoin.org/blog/worldcoin/understanding-orb-why-worldcoin-uses-biometrics

[3] Alessandro Acquisti. 2014. The economics and behavioral economics of privacy. In *Privacy, big data, and the public good: Frameworks for engagement.* Cambridge University Press.

[4] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2018. Nudges

for Privacy and Security: Understanding and Assisting Users' Choices Online. *Comput. Surveys* 50, 3 (May 2018), 1–41. https://doi.org/10.1145/3054926 Publisher: Association for Computing Machinery (ACM).

[5] Anne Adams and M. Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46. https://doi.org/10.1145/322796.322806

[6] Leah Hope Ajmani, Jasmine C. Foriest, Jordan Taylor, Kyle Pittman, Sarah Gilbert, and Michael Ann Devito. 2024. Whose Knowledge is Valued?: Epistemic Injustice in CSCW Applications. *Proceedings of the ACM on Human-Computer Interaction* 9, CSCW2 (Nov. 2024), 26.

[7] Omer Akgul, Richard Roberts, Moses Namara, Dave Levin, and Michelle L. Mazurek. 2022. Investigating Influencer VPN Ads on YouTube. IEEE, San Francisco, CA, USA, 876–892. https://doi.org/10.1109/SP46214.2022.9833633

[8] Syed Hussein Alatas. 1977. *The myth of the lazy native: a study of the image of the Malays, Filipinos and Javanese from the 16th to the 20th century and its function in the ideology of colonial capitalism.* P. Cass, London.

[9] Syed Mustafa Ali. 2014. Towards a decolonial computing. In *Ambiguous Technologies: Philosophical Issues, Practical Solutions, Human Nature.* International Society of Ethics and Information Technology, Lisbon, Portugal, 28–35. Retrieved 2024-09-03 from https://oro.open.ac.uk/41372/ Num Pages: 8.

[10] Syed Mustafa Ali. 2016. A brief introduction to decolonial computing. *XRDS: Crossroads, The ACM Magazine for Students* 22, 4 (June 2016), 16–21. https://doi.org/10.1145/2930886

[11] Adriana Alvarado Garcia, Juan F. Maestre, Manuhuia Barcham, Marilyn Iriarte, Marisol Wong-Villacres, Oscar A Lemus, Palak Dudani, Pedro Reynolds-Cuéllar, Ruotong Wang, and Teresa Cerratto Pargman. 2021. Decolonial Pathways: Our Manifesto for a Decolonizing Agenda in HCI Research and Design. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, Yokohama Japan, 1–9. https://doi.org/10.1145/3411763.3450365

[12] Joy Amulya. 2004. *What is Reflective Practice?* Technical Report. The Center for Reflective Community Practice at MIT. Retrieved 2024-09-11 from https://www.careinnovations.org/wp-content/uploads/what-is-reflective-practice65.pdf

[13] Ahmed Ansari. 2019. Decolonizing design through the perspectives of cosmological others: Arguing for an ontological turn in design research and practice. *XRDS: Crossroads, The ACM Magazine for Students* 26, 2 (Nov. 2019), 16–19. https://doi.org/10.1145/3368048

[14] Oritsetimeyin Arueyingho, Damiete Onyema Lawrence, and Helena Webb. 2024. Navigating Afrocentric Human-Computer Interaction Research: A Scoping Review and Proposition of Afro-Postmodernism for Decolonial Praxis. In *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems (CHI EA '24).* Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3613905.3644072

[15] bell hooks. 2008. Mind, Body and Soul. Retrieved 2024-09-02 from https://www.youtube.com/watch?v=sAuHQIMQUIs

[16] Ruha Benjamin. 2019. *Race after technology: abolitionist tools for the New Jim Code.* Polity, Cambridge, UK Medford, MA.

[17] Gurminder K. Bhambra. 2014. Postcolonial and decolonial dialogues. *Postcolonial Studies* 17, 2 (April 2014), 115–121. https://doi.org/10.1080/13688790.2014.966414

[18] Nicola J. Bidwell, Tigist Sherwaga Hussan, Satinder Gill, Kagonya Awori, and Silvia Lindtner. 2016. Decolonising Technology Design. In *Proceedings of the First African Conference on Human Computer Interaction.* ACM, Nairobi Kenya, 256–259. https://doi.org/10.1145/2998581.2998616

[19] Geoffrey C. Bowker and Susan Leigh Star. 2008. *Sorting things out: classification and its consequences* (1. paperback ed., 8. print ed.). MIT Press, Cambridge, Mass.

[20] Christopher Byrd. 2022. Cory Doctorow Wants You to Know What Computers Can and Can't Do. Retrieved 2024-09-08 from https://www.newyorker.com/culture/the-new-yorker-interview/cory-doctorow-wants-you-to-know-what-computers-can-and-cant-do

[21] Rosemary Campbell-Stephens. 2020. *Global Majority; Decolonising the language and Reframing the Conversation about Race.* Technical Report. 7 pages. https://www.leedsbeckett.ac.uk/-/media/files/schools/school-of-education/final-leeds-beckett-1102-global-majority.pdf

[22] Rachelle Chadwick. 2024. The question of feminist critique. *Feminist Theory* 25, 3 (Aug. 2024), 376–395. https://doi.org/10.1177/14647001231186526 Publisher: SAGE Publications.

[23] Partha Das Chowdhury and Andrés Domínguez Hernández. 2022. From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs. In *NSPW '22: Proceedings of the 2022 New Security Paradigms Workshop.* ACM, North Conway, NH, USA. https://doi.org/10.1145/3584318.3584323

[24] Rachel Clarke, Reem Talhouk, Ahmed Beshtawi, Kefah Barham, Owen Boyle, Mark Griffiths, and Matt Baillie Smith. 2022. Decolonising in, by and through participatory design with political activists in Palestine. In *Participatory Design Conference 2022: Volume 1.* ACM, Newcastle upon Tyne United Kingdom, 36–49. https://doi.org/10.1145/3536169.3537778

[25] Steve Clarke and Adrian Walsh. 2009. Scientific Imperialism and the Proper Relations between the Sciences. *International Studies in the Philosophy of Science* 23, 2 (July 2009), 195–207. https://doi.org/10.1080/02698590903007170

[26] Lizzie Coles-Kemp and Rikkie Bjerg Jensen. 2019. Accessing a New Land: Designing for a Social Conceptualisation of Access. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019).* ACM, Glasgow, Scotland, UK. https://doi.org/10.1145/3290605.3300411

[27] Lorrie Faith Cranor, Simson Garfinkel, Robert Biddle, and Mary Ellen Zurko. 2024. Reflecting on Twenty Years of Usable Privacy and Security. Retrieved 2025-10-16 from https://www.usenix.org/conference/soups2024/presentation/panel-retrospective

[28] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. 2006. A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society.* ACM, Alexandria Virginia USA. https://doi.org/10.1145/1179601.1179621

[29] Farid Dahdouh-Guebas, J. Ahimbisibwe, Rita Van Moll, and Nico Koedam. 2003. Neo-colonial science by the most industrialised upon the least developed countries in peer-reviewed publishing. *Scientometrics* 56, 3 (March 2003), 329–343. https://doi.org/10.1023/A:1022374703178

[30] Dipto Das and Bryan Semaan. 2022. Decolonial and Postcolonial Computing Research: A Scientometric Exploration. In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing.* ACM, Virtual Event Taiwan, 168–174. https://doi.org/10.1145/3500868.3559468

[31] J. Davis. 2001. American Indian Boarding School Experiences: Recent Studies from Native Perspectives. *OAH Magazine of History* 15, 2 (Jan. 2001), 20–22. https://doi.org/10.1093/maghis/15.2.20

[32] Paul Dourish and Scott D. Mainwaring. 2012. Ubicomp's colonial impulse. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing.* ACM, Pittsburgh Pennsylvania, 133–142. https://doi.org/10.1145/2370216.2370238

[33] John Dupré. 2001. *Human nature and the limits of science* (1. publ ed.). Clarendon Press, Oxford.

[34] Carl Ellison. 2007. Ceremony Design and Analysis. (2007).

[35] Frantz Fanon. 2004. *The Wretched of the Earth.* Grove Press, New York.

[36] Matthias Fassl and Katharina Krombholz. 2023. Why I Can't Authenticate — Understanding the Low Adoption of Authentication Ceremonies with Autoethnography. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23).* ACM, Hamburg, Germany, 15. https://doi.org/10.1145/3544548.3581508

[37] Federal Trade Commission. 2023. FTC Warns About Misuses of Biometric Information and Harm to Consumers. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

[38] Paul Feyerabend. 1993. *Against method* (3rd ed ed.). Verso, London ; New York.

[39] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: history, themes, and challenges* (online-ausg ed.). Number 11 in Synthesis lectures on information security, privacy, and trust. Morgan & Claypool Publishers, San Rafael. https://doi.org/10.2200/S00594ED1V01Y201408SPT011

[40] Timnit Gebru and Émile P. Torres. 2024. The TESCREAL bundle: Eugenics and the promise of utopia through artificial general intelligence. *First Monday* (April 2024). https://doi.org/10.5210/fm.v29i4.13636

[41] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security* 77 (Aug. 2018), 226–261. https://doi.org/10.1016/j.cose.2018.04.002

[42] Masitah Ghazali, Eunice Sari, and Adi Tedjasaputra. 2022. Asian CHI Symposium: Decolonizing Technology Design in Asia. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22).* Association for Computing Machinery, New York, NY, USA, 1–4. https://doi.org/10.1145/3491101.3503701

[43] Matt Goerzen and Gabriella Coleman. 2022. *Wearing Many Hats: The Rise of the Professisonal Security Hacker.* Technical Report. Data & Society. 80 pages. https://datasociety.net/library/wearing-many-hats-the-rise-of-the-professional-security-hacker/

[44] Ben Green. 2021. Data Science as Political Action: Grounding Data Science in a Politics of Justice. *Journal of Social Computing* 2, 3 (2021), 249–265. https://doi.org/10.23919/JSC.2021.0029

[45] John Joseph Gumperz (Ed.). 2000. *Rethinking linguistic relativity: arises from a conference, Werner-Gren Symposium 112, held in Ocho Rios, Jamaica, in may 1991* (transferred to digital printing ed.). Number 17 in Studies in the social and cultural foundations of language. Cambridge University Press, Cambridge. Meeting Name: Wenner-Gren Symposium.

[46] Eileen Guo and Adi Renaldi. 2022. Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users. Retrieved 2024-09-13 from https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3/

[47] Catherine Hall. 2008. Making colonial subjects: education in the age of empire. *History of Education* 37, 6 (Nov. 2008), 773–787. https://doi.org/10.1080/00467600802106206

[48] Cathy Hannabach. 2023. Editing as Worldmaking: Critical Generosity in Editorial Practice (Keynote address). In *Editorial Freelancers Association conference.* Alexandria, VA. Retrieved 2024-09-12 from https://ideasonfire.net/editing-as-worldmaking/

[49] Sandra G. Harding. 2016. *Whose Science? Whose Knowledge?: Thinking from Women's Lives.* Cornell University Press, Ithaca. Retrieved 2024-09-12 from https://muse.jhu.edu/pub/255/monograph/book/48914

[50] Christina Harrington, Sheena Erete, and Anne Marie Piper. 2019. Deconstructing Community-Based Collaborative Design: Towards More Equitable Participatory Design Engagements. In *Proc. ACM Hum.-Comput. Interact.*, Vol. 3. 216:1–216:25. https://doi.org/10.1145/3359318

[51] Ayako A. Hasegawa, Daisuke Inoue, and Mitsuaki Akiyama. 2024. How WEIRD is Usable Privacy and Security Research?. In *33rd USENIX Security Symposium (USENIX Security 24).* USENIX Association, Philadelphia, PA, USA. https://www.usenix.org/conference/usenixsecurity24/presentation/hasegawa

[52] Sam Havron, Diana Freed, and Rahul Chatterjee. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *Proceedings of the 28th USENIX Security Symposium.* USENIX Association, Santa Clara, CA, USA. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[53] Chris Jay Hoofnagle and Jennifer M. Urban. 2014. Alan Westin's Privacy Homo Economicus. Retrieved 2024-09-13 from https://papers.ssrn.com/abstract=2434800

[54] B.A. Huberman, E. Adar, and L.R. Fine. 2005. Valuating Privacy. *IEEE Security and Privacy Magazine* 3, 5 (Sept. 2005), 22–25. https://doi.org/10.1109/msp.2005.137 Publisher: Institute of Electrical and Electronics Engineers (IEEE).

[55] Liesbeth Huybrechts, Henric Benesch, and Jon Geib. 2017. Institutioning: Participatory Design, Co-Design and the public realm. *International Journal of CoCreation in Design and the Arts (CoDesign)* 13, Special Issue: Co-Design and the Public Realm (2017), 148–159. https://doi.org/10.1080/15710882.2017.1355006

[56] Lilly Irani, Janet Vertesi, Paul Dourish, Kavita Philip, and Rebecca E. Grinter. 2010. Postcolonial computing: a lens on design and development. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* ACM, Atlanta Georgia USA, 1311–1320. https://doi.org/10.1145/1753326.1753522

[57] Craig Jarvis. 2021. *Crypto wars: the fight for privacy in the digital age a political history of digital encryption.* CRC press, Boca Raton (Fla.).

[58] Asnath Paula Kambunga, Rachel Charlotte Smith, Heike Winschiers-Theophilus, and Ton Otto. 2023. Decolonial design practices: Creating safe spaces for plural voices on contested pasts, presents, and futures. *Design Studies* 86 (May 2023), 101170. https://doi.org/10.1016/j.destud.2023.101170

[59] Auguste Kerckhoffs. 1883. *Military Cryptography or Ciphers Used in Time of War: With a New Process of Decipherment Applicable to Double-Key Systems.*

[60] Jeff Kramer. 2007. Is abstraction the key to computing? *Commun. ACM* 50, 4 (Jan. 2007), 36–42. https://doi.org/10.1145/1232743.1232745

[61] Brian Krebs. 2017. Post-FCC Privacy Rules, Should You VPN? Retrieved 2024-09-13 from https://krebsonsecurity.com/2017/03/post-fcc-privacy-rules-should-you-vpn/

[62] Thomas Samuel Kuhn and Ian Hacking. 2012. *The structure of scientific revolutions* (4th ed ed.). University of Chicago press, Chicago.

[63] Neha Kumar and Naveena Karusala. 2021. Braving Citational Justice in Human-Computer Interaction. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, Yokohama Japan, 1–9. https://doi.org/10.1145/3411763.3450389

[64] Ponnurangam Kumaraguru and Lorrie Faith Cranor. 2005. *Privacy Indexes: A Survey of Westin's Studies.* Technical Report. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf

[65] Justin Langlois. 2020. Recuperating Conflict: Between Critical Generosity and Antagonistic Activation. *Art/Research International: A Transdisciplinary Journal* 5, 1 (Feb. 2020), 148–157. https://doi.org/10.18432/ari29489

[66] Shaimaa Lazem, Danilo Giglitto, Makuochi Samuel Nkwo, Hafeni Mthoko, Jessica Upani, and Anicia Peters. 2022. Challenges and Paradoxes in Decolonising HCI: A Critical Discussion. *Computer Supported Cooperative Work (CSCW)* 31, 2 (June 2022), 159–196. https://doi.org/10.1007/s10606-021-09398-0

[67] Calvin Alan Liang, Emily Tseng, Akeiylah Dewitt, Yasmine Kotturi, Sucheta Ghoshal, Angela D. R. Smith, Marisol Wong-Villacres, Lauren Wilcox, and Sheena Erete. 2023. Surfacing Structural Barriers to Community-Collaborative Approaches in Human-Computer Interaction. In *Computer Supported Cooperative Work and Social Computing.* ACM, Minneapolis MN USA, 542–546. https://doi.org/10.1145/3584931.3611294

[68] Sebastian Linxen, Christian Sturm, Florian Brühlmann, Vincent Cassau, Klaus Opwis, and Katharina Reinecke. 2021. How WEIRD is CHI?. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, Yokohama Japan, 1–14. https://doi.org/10.1145/3411764.3445488

[69] Jessica McClearn, Lucy Qin, Emily Tseng, Miranda Wei, Rikke Bjerg Jensen, Nora McDonald, Elissa M. Redmiles, Morgan Klaus Scheuerman, and Reem Talhouk. 2025. Reflexivity & Reflection (R&R) for Sociotechnical Safety: Creating a Space for Collective Learning. In *Companion Publication of the 2025 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW Companion '25).* Association for Computing Machinery, New York, NY, USA, 138–143. https://doi.org/10.1145/3715070.3748292

[70] John J. Mearsheimer. 2014. *The Tragedy of Great Power Politics* (1st ed ed.). W. W. Norton & Company, Incorporated, Erscheinungsort nicht ermittelbar.

[71] Uskali Mäki. 2013. Scientific Imperialism: Difficulties in Definition, Identification, and Assessment. *International Studies in the Philosophy of Science* 27, 3 (Sept. 2013), 325–339. https://doi.org/10.1080/02698595.2013.825496

[72] Anita Nkonge. 2023. Worldcoin suspended in Kenya as thousands queue for free money. Retrieved 2024-09-13 from https://www.bbc.com/news/world-africa-66383325

[73] Safiya Umoja Noble. 2018. *Algorithms of oppression: how search engines reinforce racism.* New York university press, New York.

[74] US Department of Defense. 2017. DOD Dictionary of Military and Associated Terms. Retrieved 2024-04-20 from https://www.tradoc.army.mil/wp-content/uploads/2020/10/AD1029823-DOD-Dictionary-of-Military-and-Associated-Terms-2017.pdf

[75] Corey Pfluke. 2019. A history of the Five Eyes Alliance: Possibility for reform and additions: A history of the Five Eyes Alliance: Possibility for reform and additions. *Comparative Strategy* 38, 4 (July 2019), 302–315. https://doi.org/10.1080/01495933.2019.1633186

[76] Kavita Philip, Lilly Irani, and Paul Dourish. 2012. Postcolonial Computing: A Tactical Survey. *Science, Technology, & Human Values* 37, 1 (Jan. 2012), 3–29. https://doi.org/10.1177/0162243910389594

[77] Edward W. Said. 1979. *Orientalism* (1st vintage books ed ed.). Vintage Books, New York.

[78] Christine Satchell and Paul Dourish. 2009. Beyond the user: use and non-use in HCI. In *Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7.* ACM, Melbourne Australia, 9–16. https://doi.org/10.1145/1738826.1738829

[79] Herbert I. Schiller. 1991. Not yet the post-imperialist era. *Critical Studies in Mass Communication* 8, 1 (March 1991), 13–28. https://doi.org/10.1080/15295039109366777

[80] Linda Tuhiwai Smith. 2012. *Decolonizing methodologies: research and indigenous peoples* (second edition ed.). Zed, London.

[81] Rachel Charlotte Smith, Heike Winschiers-Theophilus, Daria Loi, Rogério Abreu De Paula, Asnath Paula Kambunga, Marly Muudeni Samuel, and Tariq Zaman. 2021. Decolonizing Design Practices: Towards Pluriversality. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems.* ACM, Yokohama Japan, 1–5. https://doi.org/10.1145/3411763.3441334

[82] Daniel J. Solove. 2021. The Myth of the Privacy Paradox. *THE GEORGE WASHINGTON LAW REVIEW* 89, 1 (Jan. 2021), 1–51.

[83] Katta Spiel, Kathrin Gerling, Cynthia L. Bennett, Emeline Brulé, Rua M. Williams, Jennifer Rode, and Jennifer Mankoff. 2020. Nothing About Us Without Us: Investigating the Role of Critical Disability Studies in HCI. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20).* Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375150

[84] The Mentor. 1986. Hacker's Manifesto. Retrieved 2025-11-04 from https://phrack.org/issues/7/3.html

[85] John Tomlinson. 1991. *Cultural imperialism: a critical introduction.* Pinter Publishers, London.

[86] Jennifer Urban. 2016. The Privacy Pragmatic as Privacy Vulnerable. https://doi.org/10.31235/osf.io/yh8nj

[87] Ari Ezra Waldman. 2019. Rationality, Disclosure, and the "Privacy Paradox". Retrieved 2024-09-06 from https://www.behavioraleconomics.com/rationality-disclosure-and-the-privacy-paradox/

[88] Miranda Wei, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M. Redmiles, and Franziska Roesner. 2024. {SoK} (or {SoLK?)}: On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. 7011–7030. Retrieved 2024-09-12 from https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-solk

[89] Alma Whitten and J D Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium.* 169–183.

[90] Marisol Wong-Villacres, Sheena Erete, Aakash Gautam, Azra Ismail, Neha Kumar, Lucy Pei, Wendy Roldan, Veronica Ahumada-Newhart, Karla Badillo-Urquiola, J. Maya Hernandez, Anthony Poon, Pedro Reynolds-Cuéllar, and Vivian Genaro Motti. 2022. Elevating strengths and capacities: the different shades of assets-based design in HCI. *Interactions* 29, 5 (Sept. 2022), 28–33. https://doi.org/10.1145/3549068

[91] World Health Organization. 2021. *"Nothing about us, without us".* Technical Report. Retrieved 2025-10-18 from https://www.who.int/europe/publications/nothing-about-us--without-us

[92] Robert J. C. Young. 2015. *Empire, Colony, Postcolony.* Wiley Blackwell, Chichester, West Sussex.

[93] Robert James Craig Young. 2020. *Postcolonialism: a very short introduction* (2d ed ed.). Number 98 in Very short introductions. Oxford University Press, Oxford (GB).

[94] Phil Zimmermann. 1995. Threats to the Net: Why do you need PGP? *The Ethical Spectacle* 795 (July 1995). Retrieved 2024-08-23 from https://www.spectacle.org/795/byzim.html

[95] Jonathan Zong and J. Nathan Matias. 2024. Data Refusal from Below: A Framework for Understanding, Evaluating, and Envisioning Refusal as Design. *ACM Journal on Responsible Computing* 1, 1 (March 2024), 1–23. https://doi.org/10.1145/3630107