The access control double bind: how everyday interfaces regulate access and privacy, enable surveillance, and enforce identity.

GARDNER, D.L. and TANENBAUM, T.J.

2024

The Access Control Double Bind: How Everyday Interfaces Regulate Access & Privacy, Enable Surveillance, & Enforce Identity

Daniel L. Gardner

Grand Challenges Initiative, Chapman University, dgardner@chapman.edu

Theresa J. Tanenbaum

Informatics, University of California, Irvine, tess.tanen@gmail.com

Abstract. Access controls are an inescapable and deceptively mundane requirement for accessing digital applications and platforms. These systems enable and enforce practices related to access, ownership, privacy, and surveillance. Companies use access controls to dictate and enforce terms of use for digital media, platforms, and technologies. The technical implementation of these systems is well understood. However, this paper instead uses digital game software and platforms as a case study to analyze the broader socio-technical, and often inequitable, interactions these elements regulate across software systems. Our sample includes 200 digital games and seven major digital gaming platforms. We combine close reading and content analysis to examine the *processes* of authentication and authorization within our samples. While the ubiquity of these systems is a given in much academic and popular discourse, our data help empirically ground this understanding and examine how these systems support user legibility and surveillance, and police identities in underexamined ways. We suggest changes to the policies and practices that shape these systems to drive more transparent and equitable design.

1 INTRODUCTION

"You could sit at home, and do like absolutely nothing, and your name goes through like 17 computers a day. 1984? Yeah right, man. That's a typo. Orwell is here now. He's livin' large. We have no names, man. No names. We are nameless!"

Matthew Lillard performing as Emmanuel "Cereal Killer" Goldstein in *Hackers* (1995)

Access control *procedures* often tied to an array of accounts are common requirements for our increasingly digitally enabled world. Personally authenticated accounts are necessary for a wide array of everyday collaboration and communication tools. Americans average between 4.6 and 8.1 social media accounts alone, varying across generational lines (GWI 2021). In 2007, Florencio and Herley found that a sample of half a million people had on average 25 password-controlled accounts (2007). While this average has almost certainly increased in the interim 16 years, a more current analogous study could not be found. Any increase in accounts is complicated by the fact that some of these accounts—notably Google and Facebook—support single sign on authentication APIs that other platforms use, meaning one account may control access to dozens or hundreds of other infrastructures. In addition to every social media platform, authorization and authentication are essential for accessing emails, work-related tools, online retailers, online-enabled software platforms, newspapers, gaming platforms, and various other websites or web-enabled services. The full scope of how many electronic systems with which we must negotiate access daily is staggering, yet these transactions often disappear into the background noise of our lives. Further, opting out of all these different technologies is hardly an option for any average active member of society.

Although we may collectively understand that digital media and games reside within broader software, platforms, and systems, there is still much to learn about the nature of how we interact with digital media *through* these systems. The general technical functionality of access control systems is well-documented and understood. However, these systems mediate more than finite technical procedures at the cusp of access; their influence stretches on through every following interaction within the domains they control, dictating privileges and privacy—inherently social processes. In addition, the design of the interfaces that manage these processes often fall to UI/UX teams, whose explicit focus is usability and whose objective is to get users to core content as efficiently as possible. Much like access control, usability is a necessary and valuable component of digital technologies, but its practice is full of potentially troubling maxims, such as making sure users "think" about the interfaces they develop as little possible (Krug, 2000). Positioning access control interfaces in the realm of UI/UX compounds our inattention to them, obscuring their broader consequences on digital media consumption and our everyday lives from general attention.

Computer scientist Mark Stamp has described how access control comprises authorization and authentication processes that "both deal with issues of access to resources" (2011: 4). Authorization "places restrictions on the actions of authenticated users" (Stamp 2011: 3), and authentication is the process of verifying a user's identity—or at least confirming that an identifier provided by a user matches one recorded by a given system as we will discuss in greater detail below. Stamp describes both these processes under the umbrella of access control. This general understanding of authorization and authentication is well-established and the technical means of employing these processes are no mystery. However, empirical accounts of the pervasive influence of these processes in digital domains are limited.

In this study, we interrogate the *role* of authorization and authentication in relation to digital media experiences. It is important to differentiate between the technical expressions of these processes and their broader, social meanings. These words encompass more than coded, automated, technical operations and have existed long before these technical means. At times, we may appear to conflate these terms with other digital functions. However, this seeming conflation is because we sometimes discuss technical elements commonly described as authorization and authentication that do in fact mediate these processes and other times we discuss technical elements that manage some aspect of these processes but are *not* commonly described by them. We use contemporary digital game software and platforms to re-examine how these processes that have only relatively recently become *attached* to media have changed those media and our experiences of them as a result.

Digital Games offer one powerful context for examining the broader influence of access control on digital media. They show how even a domain ostensibly prefaced on fun, frivolity, and liminal escapism is not exempt from these transactions of authority, identity, and surveillance. Further, digital games represent a difficult to disentangle amalgam of the complexities of traditional games *and* software. Many scholars have debated what is or is not game, play, or gameplay (Avedon & Sutton-Smith 1971; Juul 2011; Strenros 2017; Salen-Tekinbas & Zimmerman 2003; Suits 1990). However, regardless of how these phenomena are theoretically understood in a broad sense, *digital* games and gameplay are embedded within technical infrastructures that mediate our access, interactions, and experiences. Although the interfaces that support access control may be a part of contemporary digital gaming and can at times manifest outcomes *during* gameplay, they are *not* a part of any common conception of games or gameplay. The protections and affordances digital access control mechanisms support in relation to digital games represent broader contemporary software industry best practices and function much the same as those attached to other digital platforms and applications, and are subject to the same greater challenges that face all software. Though our analysis may provide insights about gameplay and for game scholars, our focus is on the infrastructures and mediations that *surround* digital games and have implications for similar infrastructures across digital media. Juxtaposing access control mechanisms and play simply serves to highlight the reach and influence of these practices *and* interfaces.

In this paper, we look at digital games as a case study for how access control systems help regulate our broader experience with software systems, platforms, and technologies and potentially support inequities of information. We rely on a sample of seven digital distribution and gaming platforms and 200 digital games. Our data help to empirically ground common assumptions about these functions and begin to improve our understanding of how these ubiquitous, otherwise mundane, systems restrict digital activities, enable user surveillance, and police identities. Our findings discuss software released for use on personal computers or proprietary gaming hardware observed in the United States. However, while the expression of the relationships we identify—or specific outcomes and terms—likely vary based on region (e.g., in response the EUs General Data Protection Regulation (GDPR)) or platform (e.g., smart phones), our insights into the general

regulatory relationships these interfaces have with digital media should translate to broader applications.

The two primary high-level research questions that motivated this research were: How do access control interfaces influence our experiences with digital games? And how do these systems influence, regulate, or enable functions and outcomes beyond access control? Although fully answering every dimension of these questions is beyond the scope of any single study, our approach and findings begin to answer pieces of them and highlight underexamined regulatory elements of access control technologies and policies that are too often *assumed* necessary. However, we do not suggest removing or replacing access controls for purposes of security or legibility. The double bind of access control is that despite the issues we describe here, *some* form of it will likely remain necessary. Instead, we suggest a more holistic perspective on the role of these processes and suggest some ways to improve the transparency, equity, and user experience and autonomy within these systems. We offer two main contributions: For game scholars, we complicate conceptual constructions of the contemporary phenomenon of digital gaming by foregrounding infrastructures that undergird broadly applied models describing the boundaries of gameplay. For digital designers more broadly, the human-computer interaction (HCI) community, and users, we support a greater understanding of the tensions between membership and participation in these systems—the surveillance and control that participation assumes—and the degree of autonomy users might express or demand as subjects to these systems.

2 TECHNICAL AND SOCIAL PROCEDURES, AND CONSEQUENCES

Interfaces that demand assent to End User License Agreements (EULAs) and Terms of Service (ToS) are not often described, in a technical sense, as access controls but they do function to *authorize*—a mode of access control described by Stamp above and employed by bouncers of trendy clubs since ancient times through nods and pointed thumbs. EULAs and ToS "place restrictions on the actions" of users *and* software/platform companies. Although EULAs and ToS are not precisely the same documents, we group them together in this paper because we observed them defining overlapping terms, and their shared core function is determining the conditions of continued access and use. Interestingly, these authorizations work in two directions. Firstly, the obvious authorization of users. In a broader, more traditional sense, however, users assenting to these documents with the click of "I agree" also *authorize* software/platform company claims related to ownership, rights, and behavioral expectations, as well as access to certain resources such as user data.

Through the interfaces that present them, EULAs and ToS confirm expectations for certain services while maintaining some legal protection over intellectual property and restricting certain actions (by both users and companies). The precise terms of these documents may vary by media, platform, company, or global region but always define the legal and day-to-day responsibilities of users, platforms, and software publishers and dictate the consequences of violating conditions, such as loss of access or legal prosecution. What is uniform, is the *relationship* these interfaces have to the media they are attached to and how the interaction with these interfaces serves as authorization and access control, to software, platforms, *and* user information.

We may take for granted that submitting to the "legal regimes" EULAs and ToS represent requires users to conform to explicit "conditions under which [continued] access is permissible or not," and whatever sorts of actions or conduct they define as permissible (Burk 2010: 9, 11). However, scholarly considerations of EULAs and ToS often focus only on how the the transaction of assent can be improved (Böhme and Köpsell 2010; Good et al. 2007; Kay and Terry 2010; Nejad et al. 2016; Nejad et al. 2017; Obar & Oeldorf 2020; Turow 2003; Waddell et al. 2016), rather than how the presence of these interactions influences a broader socio-technical ecology or how they formalize, mechanize, and prolong previously abstract or informal relationships.

Identity verification systems that *authenticate* users may be more immediately recognizable as access control. The different formats of authentication we users must submit to in return for access software or a given platform constrain what information, platform services, or games we may access—and ideally, what information or assets of *ours* others may access. Identify verification/authentication also differentiates individual users for the sake of online interactions.

Recurring, everyday authentication, however, can exert power over individuals over time. In the most basic, pragmatic, and justifiable sense, authentication exerts power by limiting what content, services, or information users may access—a reasonable and often desirable outcome for all involved. Not always so obviously, perhaps, authentication is also *the* function that labels users for the sake of online interactions and surveillance. This surveillance is less consistently for the benefit of all involved, though it *does* often serve the needs of users. Too often, however, consistent authentication needs and surveillance practices encourage companies to require identifiers that remain static from the moment users first establish them, tethering users to names that may no longer apply due to common (and less common) life events such as marriage, divorce, religious conversion, or gender transition.

Much like submission to EULAs and ToS, the *presence* of authentication is often taken for granted and the systems that mechanize these processes are well studied. However, these studies often focus on how authentication transactions and services influence the integrity of specific technologies or how the efficacy or usability of these systems can be improved (Bonneau et al. 2012; Routi et al. 2015; Sirivianos et al 2014; Somayaji et al. 2013), rather than how pervasive authentication systems alter broader processes and the experiences of media production or consumption.

Access control interfaces, such as those that manage authorization *and* authentication processes, establish a variety of ongoing relationships with users that go beyond the transactional enforcement of permissions and access, and beyond the core media these processes surround. Users are authorized for conditional access and in return authorize software publishers, digital service providers, and retailers to track details about their consumption and use. Users authenticate a recognized identifier to confirm their privilege to content and information and to validate collected data that may or may not be used for their benefit, while potentially denying actual aspects of themselves in the process.

A key outcome of access control that begs questions beyond the well-trodden territory of security, is how these systems enable or enforce consistent, linkable, *legibility*. We use legible in the sense

that is used by Michel Foucault and James Scott to describe how an institution *sees* or—more importantly—*discerns* individuals subject to those institutions (Foucault 1977; Scott 1998). Companies that need to differentiate users for access and/or that rely on large-scale data collection as a component of their technological services and revenue streams require means for making individual users legible/discernable. Authentication fulfills this need and authorization makes the process permissible.

The structural and functional parallels between contemporary digital authentication systems and those employed by historic states or institutions to verify the identities of—or track—*their* citizens or members include pragmatic similarities in their specific implementation. For example, Scott describes the imposition of surnames in England and Italy to better track tax and tithe collection. Just as individuals might choose surnames in these cases to reflect their profession or another element of their identity (e.g., Smith, Cooper, or Woods), we also often index aspects of our identities when naming accounts or other facets of our media use (Crenshaw & Nardi 2014). Contemporary account identifiers act as additional surnames, whether they use our names, email accounts, selected username, or random number string. In both the historical and contemporary context, "some second designation [is] absolutely essential for the records, and, if the subject suggested none, it [is] invented for him by the recording clerk" (Scott 1998: 67-68), or by the authentication interface (e.g., "how about randomusername12345?")

In many contexts, companies *and* users benefit from this legibility. Companies being able to tell users apart means they can take the correct action against the correct user for malicious behavior and charge the correct user's payment information for purchases. Unfortunately, however, as discussed in greater detail below, authentication can also support opaque data-driven practices, and can too often treat user's names or account names as immutable indicis that inflexibly dictate facets of our relationships with these platforms and services over time.

Access control interfaces formalize and mechanize transactions of *permission* and *identification*. Authorization settles terms for how users are permitted to interact with software or platforms and authentication dictates—to an extent—who we are permitted to *be* during use. Access controls confirm ownership, maintain security and privacy, and in these digital contexts make many data-driven practices possible—including for the benefit of users. However, these same systems often establish and enforce a variety of under-acknowledged, and potentially inequitable relationships between users and those who produce the software and services to which they are attached (Stylianou et al. 2015).

2.1 Accessing Gameplay

There is a continuous stream of scholarship dedicated to defining what *are* games, play, or gameplay (e.g., Avedon & Sutton-Smith 1971; Juul 2011; Salen-Tekinbas & Zimmerman 2003; Strenros 2017; Suits 1990). There is a growing body of literature around the accessibility and games, play, or gameplay mostly related to an array of physiological impairments (e.g., Baltazar et al. 2022; Garber 2013; Hassan and Baltzar 2022; Miesenberger et al. 2008; Porter and Kientz 2013;

Said and Kane 2013; Yuan et al. 2011). However, aside from some technical approaches described in the following section, there is little to no work examining the simple procedural methods of how access to play, games, or gameplay is *controlled*, particularly digitally.

To be fair, authorization and authentication are unlikely elements to include when describing games and gameplay generally. We would not begin describing a game to a potential player with access controls. However, play and game theorists such as Elliot Avedon and Brian Sutton-Smith or Bernard Suits have examined the "voluntary" nature of play and how players assent to—and so authorize—the rules that define gameplay and player roles within it (Avedon & Sutton-Smith; Suits 1990). There have always been processes to determine who is playing a given game as well, such as asking friends directly, traumatically picking teams during recess, or any of a host of other metagames players might utilize to *authenticate* participation and/or team membership. However, until games became game software and digital, computational phenomena, these processes were rarely formalized or automated thresholds of gameplay. Precisely because certain conceptual characteristics of games or play may remain unchanged by their entanglement in digital technologies, studying the features that are different and new can help us learn more about games and play, as well as the new mediums through which we access them. Despite their ubiquity, authorization and authentication interfaces that resolve legal assent and verify identities as means of enforcing everyday access are one important, relatively new component of games as they have become embedded in networked software.

3 RELATED WORK

This work builds on research at an intersection of HCI, social science, and media and game studies such as Susan Leigh Star (1999), T.L. Taylor (2006), Noah Wardrip-Fruin (2009, 2020), Alexander Galloway (2009, 2012), and Gardner and Tanenbaum (2021), who all suggest looking beyond the immediate experiences and obvious functions of games and/or information technology. Star suggests we must study the "hidden mechanisms subtending those [more familiar] processes" to better understand essential aspects of their operation and design (1999: 377). Although access control itself is not always a hidden mechanism, many facets of its operation and outcomes it supports are made less visible by their mundane ubiquity, or are intentionally obscured. Describing "issues not seen as central in the retellings of … games," Taylor describes how *boundaries* "can be the place in which definitions become problematized or previously hidden practices are accounted for" (2010: 10). Access Controls are an explicit boundary, and this paper observes unaccounted aspects of their implementation. Wardrip-Fruin urges us to consider the "operational logics" defined by the patterns of data, process, interaction, and intent beneath the "surface" that users or players experience, which nonetheless shape their experiences of that media (2009, 2020). Galloway's "non-diegetic machine actions" encompass a variety of processes and functions that must all be present and operational for digital media to be consumable, but that aren't commonly included in our collective articulation of that media (2009). Gardner and Tanenbaum describe the importance of examining peripheral-to-gameplay interfaces in digital games—such as access control interfaces—and suggest a "periludic" lens to highlight broader relationships dictated by

these interfaces "on the periphery" of familiar media and technology (2021). They argue that examining these interfaces in games can provide insight about broader digital contexts and emphasize the different ways interfaces designed to operate *between* users and the games/media/services/functions for which we come to digital contexts exert observable power over our experience. We apply the reasoning of these scholars to move beyond a lens of efficacy and investigate some of the broader socio-technical implications of access control in digital games and beyond. We position this study within two primary literature categories: Access control and HCI, and legibility, linkability, and memory.

3.1 Access Control and HCI

Apart from a growing number of studies concerned with too often discriminatory implementations of facial recognition-based authentication (Buolamwini & Gebru 2018; Raji et al., 2020; Scheuerman et al., 2020), the study of access control in the HCI community primarily focuses on functional security or general efficacy and usability (e.g., Bonneau et al. 2012; Marky et al. 2022; Routi et al. 2015; Sirivianos et al 2014; Somayaji et al. 2013). The scant studies that address access control in digital games similarly tend to examine functional security for game software or services (Assiotis & Tzanov 2006; Dotan 2010; GauthierDickey et al. 2004), or games used *as* access control (Boella et al., 2005). Although building more secure systems is essential work, surprising little research in the HCI community explores the broader socio-technical relationships enabled by these processes attached to our everyday use of interactive technologies.

Studies of the effectiveness and usability of authentication are especially common (e.g., Bonneau et al. 2012; Marky et al. 2022; Routi et al. 2015; Sirivianos et al. 2014; Somayaji et al. 2013). Although the findings in these studies provide insights on immediate transactional interactions, how authentication systems integrate into users' lives more long-term is reasonably beyond their scope. Somayaji et al. do offer an example of considering users' lives, but only insofar as they may be leveraged to create more "usable" but still complex, difficult to crack narrative-based authentication (2013).

Sirivianos et al. bring in broader social contexts to examine how leveraging social connections could make authentication more reliable—and invasive—by strengthening links in the webs of information connected by identity verification (2014). Sirivianos et al.'s stated goal is increasing "trust" while maintaining individual anonymity. However, their solution relies on users becoming *less* anonymous to their platforms by linking additional dimensions of personal information—and information related to friends and other connections on social networks. Their technical solution counters their own stated goal by increasing linkability and decreasing anonymity. In addition, Sirivianos et al. explicitly describe how their solution circumvents current social network API terms of use to collect and retain accurate information in a questionable ethical move. Sirivianos et al.'s study, which prioritizes technical efficacy without fully acknowledging personal and ethical implications, is an exemplar for why the sort of analysis we provide in this paper is essential. Efficacy and integrity *are* important, but they cannot come solely at the personal cost of user privacy and autonomy.

Other studies provide insight into how formal and informal processes of authentication may influence social interactions *through* the digital platforms they support (e.g., Cho & Kwon 2016; Wang et al., 2017), while other scholars have studied how anonymity more broadly—often prevented by authentication—influences online interaction (Dahlgren 2005; Kushin & Kitchener 2009; Lampe et al., 2014; Ma and Agarwal 2007; Papacharissi 2004; Ruiz et al., 2011). Though not always directly, these studies all illustrate how authentication can impact behavior, community, and ~~general~~ relations with fellow users, and suggest non-technical consequences of these processes in digital contexts. Our study adds complexity to these analyses by highlighting additional underexamined technical and processual relationships und outcomes authentication can establish between platforms that require it and users.

As with authentication, few HCI scholars consider the role of authorization beyond improving the systems through which it is obtained, or addressing the fairness of terms (Böhme and Köpsell 2010; Good et al. 2007; Kay and Terry 2010; Nejad et al. 2016; Nejad et al. 2017; Obar & Oeldorf 2020; Turow 2003; Waddell et al. 2016). Too often, this research tends to treat accepting EULAs and submitting to similar authorizations as a necessary given and focuses on aligning attention and comprehension with assent or general usability. Though some scholars have acknowledged that certain socio-technical systems—such as smart cities, for example—rely on authorization for infrastructural stability and cohesive administration (Lämmel et al., 2017), many more general relationships remain under-examined. Scholars such as Lippi et al. (2019) and Drawzewski et al. (2021) attempt to provide some tools to potentially *disrupt* assent by notifying users of "unfair" clauses. However, outcomes beyond the acquisition of assent are rarely fully explored or remain unaddressed.

Scholars often acknowledge or treat as a given that many users do not understand or even engage with the content of EULAs, ToS (Turow 2003, Obar & Oeldorf 2020), further problematizing assumed assent. Felt et al. find that even with high rates of accepting permission requests—*authorizing* application permissions on a device—only a very small minority of users (3% of 308 survey respondents) displayed awareness and understanding (2012). Several scholars have suggested methods of simplifying, dispersing, or otherwise annotating or re-presenting terms to make key clauses more accessible to a wider array of users (Waddell et al. 2016; Kay and Terry 2010; Nejad et al. 2016; Nejad et al. 2017). However, Good et al. observed complementary findings that adding a summary statement before or after presenting EULAs led to more engagement and greater comprehension of terms, but also to significantly reduced software installations and more expressions of regret and uninstalls shortly after installation (2007). Further, Böhme and Köpsell found in a sample of 80,000 users that people were more likely to accept even coercive terms, the more they resembled a standard EULA, as opposed to more polite or clearly articulated terms (2010).

This previous research highlights how assent can be more easily tied to presentation and the interfaces used to obtain it than content—and that comprehension decreases acceptance. These are troubling findings about the nature of our digital landscape that highlight the need for studies like ours focused on the broader processual implications of these interfaces. If greater engagement with

EULAs increases regret and uninstalls as Good et al. find and even deliberately unfavorable language does not dissuade users as Böhme and Köpsell and Obar & Oeldorf find, there is little to motivate companies to clarify terms or improve transparency. Instead, software companies are incentivized to streamline authorization mechanisms into as simple and forgettable an interactive experience as possible. Good et al.'s study especially begs us as a community to go beyond usability, accessibility, awareness, and comprehension, to examine the actual consequences of these broadly—and too often blindly—assented-to terms and conditions. With this paper, we hope to enhance the discourse around these topics and shift our fundamental perspective on these systems.

There are precious few studies that provide deeper analysis of the *conditions* set by EULAs or ToS themselves. Two exceptional recent articles related to games examine how epitextual server rules and "codes of conduct" can positively impact player communities (Jagannath & Salen 2022; Grace et al. 2022). However, Willson and Leaver (2015), Yeol Roth (2015), and law Scholars Stylianou et al. (2015) and Dan Burk (2010) are some of the few to closely analyze the stakes of the ToS that determine default software access. Willson and Leaver provide probably the most direct example of the *kind* of work we suggest is necessary by describing exploitation of players of "social games" that leverage assent to ToS and social media authentication to data mine massive networks of activities and interests (2015). In their example, "villain" game publishers appear to specifically rely on an assumption that players will not read ToS to ensure ethically dubious services *disguised* as games are permissible. Roth describes ToS as "basic units of governance in the relationship between service providers and individual users," in his case leveraged disproportionately to moderate/censor gay user-generated content online (2015: 3). Stylianou et al. provide a comparative analysis of several cloud-hosting platforms and identify how power asymmetries permit companies to maintain abusive practices (2015). Burk describes how "technical design may be deployed to control behavior" through the "legal regimes" these documents define, and the methods through which they are presented and enforced (2010: 6).

Our examination of the mechanisms through which we *enter* relationships like those Roth describes, become subject to Burk's "legal regimes," and submit to a range of potentially inequitable power asymmetries is in direct conversation with Böhme and Köpsell's, Good et al.'s, Roth's, Stylionou et al.'s, and Burk's findings. Böhme and Köpsell's, and Good et al.'s analysis highlight how companies are incentivized to optimize these systems for inattention and neglect to favor their own priorities. Willson and Leaver's, Roth's, Stylionou et al.'s, and Burk's findings highlight how these intentionally inattentive interactions can compound intentionally inequitable outcomes for users. Our study brings these analyses together to highlight additional mechanical components of these processes and their longer-term consequences.

3.1.1 Privacy Settings

Privacy settings are a gray area in relation to the scope of this research that we need to briefly acknowledge. Privacy policies may be dictated by EULAs or ToS but ongoing privacy settings are often managed by an independent interface—a feature other dictated terms do not benefit from. As such, while the *establishment* of these privacy policies may be within the scope of our analysis, the

systems that manage ongoing preferences or settings are not. However, there are insights from research on privacy settings and notifications worth considering. Though some acknowledge and argue against "dark patterns," research in this area within the HCI community still too often focuses on "effective" and "efficient" design much the same as with above topics (Frik et al., 2022; Li et al., 2022), or on providing ethically ambiguous insights about what user characteristics make them more or less likely to exchange privacy for use (Alsoubai et al., 2022; Jin et al., 2021). Unlike research about authorization and authentication more broadly, however, there are scholars who recognize assent is often opaque (Anton et al. 2004; Gomez et al. 2009; Nissenbaum 2010) and should not be treated as a given (Liu et al., 2022). Others examine how some groups may be more vulnerable to the risks involved with how privacy is managed based on—for example—socio-demographic membership or western-centric designs (Frik et al., 2022), or explore how collective action may be leveraged to overcome the inherent power differentials bound to these systems (Wu et al., 2022). Seberger et al. argue for how privacy should be studied "beyond the point where the thumb meets the screen," to encompass users' broader experiences (2022). Although we do not have space to include a deeper discussion of privacy settings in this paper, we see these insights as aligned with our purpose and as an opportunity to bring these two overlapping, co-dependent domains into greater dialogue.

3.2 Legibility, linkability, and memory

Linkability and memory are related concepts in the context of systems that identify and track our activity. Linkability is described and applied in a variety of fields to describe relationality between distinct events, contexts, and times (Backes et al., 2016; Clauß 2006; Cvrček et al., 2005; Pfitzman and Köhntopp 2001; Zimmer et al., 2020). Memory is a repository of events linked by our experience across contexts and time. Phenomena must possess some essential level of legibility to establish linkability or be memorable.

Computer, data, and security scholars Pfitzman and Köhntopp argue "unlinkability" is a prerequisite for anonymity (2001). They describe unlinkability as when two or more "items are no more and no less related than they are related concerning the a-priori knowledge. This means that the probability those items being related stays the same before (a-priori knowledge) and after" encountering them (2001: 2). In this sense, any sort of identity verification or authentication is automatically inconsistent with anonymity. Authentication makes otherwise distinct humans, gameplay events, and platform-related or social media activity clearly *linkable* (often for purposes of monitoring and data collection) by the consistent use of a verified account or identifier (even a pseudonym).

Scott's account of institutional *sight* and surnames is a story about institutions developing systemic memory to make individuals and their tax or tithe activities distinct, legible, and *linkable* in records (1998). This legibility helps the institutions track who they are collecting money from and helps individuals avoid double taxation/tithing. As we began to describe in the above, we apply elements of Scott's analysis to account names and the processes that digital platforms rely on for user legibility and linkability.

Several scholars have observed how data collection and surveillance practices occur across social media, varying software industries, and digital contexts (Caplan & boyd 2016; Clarke 1988; Egliston 2020; Gregg 2015; Haggerty & Ericson 2000; Seaver 2019; Zimmer 2008). Haggerty & Ericson's idea of the "data double" (2000), which software and platform companies create using data collection and surveillance practices authorized by EULA assent and enabled by authentication, is essentially a persona of *us* built from *linked* activity. Our names, account names, or emails provide a persistent index that labels the records of all our activity related to a given software, platform, or network of connected platforms, ensuring that any data on that activity is *legible*. Each time we authenticate, we validate the reliability and integrity of data collection. These data allow companies to create descriptive and predictive algorithmic models that ideally help them encourage or optimize certain behaviors within their domains, not necessarily in the immediate best interests of users.

Scholars and journalists have observed how the algorithmic content that surveillance so often fuels can gently narrow our perspectives, sow social division, and curb critical, reflective thought (Finkelstein 2016; Levy 2021 Rainie & Anderson 2017; Sadagopan 2019; Seaver 2017; 2019; Singh 2019; Willson 2017). Anthropologist Nick Seaver describes how the algorithms that shape, confine, or filter our digital experiences are a "trap" users become "ensnared" by (2019). If algorithms are traps, *authentication* is what triggers their firing, and *authorization* provides permission. Seaver also writes critically elsewhere about how algorithms are too often considered only as "conceptual objects indifferent to implementation details," demanding longer-term, ethnographic accounts of their *impact* (2017:1). Similarly, in line with Seberger et al. above regarding privacy settings (2020) as well, we suggest the need to move beyond considering the access control mechanisms through which users are enrolled in these algorithms as a condition of accessing digital media as more than conceptual or technical objects, indifferent to their implementation.

Gender studies philosopher Marie Draz helps to bring other essential, critical, less security-driven consequences of these systems and legibility into focus. She describes how the experiences of transgender individuals foreground the potential harms of the "externalization of memory" that occurs when we invest infrastructures with authority over aspects of our identities (2018). She highlights how our institutions and infrastructures deploy rigid classification schemes for gender and sex when recording individuals within our information systems, often leading to situations where the same individual is registered under multiple names and gender markers across private, corporate, local, state, and federal data systems (Draz 2018). Draz describes how there are real consequences for anyone whose daily lived experiences are incongruent with the externalized memory maintained by identity infrastructures, or for whom the terms of their legibility are externally defined:

> "The effects of being illegible within a particular classification system are intensified by one's location in intermeshed systems of power such as race, class, nationality, and ability […] As one

result of this interplay between a lack of consensus and the countervailing certainty that it must be possible to legislate a sexed body, identity documentation remains a source of harm." (Draz 2018: 9)

Draz describes how information systems can exert power over us in ways that disproportionately harm some people and not others through identity documents—akin to account identifiers—when there is a conflict between their "lived" and their "documented" name and gender:

"While for many people such documents are barely noticeable (a *mundane* matter of paperwork), the memory is sufficiently punishing for others. Regardless of how someone is living, or how others affirm their lived gender, the past assignment preserved at this level can resist forgetting. The documentation too easily serves as a reminder; this memory, in turn, is used to either support or contradict the present. For those who are privileged by current arrangements, for whom the memory is more or less "correct," these systems of classification do not feel punishing. To the contrary, they feel quite boring." (Draz 2018; 10, emphasis added)

Draz highlights how systems of legibility are experienced in radically different ways by those for whom they represent a basic administrative function and those for whom they represent a denial of their existence. For example, she discusses how the largest survey of trans people in the US to date "found that only 11 percent of respondents had their preferred name and gender on all IDs and records, while 67 percent" did not have any identification or records with their preferred name and gender (2018: 10; Grant et al., 2011; James et al., 2016). Having basic identification that matches who we *are* demonstrates a bare-minimum acknowledgement of that identity by society, or a digital platform.

These examples show the potential for harm that occurs when there is a breakdown between the expectations of those who implement authentication and the expectations of users who must accept these systems as a condition of everyday media and software access. Scholars have analyzed how certain assumptions about gender may be "baked into" designs, policies, and practices (Haimson and Bivens ..), how social media may frustrate or interfere with identity and life transitions (Haimson & Hoffman 2016; Haimson et al., 2016), or even how academic publishers may enforce author names in ways that do not permit scholars to decouple from potentially traumatic past designations (Tanenbaum 2020; Tanenbaum et al., 2021). However, Draz's analysis applies beyond the context of gender and these more specific contexts. One of our central concerns is how the potential harm she describes is emphasized whenever systems of authentication are invested with authority over the actions, identity, and legibility of the people who use them, and when those systems are opaque, inflexible, and compulsory.

4 METHODS

We used hermeneutics and content analysis to examine the authorization and authentication interfaces, as well as the contents of EULAs and ToS, in a sample of seven digital game software

distribution and gaming platforms and 200 digital games hosted by one of those platforms. Hermeneutics helps better understand how media format and content may be experienced, built on evidence from close reading media and the expertise of an observer (Føllesdal 2001; Gadamer 2006; Tanenbaum 2015). Content analysis helps with systematically collecting and organizing evidence of pervasive themes in the mechanisms and content we observed (Cole 1988; Creswell & Creswell 2017; Downe-Wamboldt 1992; Hsieh & Shannon 2005; Saldaña 2015).

We used hermeneutics to make qualitatively reasoned claims about how access control interfaces and processes may come to matter by participating in the same activities users would when accessing these games. We observed all layers of access control attached to platforms and game software that a player would be required to interface with to access gameplay, and any terms and conditions to which players would become subject during this process. The core of our hermeneutic inquiry was *using* each interface that managed assent to documentation and verified identities while taking extensive notes and screenshots and organizing quantitative details in a spreadsheet for content analysis. We participated in account creation, account login/identity verification, and all aspects of the platforms we were *required* to interact with to access core gameplay experiences. Although we had to use an existing account to access the game library, we created new accounts for the purposes of observing each platform.

We examined the content of all EULAs and ToS to identify consistent themes in the conditions resolved by the interfaces that manage assent or dictate authorization. One author conducted an initial pass observing, noting, and screenshotting all interfaces and associated documentation before applying emergent, conceptual, and thematic coding (Saldaña 2015). We identified notable themes and conditions in all required licensing or account-holder agreements and terms as encountered and both authors reviewed and discussed these coded themes until agreement was reached. One author observed, noted, and took screenshots of any element of the platforms and game software we encountered that they perceived as related to either authentication or authorization to round out our understanding of the outcomes they can produce (e.g., personalized content or elements labeled with account names and evidence of data monitoring such as play times or play history information). Both authors reviewed and discussed all collected evidence until agreement was reached.

Four of the seven digital game software distribution and gaming platforms were PC-based and three were home-gaming consoles. We only included platforms that provide distribution *and* mediate access and hosting services for everyday gameplay. The PC distribution platforms chosen were Blizzard/Activision's Battle.Net, EA's Origin, Valve's Steam, and Ubisoft's uPlay as they were the most successful or prominent distribution platforms at the time of data collection, with no other platform at the time having a notable portion of the market in North America. For instance, sales through Steam alone accounted for approximately one-sixth of all digital game sales in the United States in 2017 (Bailey 2018; ESA 2019). Steam sells and hosts games for an extensive roster of publishers that create a wide variety of types of games and supports insights about a wide array of game software development companies. Battle.Net, Origin, and uPlay only support games published by one company. The home-gaming consoles we examined were Nintendo's Switch,

Microsoft's Xbox One and Sony's Playstation 4, the three most prominent gaming consoles at time of observation. Like Steam, all three support a diverse array of games and publishers.

We sampled game software from Transformative Play lab's 1500+ game Steam Library at University of California, Irvine. Lab affiliates, local game publishers, friends, and families contribute to this library. It contains a wide variety of games representing diverse tastes and genres. We chose the games in our sample by progressing through the alphabetized list randomly based on rolling a die to mitigate selection bias, and additional selection criteria unrelated to access control described in a previous article (Gardner and Tanenbaum 2018). This previous article investigates details related to character configuration interfaces in sampled games, so games without characters did not meet the selection criteria. The initial data collection and analysis presented in this paper began in response to a secondary research question for this earlier article but grew beyond the capacity of that paper. Based on the ubiquity of our findings and the lack of reference to characters in any of the EULAs we read, however, we are confident this additional criterion had little or no effect on our results. The oldest game was originally released in 1999 (though re-released for Steam much later), the newest was released in 2015. We coded 101 games in our sample as published by larger "AAA" game companies and 99 as published by smaller "indie" companies. A complete ludography can be found at: https://dang.page/ludography.

Because updates, expansions, and unlockable content are common with game software, and these changes can potentially alter conditions of access control, our data collection is a snapshot of a point in time. To mitigate this potential issue and be as consistent in observations as possible, we observed all game software as a fresh installation at time of collection and ignored any unlockable, extra, downloadable, or purchasable content. EULAs and ToS are similarly subject to change and our findings represent a snapshot here as well. Data collection completed in 2019.

5 FINDINGS

Confronting interfaces that managed bidirectional authorization of users *and* the conditions contained in EULAs and ToS as well as interfaces that authenticated account information was a condition of accessing every platform and all game software we observed. We were consistently required to assent to two to three EULAs and/or ToS and verify an identifier one to two times to access all 200 games. All sampled game software was installed through Steam, subsuming them in the platform's access control features. Because every platform observed required assent to a EULA and identity verification, a minimum of one layer of authentication and authorization would also have been required to access games on the other platforms observed as well had we observed them there for the same reason, and at least two layers of assent would be likely.

5.1 Authorization: accounts and assent

Empirical accounts of EULA and ToS assent is essential to contextualize later findings and analysis. As stated, all platforms required assent to some form of terms when creating an account necessary to access that platform, or to access key functions of that platform (more details below). The conditions associated with platform accounts regarded user interactions with platforms and their

role as both digital retailer and game library manager. All game software observed required assent to a EULA during installation. Game software EULAs described the conditions of accessing that specific game software artifact. Nineteen of the 200 games included a requirement to assent to a third set of conditions attached to a game publisher specific account that resembled platform accounts—except only associated with that publisher's game software. All nineteen of these games were published by AAA-coded publishers and were released after 2010, suggesting this to be a comparatively recent practice by larger companies.

We did not always observe clear or immediate access to the terms to which we were assenting. Two of the seven platforms and *all* game software—hosted on Steam—displayed EULA conditions as a visible feature—and result—of Steam's standardized authorization interface format (e.g., Figure 1). The other five platforms used a link to a separate screen or externally hosted document containing the conditions to which we were assenting (e.g., Figure 2). Clicking these links, accessing, or scrolling through those conditions was *not* a requirement of authorization or access in any interface. Because all game software observed was hosted by a distribution platform—as is standard in the contemporary ecosystem—all games observed were automatically subject to the additional layers of authorization and conditions defined by those platforms, as would any games we *would* have observed on the other platforms. Table 1 summarizes the occurrences of different assent acquisition formats.

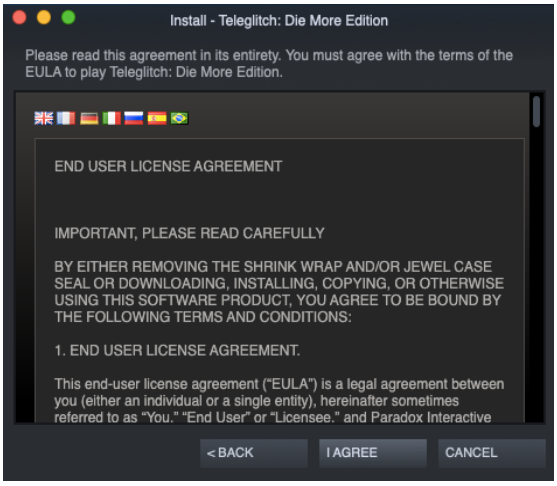

Figure 1: Screenshot by authors of example of game software EULA from Steam Platform with visible/available terms and "I agree" button

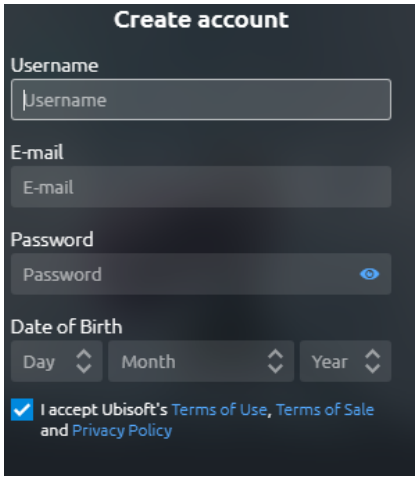

Figure 2: Screenshot by authors of example of account creation with links to EULAs and check box with "I agree/accept" label from Ubisoft account creation

Table 1: Summary of authorization interface formats for acquiring assent and presenting EULAs.

Sample	% of sample requiring assent to at least one EULA/ToS to access	% of sample requiring assent to two EULAs/ ToS to access	% of sample requiring assent to three EULAs/ ToS to access	% of immediately visible conditions	% of linked external conditions
Seven Platforms	100%	0%	0%	29% %	71%
200 Games	100%	100%	9.5%	100%	0%

Authorization interfaces relied on two designs for acquiring interactive assent: the first was a button labeled "I agree" or similar (e.g., Figure 1). The second was a check box with "I agree" or similar next to it (e.g., Figure 2). All game software had a templated authorization interface to manage their initial assent provided by the Steam platform (Figure 1). The details of the authorization interfaces games used to acquire any third assent to conditions varied visually but followed one of these two formats. In line with Böhme and Köpsell's findings, it appeared that all companies prioritized formats that followed broader EULA assent standards.

5.2 Authorization: Terms, conditions, ownership, and licensing

All EULAs we observed dictated the terms under which players were granted license to access respective distribution platforms or game software. *All* these documents explicitly identified publishers as the owners of all assets, whether software or intellectual in nature, regardless of ownership of the device upon which said software was installed. Players would only be permitted

to maintain accounts and access to relevant software provided they abided the terms within these documents—whether or not these documents were immediately visible, attached to the interface through which they authorized these terms, or accessed. All EULAs prohibited or heavily restrained players from copying, corrupting, modifying, redistributing, or otherwise risking the integrity of the software and any related services.

5.2.1Data monitoring

The EULAs for all platforms and 43 games contained terms for data monitoring or an *assumption* of data monitoring within conditions describing the management of that data. Data collection terms did not include specifics about what sort of data were collected, beyond generalities about account and/or gameplay activity. The overwhelming majority of the examples of game software with data monitoring terms were coded as published by AAA publishers, with only two being published by indie-coded publishers. The earliest game software EULA with conditions for data monitoring was released in 2008, with 60% of those containing these conditions being released after 2010. These data suggest this sort of surveillance is still relatively new in digital game software. Based on our data, we would expect a much larger portion of a sample of contemporary games published by AAA publishers to contain these terms.

Surprisingly to us, only 16 of these 43 games supported online multiplayer modes. Early on, we expected online play to be a strong predictor of data monitoring. However, less than half those with data monitoring terms supported it, meaning the data collected *must* be about more than player interactions, moderation, or matchmaking services.

All EULAs and ToS clearly defined the consequences for players who failed to uphold the rules they contained. The most common outcome we observed was loss of player access to the game software or platform. Table 2 summarizes occurrences of these highlighted terms and conditions in our sample.

Table 2: occurrences of highlighted terms and conditions

Sample	% of EULAs that defined publishers as sole owners of software installed on player devices	% of EULAs that prohibited or severely restrained players from copying, modifying, etc. software	% of EULAs that contained terms for data monitoring	% of EULAs that demanded complete conformity to terms therein as a condition of continued access.
Seven Platforms	100%	100%	100%	100%
200 Games	100%	100%	21.5%	100%

5.3 Authentication: identity verification

All platforms required authentication to access. Any level of access to all PC platforms and the PlayStation required identify verification. The Xbox and Switch allowed *some* level of access to basic platform navigation without identity verification. However, verification became required

when attempting to access game software, system features, or other applications. Both the PlayStation and Xbox did offer a "guest" account access option. However, guests gain only limited access to platform services, game software, and are prohibited from saving gameplay progress. The Switch permits the creation of a local account that is comparable to a permanent guest account, with slightly more access. Although this local account did allow some game software to be accessed and gameplay to be saved, accessing all games and platform functions required the account to be linked to a Nintendo account, with functions and conditions that resemble the accounts of other platforms.

Because accessing all game software required platform access first, all games inherited the authentication imposed by platforms, resulting in 100% requiring authentication to access. The nineteen examples of game software that required assent to an additional publisher account-specific EULA also required additional identity verification. After initially encountering these publisher accounts, the same account/identifier could be used for subsequent game software we encountered by the same publisher. Our sample is insufficient to identify when companies like these began this practice. However, we did observe game software released earlier by these same publishers that was not equipped to require this additional identity verification or account linking, suggesting it is a relatively recent practice and would expect this number to be higher in a sample of contemporary game software. We did not encounter any singular game-specific identity verification in our sample, though we are aware these exist.

We encountered only two varieties of authentication interfaces. The first was standard username and password, two-textbox, entry interfaces (analogous to account creation interface in Figure 2). This format requires players to provide a username or account name and password as a two-part identifier in return for access. The second broad category of authentication interfaces we observed included two versions of simplified account verification where username and/or passwords were not required to be entered. The first version was a form of the two-textbox screen with one or both fields "remembered" by the system from a point of earlier access, requiring us only to press the "login" button. On console platforms, we observed an even more simplified category of authentication, only requiring the selection of a saved and previously verified account with an option to select a "default" account that auto-authenticates upon system start up.

All platforms and the nineteen games with additional authentication permitted some form of simplified identity verification. Although these authentication processes are streamlined or automated for return visits, we need to highlight they still enforce authentication as a condition of accessing or beginning every instance of gameplay. Table 3 summarizes the occurrences of the different conditions of authentication we observed.

Table 3: occurrences of different authentication conditions

Sample	% of sample that required at least one instance of authentication to access	% of sample that required two instances of authentication to access	% of sample that could be accessed using *only* streamlined or automated authentication, after initial use
Seven Platforms	100%	0%	100%
200 Games	100%	9.5%	100%

5.4 Authorization *and* Authentication: Names, identity, and autonomy

None of the EULAs or ToS we read informed players about name change policies or publisher responsibilities regarding account *names* or identifiers being established. These documents dictated what companies could do with the accounts themselves (e.g. share them attached to data) and warned what players could *not* do with them (e.g., share them with friends or sell access to them). However, no EULA contained policies that described whether or how players may change their account name.

After searching their websites, we did discover that all seven companies that maintain the platforms we observed did have name change policies; these policies just were not immediately available in documentation provided during account creation. At time of writing, Steam and Nintendo did not permit account name changes (though both did allow *displayed* names to be changed). Battle.Net and Xbox permitted one free change, with a small fee for subsequent changes. Origin and Uplay permitted an indefinite number of changes but limited how often changes may occur. PlayStation permitted changes at any point.

6 DISCUSSION

Access controls are intentionally placed technical and procedural barriers at the borders of gameplay, common application use, and Burk's "legal regimes" (2010). These systems explicitly control whether and how we *can* enter those regimes and access any core media content and experience within. How these interfaces regulate access to core media highlights the inherent, recursive, mediation of contemporary digital, computational, media in a way that overlaps with but is distinct from a platform studies perspective (Montfort and Bogost 2009; Boellstorff and Soderman 2017). That is, access controls are often part of platforms but they are not exclusively so, and our focus is on relationships with media *through* medium, while platform studies is often explicitly focused on medium.

In our findings, authorization and authentication interfaces dictated the terms of participating in the legal domains of software publishers within which digital media reside, and enforced a loss of autonomy in return for that participation. Authorization interfaces that acquire or record our assent enable, confirm, and enforce the rules that determine the relationships between users, media, publishers, and platforms. Authentication interfaces that verify our identities consistently validate access while indexing user activity. That is, Index in two senses: in the semiotic sense of *pointing* at users indicating their presence and who they are alleged to be, and in the sense that user data is *arranged* to better organize and validate access control and surveillance databases.

Our findings may at times feel obvious, or modest, in their mundane description of potentially familiar details of authorization and authentication. However, they help to empirically ground under-examined understandings that—while common—have largely been assumptions about digital media. Our data permit us to make more clearly evidenced claims about these systems that both reinforce *and* complicate common, assumed perspectives that go beyond technical

understandings. Though our data draws on older game software at times, this is the first data set of this type to be gathered and analyzed in this way, though hopefully not the last.

Because access controls sit—intentionally and pragmatically—*between* users and the digital games, media, or platforms they wish to access, they serve as a fulcrum for companies to apply leverage. Our findings can encourage users to critically reflect on some of the systems underlying their everyday media use. Our data can help designers and developers reflect on the scope of conditions they impose on users through the ecology of interfaces that *surround* their core product, and in some senses *define* that product. Our analysis can help researchers better examine social concerns and relationships these interfaces manifest and maintain between users, digital media, platforms, and the companies that produce them.

Access control interfaces and processes are reasonable adaptations to digitization and computerization and many of the norms we observed are aligned with broader software development and implementation. However, we focus on how authorization and authentication demanding users provide personal information, submit to legal regimes, and enroll themselves in too often vaguely defined networks of surveillance and algorithmic influence in return for access influences or alters core media experiences. Because practices like these are so common, our claims—and critiques—provide insight beyond the context of only games. And, to echo Seaver (2017) and Seberger et al. (2022), our analysis suggests studying these systems and transactions beyond the moment of interaction within a broader socio-technical ecology.

Access controls make possible a variety of economic, legal, and social outcomes beyond gameplay or other digital media contexts through the software and platforms with which we must interact to consume them. Authorization and authentication interfaces enable familiar consequences such as loss of access or prosecution for copyright infringement or intellectual property theft, but are also what make it possible to collect, sell, or unlawfully disclose personally identifiable information to third parties. For users whose interests or identities have shifted, unchangeable or difficult to change identifiers provide a regular—potentially traumatic—reminder of a past they prefer to leave behind.

Access control interfaces become a threshold that dictates important facets of the experience of digital games and other digital applications and platforms via the access, policies, and processes they enable and enforce. Again, the immediate technical dimensions of authorization and authentication interfaces and services are well trodden. However, what makes them especially powerful is how their ostensibly mundane functions and the transactions they mediate enroll users in relationships, terms, outcomes, and networks of surveillance that extend so far beyond everyday gameplay, media consumption, and use.

6.1 Controlling Access to Gameplay

The forms of assent described above in relation to traditional or theoretical games or gameplay dictate what players may do *in* games and/or define gameplay. The mechanical, formal assent to EULAs and ToS like those we observed dictate which non-gameplay behaviors would be acceptable during/alongside gameplay or what players may do *to* games and game software. In their most

closely aligned moments, EULAs or ToS ask players to agree to a particular *tone* of gameplay, where previously observed modes of assent ask them to agree to rules that define the nature of gameplay itself. More centrally, however, our observed processes, interfaces, and the terms they resolve determine what sorts of authority publishers may exert on players independent of gameplay in ways earlier games as artifacts were incapable of supporting, and play scholars were ill-equipped to observe. That is, rather than assenting to abide by certain gameplay actions—such as how chess pieces move or how to score in tennis—assenting in interfaces like those we observed determines how we may interact with the artifactual game itself. Analogically, this assent is more about where a chessboard or stadium is physically permitted to exist and who is permitted to experience any gameplay they host. Players never had the authority to move, copy, or distribute stadiums, but in this analogy, we must now affirm they will not do so every time they wish to play there. How these interfaces serve as features of ordinary software infrastructure cannot be separated from how they influence digital games and gameplay in ways that games and digital media scholars have yet to fully engage with.

In our observations, authorization was required a minimum of twice prior to being permitted to install any game software on our machine. Burk describes the phenomenon of easily clicked-past conditions like those we observed as "clickwrap" licensing, an offshoot of "shrinkwrap" licensing where the terms to which we assent take effect through the simple act of removing physical packaging (generally without active access to—or awareness of—said terms) (2010). In both cases, it is assent to and the authorization of company claims that is the priority.

Authentication interfaces that consistently verify identities are another relatively new threshold attached to games and gameplay that scholars have yet to properly reckon with in *relation* to the games and media we consume. Pre-digital games only relied on rigid identity verification in formal competitive or professional contexts. As our finding of requiring a minimum of one layer of authentication to access *all* games suggests, even the most casual of everyday digital gameplay interactions are likely to require players authenticate a verified identifier.

Based on our read of observed EULAs, ToS, and observed interfaces and attached systems, publishers and platforms verify identities to serve a variety of priorities. Authentication offers minimal protection for user information such as saved payment information. However, the primary reasons we could discern for the implementation of authentication, based on available terms observed outcomes of authentication across platforms, were primarily serving publisher priorities, not user needs. Authentication can only enforce the conditions established by EULAs and ToS, revoke access or prosecute, or monitor user activity if users are *legible* enough to differentiate between them. This legibility comes only from reliable identify verification across multiple instances of access. Authentication is rarely explicitly addressed in EULAs or ToS but without it the most punitive or invasive terms in these documents would be impotent.

Without authentication, even basic conditions would be challenging to enforce. For example, it is now difficult for players to share games with each other. Where players can readily share traditional, and even theoretical games, without notable consequence, sharing *digital* games and is difficult without uncommon technical skill and is explicitly prohibited by all EULAs we observed.

Identity verification is an essential aspect of contemporary gaming that dictates access to gameplay and reconfigures important relationships players may have with contemporary games, publishers, and platforms. However, this description applies because of their digital, computational nature, not their gameness. That games have only adopted pervasive formalized authentication as they became digital and networked highlights how these functions are more essentially facets of broader digital applications and platforms than of games or gameplay. We must be careful not to neglect similar processes across digital media, platforms, and contexts that represent essential aspects—and consequences—of the underlying systems and priorities that shape broader digital, media, and social experiences.

Identifying the distinct layers of procedural and mechanical assent bounding gameplay, game software, and game platforms as we have helps to compartmentalize and better understand other facets of digital games and media. Acknowledging how periludic authentication directs how players *must* interact with game software, platforms, and publishers to retain access to gameplay highlights how contemporary digital gaming activities comprise so much more than familiar conceptions of games or gameplay. Understanding digital games requires recognizing these layers of systems that mediate our access to, and experience of, gameplay. Acknowledging how similar processes shape our experience with other forms of recently or natively digital media highlights basic, essential, and yet often overlooked, aspects of how we are *permitted* to interact with contemporary digital media *through* software and platform mediation.

Figure 3 visualizes our findings to further illustrate how accessing digital gameplay isn't simply a matter of voluntarily choosing to play or not as some historical models of play might suggest is the norm. Our findings highlight how accessing *digital* gameplay requires players submit to multiple layers of permissions, verification, and validation unrelated to the rules of play, and unaccounted for by game scholars. Our observations about these processes and interfaces suggest that understanding how we actually interact with digital games and broader digital media demands broader recognition of the socio-technical ecology within which they reside, not just core content.

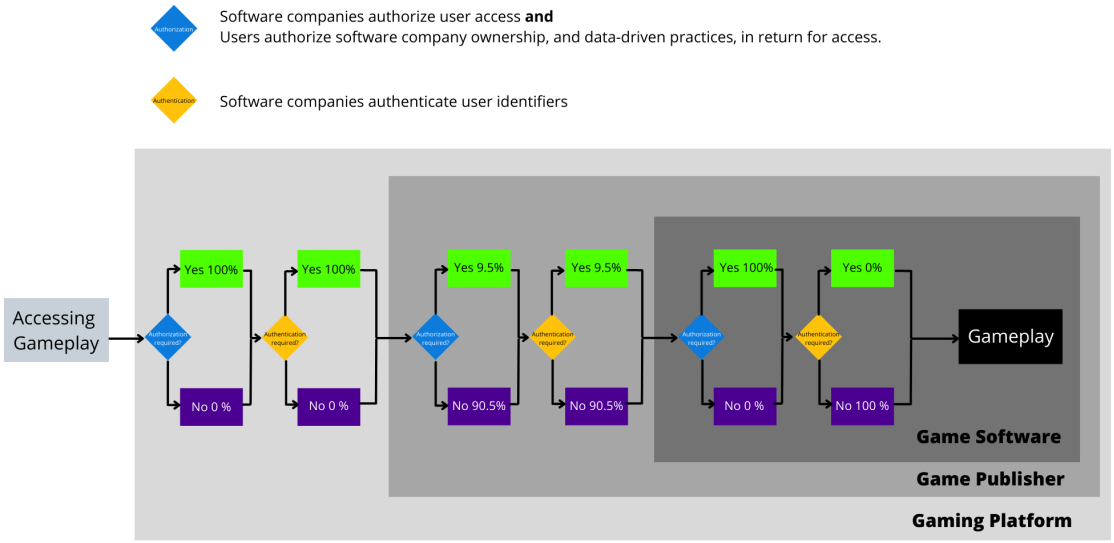

Figure 3: Visualization of our findings that illustrates the procession of access control mechanisms at different stages of software interaction necessary only to access gameplay

Our findings identify a need to better address these functions *around* digital games. These interfaces and systems reconfigure familiar media-forms and our conceptual models of them and game scholars need to broaden their field of observation. These systems may not be part of *the* game, play, or gameplay, but they are essential to accessing them. The HCI community needs to consider more than the technical efficacy of these systems or the usability that makes obtaining assent or verifying identities more efficient. The primary intent and immediate outcomes of these systems may represent common, reasonable best-practices but they have unintended and unattended outcomes *in* games or that influence users/player experience that demand attention. As following sections will discuss in greater detail, it is important to recognize when the transactions these interfaces manage *attach* potentially opaque and/or inequitable practices to media through interfaces that are unethically optimized for inattention.

6.2 Surveillance and Data

It bears repeating that submitting to data monitoring was an essential condition for accessing *all* games in our sample, or any game that would be played on any of the platforms we observed. Given the platforms themselves monitor, there is no option to choose between games that do or do not surveil and no choice to opt in or out save opting out of using seven of the largest gaming platforms and so a large majority of digital games. That is, our findings suggest the only available choice players have regarding surveillance in digital games is to submit to it or to opt out of the medium itself.

There are likely some readers that might minimize concerns about surveillance as a condition of accessing digital games based on their oft-perceived status as leisure items. However, games are a powerful socio-technical phenomena that are as much a part of many contemporary cultures—and economies—as books, film, music, or social media. Moreover, as we argue just above, the presence of these systems is less a feature of games than of their digitization. These systems exist in much the same form across digital contexts with an *assumed* ubiquity our findings essentially confirm with games, based even on the sample of platforms alone. Games are one—very common—lens through which we might examine the influence of these systems and highlight their expansive reach. Although precise manifestations may vary, our analysis of the mechanisms through which players/users are enrolled in surveillance applies beyond digital games. However unlike games, because of how integrated broader digital media and communication platforms are throughout personal, professional, and cultural contexts, choosing not to participate in surveillance by opting out of digital media and platforms would be comparable to opting out of society.

Long-term surveillance *can* be used to benefit players or users. Data recorded on player activity are used to help balance gameplay mechanics, improve matchmaking services that ensure players compete with similarly skilled opponents, or update and repair underlying game code. When made available to players, activity data can be used to reflect on past gameplay to improve performance (Egliston 2020). Game software publishers may use records of chat logs to arbitrate disputes between players or as evidence for punitive actions against malicious players—an outcome outlined in several EULAs we observed, even if the method was not explicitly identified.

Although supporting restrictive and punitive actions is valuable on one hand, the key reason surveillance appears to be attached to gaming platforms—and by extension all games they host—appears to be increasingly common data-driven and algorithmic processes. Just as the attachment of access controls to games is more a characteristic of their digitalization, so too are contemporary gaming platforms. What defines many of these platforms, especially on PC as "game platforms," is the nature of the software they peddle. In why likely appears to be a familiar practice, they use the data they collect on player activity to enhance that peddling much more visibly than any other use of these data. For example, we observed Steam making and updating recommendations for games we might purchase, based on accessing the wide array of games in our sample (e.g., Figure 4).

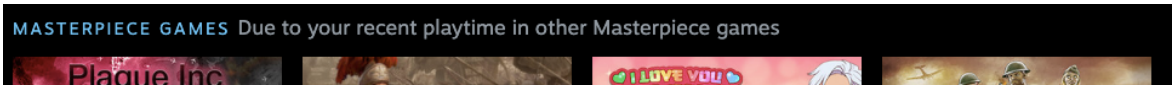

Figure 4: Example of Steam recommendation based on accessing sampled games, explicitly implicating their surveillance of activity. It was unclear to us precisely what qualified games as "masterpiece games" based on presentation.

These familiar practices present more evidence that while there are functions, findings, and implications specific to the relationships access controls have with digital games, our analysis likely applies more broadly. Broader digital platform interactions and activities are subject to similar practices as a basis for actions taken on behalf of—or against—users. In many cases readers are likely already familiar with, such as with social media feeds, online retail settings, or the music

streaming platforms described by Seaver (2019), companies use these data to algorithmically recommend new content or products.

As we have mentioned before, one benefit of studying digital games compared to some other digital contexts, is that they are heavily studied and theorized *apart* from their digitally embedded expressions. The opportunity to pick apart components of gameness and digitalness can lend perspectives that might otherwise be more challenging to pick apart. For game scholars, there is a real need to add pervasive surveillance to the insights from the previous section, and to broaden their scope still further to question the differences between gameplay and gameplay under the ever-watchful, algorithmic eye. For HCI scholars, there are broader topics to consider about the relationships authentication, in particular, has with broader surveillance and algorithmic practices.

To reiterate, if authorization interfaces are what secure our—often naive—assent to data-driven activities, authentication interfaces are where our surveillance begins. In our findings, surveillance practices, precisely what data is collected and when, and any associated positive and negative outcomes were rarely if ever fully transparent and—to points already made—how much choice or autonomy users ever had over what was collected about them was questionable. Further, the irony of authentication is that while it ostensibly limits access to player/user data, it's ability to make that data *legible* is also what invites data leaks, breaches, or attacks (Haggerty et al. 2015). Without authentication, data *might* be freely accessible but unlinked, highly illegible, and without value. With authentication, data *becomes* valuable—to companies that collect it and entities that leak or thieve it—because it becomes legible, organizable, and *linkable* to individuals. That is, even if personal or private information is often protected by authentication, it is often precisely because of authentication that our privacy is lost (Vertesi 2014).

There is dire needs for a greater discussion of the means in which we *enter* surveillance and Seaver's algorithmic "traps" (2019). Whether we are discussing games or broader digital media, how the data that surveillance produces is procured or used and how companies implement and enroll users in that surveillance matters (Vertesi & Dourish 2011). We cannot *only* rely on technically sound, highly efficient/usable interfaces that do not demand our attention while enabling surveillance and potentially endangering privacy. How clearly and transparently users are made aware of these practices, and their stakes, matters. The ethics of design decisions companies make despite Good et al., Böhme and Köpsell, and Obar & Oeldorf's findings incentivizing optimizing inattention must examined. Whether or not users truly have a choice to be surveilled or not—or to be enrolled in these algorithmically tailored experiences—matters.

6.3 Names

It was not clear to us why account name change policies were omitted prior to account creation, given how much attention EULAs pay to the state of the accounts themselves. EULAs were the *only* policies the platforms we observed presented prior to account creation—if only indirectly through links in some cases. As described above, these documents identify a range of things companies may do with user accounts and a range of things users may *not* do with them. For

example, EULAs establish the right of companies to share—or sell—information on user accounts and prevent users from undermining profits by freely sharing account access.

Like authorization and the authentication interfaces where account names must regularly be input, accounts themselves are a feature of digitalization more than games, which permits insights into broader contexts. The *absence* of policies informing users how account names are managed is especially telling, given users become subject to these policies at the same transactional points of initial authorization and account creation.

No platform observed enforced the use of legal names for accounts and all permitted the change of—at a minimum—*displayed* names. We must assume that the platforms that allow account name changes either index users with some form of unique, invisible to the user, identifier *linked* to their account name, or their systems are equipped to re-link data to new identifiers as they are changed (probably the former, though this is proprietary information we could not access). Others have examined how insensitive naming policies and a lack of independent identifiers can impact marginalized communities in broader digital contexts such as social media (Haimson & Hoffman 2016; Haimson et al. 2016), or even academic publishing (Tanenbaum 2020; Tanenbaum et al., 2021). We, however, draw attention to the mechanisms and procedures where users initially submit to these policies (knowingly or not), and where they are potentially consistently reminded of their rigidity.

Account and account name policies help define basic digital housekeeping, index users, and reasonably (for companies) protect against lost revenue. However, in our observations, users are rarely provided with these policies when creating accounts and their transparency is not guaranteed. Whether users *can* change their names is not guaranteed, potentially requiring users who wish to leave an old name behind to start completely new accounts. These users must then abandon any assets—and potentially reconstruct meaningful social networks—tied to their old accounts.

Although our own priorities are primarily aligned with users, this situation is less than ideal for companies as well, as it interrupts and devalues collected data. While imperfect, the gaming platform policies we observed that did not enforce "real" or rigid unchangeable names suggest means for other domains to improve their access control policies and procedures to provide users a modicum of autonomy over their experience while improving data continuity.

6.4 Ownership

The ubiquity of ownership claims in our findings beg for deeper analysis of the mechanical, transactional points where the topics of these debates are confirmed and made to matter. However, an array of scholars and journalists have already examined this shift to licensing over ownership in a broad spectrum of applications and technologies and speculated on the consequences of this shift (Boyle 2017; Frederiksen 2020; Gruning 2017; Pegoraro 2015; Sinclair 2022; Squires 2021; Szpytek 2021; Walker 2012). There are also related scholarly themes on modding in games (Kretzschmar and Stanfill 2019; Postigo 2008; Taylor 2009; Wallace 2014), or a broader "right to repair" or "tinker (Bergen 2021; Gault 2020; Grinvald & Tur-Sinai 2019; Svensson et al., 2018; Waldman & Mulvany 2020). Although we *do* add some basic empirical grounding to this topic that

is not always present in this work, we do not have broader analysis to add. Instead, on this topic, we offer only a brief contextually specific insight.

Claims of ownership and conditional player licensing are intended to reduce theft of actual and intellectual property. Although a reasonable goal, one underexamined consequence of this shift in ownership models related to games and other media is how they make lending or borrowing more difficult, as briefly mentioned above. Limiting the ability to share erases a meaningful way players historically could have first experienced new games and new consumers might explore their tastes and develop fluency in the medium. These limitations reduce accessibility to the medium along clearcut economic lines.

7 IMPLICATIONS FOR DESIGN

Throughout this paper, we have described how streamlining or automating submission to access controls systems serves to place users in unfavorable positions with unethical efficiency. Instead, it may be time to reconsider the strategies designers rely on to authorize standard terms of use and access, and to better acknowledge the full reach of authentication. We cannot offer specific suggestions for *every* issue we have identified and recognize the logistical constraints of replacing or completely re-imagining these systems. However, we offer two key implications that should be relatively feasible and address *some* of the issues we describe related to user autonomy and the equity of ongoing relationships: more transparent and complete data preferences and using identifiers that are independent of actual and displayed names.

The first minor change we suggest with major implications is simply giving users *any* real control over how their data is used, given how we identified they currently have little or no control over their participation in surveillance. This change could be technically deployed any number of ways. However, *any* user control over data preferences would be an improvement over a current lack. If data monitoring is too central to the functions of a product or a company's revenue stream to make blanket participation optional, we suggest making those practices minimally transparent. Even if they are hardly read, adding details about what sorts of data are collected and for what purposes to data-monitoring or processing sections of EULAs or even making these details available online would also be a constructive step. These changes are in line with increasingly common practices around cookie preferences for websites, as more companies apply the EU's GDPR requirements to websites regardless of regionality. Cookies are a piece of the data surveillance puzzle online and allowing users to control which are collected *and* requiring users to opt *in* to non-essential collection is a good model. However, no game platform nor—to our knowledge—any major app or social media platform applies a similar model regarding user data. Granting users even a small level of autonomy over how much they are surveilled feels like an obvious, minimum, but still too uncommon step toward creating a more equitable data environment for digital games or beyond.

The gaming platforms we observed that decouple their account names from preferred, assigned, or legal everyday names provide a constructive example for broader platforms to permit more sensitive, flexible, and reliable identifiers. Indexing people independent of their assigned or legal designations permits services—and collected data—to remain uninterrupted while allowing users

to better align their account information to lived or preferred identities. Permitting changeable account titles or assigning users a number or hex string of some kind permits the names users otherwise become shackled to, to be more fluid without disrupting use. Plenty of broader platforms or services already distinguish account names and/or identifiers from display names, so this seems to be a logical next step. Even if broader digital platforms followed the model we observed of charging for these changes, many users who are haunted by previous names might consider these change fees a small price to—for example—escape potentially traumatic designations.

Although there are technical challenges associated with permitting users to personalize their surveillance or overhauling identifier databases, these suggestions do not ask digitally focused industries to dramatically alter their practices, and both suggestions are already currently used by *some* companies. The relative modesty of these interventions highlights the disproportionate amount of neglect shown to the personal and ethical influence these systems may have. If granting users even these seemingly trivial levels of autonomy cannot be accommodated by these industries, it then highlights how much their priorities are not users, and their practices cannot be user-centered.

8 LIMITATIONS AND OPPORTUNITIES

This study has three immediate limitations related to the selection of game software and breadth of our data. However, none of these limitations discount the value of the data we *do* have, and each suggests an opportunity for future study building on the insights presented in this paper.

The first and most obvious limitation in of our analysis is the date range on the sample. At time of writing, the most recent game from our sample is seven years old and much can have changed in the time since its release. Our own findings suggest this is likely. However, our observations and findings are less about the current *state* of the digital game medium, and more about the *nature*, and the nature of related media. A more recent sample would undeniably enhance our analysis, but we are confident it would not change the fundamental contribution, or demand for these systems to receive greater attention.

Our observations of each platform allow us to strongly infer that many of the themes we observed with our sample of games on Steam would persist across those platforms as well. However, one hole in our analysis is mobile gaming which likely has unique expressions of some of the themes we discuss. Mobile devices offer a perfect opportunity for complementary or future research that would necessitate a consideration of the *linkability* of location data.

Our exclusion of games without playable characters precludes some comparisons. However, we did have a wide variety of genres and game types in our sample and as our findings suggest, publisher and date of release are likely to be bigger indicators of varying terms than gameplay elements—and to a lesser extent perhaps, the presence of online multiplayer game modes.

9 CONCLUSION

Consistent, pervasive access controls are a mundane component of our everyday digital game software, media, tools, applications, platforms, and lives, yet they highlight a shift in how we

participate in any activities related to these contexts. The authorization and authentication procedures tied to these technologies means we are never really accessing digital content or contexts alone, or without consistently verified identities and a need for permission—often even when in offline modes. This shift is not unique to games and creates ongoing—often obscured—relationships with the digital media, platforms, and technology we interact as well as those who produce them with that harkens back to the quote with which we began this article.

There may not be inherent problems with the presence or use of access control mechanisms. These systems represent practical responses to needs associated with the production, maintenance, and use of digital technologies. However, they also represent a fundamental mediation of everyday experiences the influence of which we have yet to properly reckon with due to them being a frighteningly recent component of consuming media in a grander scale despite their ubiquity.

In Star's explanation of why ethnographies of infrastructure are so important, she emphasized the importance of studying the "boring" infrastructural components of information systems (1999). Access control interfaces are one of those essential and otherwise boring mechanisms that subtends processes more familiar to games, media, and researchers. Characterizing these systems as boring also recalls Draz's analysis, and how it is especially those who benefit from the status quo who will find them such. Neglecting the broader, qualitative, personal, and institutional aspects of how these interfaces and processes shape digital games and media more broadly means missing equally essential aspects of the authority, identity, privacy and surveillance, autonomy, and exclusion they establish or enforce.

Our analysis of access control interfaces and the conditions they mediate provides greater insight into how these concepts and consequences are enacted within everyday technology use beyond their immediate technical functions or immediate player/user interactions. Our data ground common assumptions about these technologies with empirical weight and our analysis describes how these interfaces could center future studies that invite input from users about more than their usability. Our analysis should support new studies with mobile technologies—which increase the depth of surveillance by linking additional parameters to user data, such as location. Further, scholars should examine how different outcomes may respond specifically to the socio-demographic position of users, or in response to national or legislative policies such as the EU's GDPR, or when designed counter to hegemonic norms.

Access control interfaces are common, familiar facets of digital games and broader digital technologies that reinforce the authority of publishers, support powerful software functions, and limit the autonomy of users. Despite deep knowledge of their technical parameters and widely held notions of their reach across digital contexts, we identify a lack of analysis of their broader implications and recommend researchers move to fill this gap. We highlight moments of opacity and optimized neglect and suggest how to *begin* to address these concerns. Investigating the personal, infrastructural, and societal impacts of these seemingly mundane features can profoundly expand our understanding of their place in our lives and their responsible design.

ACKNOWLEDGEMENTS

This work was initially supported in part by an endowment by the Kleist family. We would also like to acknowledge The Grand Challenges Initiative at Chapman University who made completing this project possible with their support.

REFERENCES

Alsoubai, A., Anaraky, R.G., Li, Y., Page, X., Knijnenburg, B., & Wisniewski, P.J. (2022). Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proceedings of CHI Conference on Human Factors in Computing Systems*, 1-18.

Antón, A.I., Earp, J.B., He, Q., Stufflebeam, W., Bolchini, D. and Jensen, C. (2004). Financial privacy policies and the need for standardization. In *IEEE Security & privacy, 2(2), 36-45.*

Assiotis, M. & Tzanov, V. (2006). October. A distributed architecture for MMORPG. In *Proceedings of 5th ACM SIGCOMM workshop on Network and system support for games,* 4-es.

Avedon, E. & Sutton-Smith, B., eds. (1971). *The Study of Games.* John Wiley & Sons.

Backes M, Berrang P, Goga O, Gummandi KP, & Manoharan P (2016) On Profile Linkability Despite Anonymity in Social Media Systems. In *Proceedings of the 2016 ACM Workshop on Privacy in the Electronic Society:* 22-35

Bailey, D. 2018. With $4.3 Billion in Sales, (2017). Was Steam's Biggest Year yet. *PCGames*. Retreived from PCGamesN. https://www.pcgamesn.com/steam-revenue-2017 (September 9, 2021)

Baltzar, P., Turunen, M. and Hassan, L. (2022). Popular Accessibility Settings in Digital Games: What accessibility settings do players with disabilities use and need?. In *Proceedings of the 25th International Academic Mindtrek Conference, 359-363.*

Bergen, M. (2021). Microsoft and Apple Wage War on Gadget Right-to-Repair Laws. In *Bloomberg Technology + Green*. Retreived from https://www.bloomberg.com/news/articles/2021-05-20/microsoft-and-apple-wage-war-on-gadget-right-to-repair-laws (September 9, 2021)

Boella, B., Hulstijn, J., & van der Torre, L. (2005). Argument games for interactive access control. In *the proceedings of the The 2005 IEEE/WIC/ACM International Conference on Web Intelligence (WI'05)*. IEEE.

Boellstorff, T. & Soderman, B. (2017). Transplatform: Culture, Context, and the Intellivision/Atari VCS Rivalry. In *Games and Culture 14(6), 680-703.*

Bonneau, J., Herley, C., Van Oorschot, P.C., & Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *2012 IEEE Symposium on Security and Privacy,* 553-567

Böhme, R. & Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. In *Proceedings of the SIGCHI conference on human factors in computing systems*, 2403-2406.

Boyle, E. (2017). Why your digital games collection isn't yours to own. Retreived from *Techradar,* May, 2022. https://www.techradar.com/news/the-double-edge-of-digital-games-and-changing-ownership.

Buolamwini, J. & Gebru, T. (2018). January. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*, 77-91.

Burk, D.L. (2010). Authorization and governance in virtual worlds. In *First Monday*, 2012-33.

Caplan, R & boyd, d. (2016). Who Controls the Public Sphere in an Era of Algorithms? In *Mediation, Automation*, *Power*, 1–19.

Cho, D. & Kwon, K.H. (2015). The impacts of identity verification and disclosure of social cues on flaming in online user comments. In *Computers in Human Behavior 51 (2015)*, 363-372.

Clarke, R. (1988). Information Technology and Dataveillance. In *Commun. ACM 31(5),* 498–512.

Clauß, S. (2006). A Framework for Quantificati.on of Linkability within a Privacy-Enhancing Identity Management System. In *International Conference on Emerging Trends in Information and Communication Security:* 191-205

Cole, F.L. (1988). Content Analysis: Process and Application. In *Clininical Nurse Specialist, 2(1):* 53-57

Crenshaw, N. & Nardi, B. (2014). What's in a name? Naming practices in online video games. In *Proceedings of the first ACM SIGCHI annual symposium on Computer-human interaction in play*, 67-76).

Creswell, J.W. & Creswell, D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications Ltd.

Cvrček, D., Matyas, V., & Kumpošt, M. (2005). A Privacy Classification Model Based on Linkability Valuation. In *Security and Embedded Systems:* 91-98

Dahlgren, P. (2005). The Internet, public spheres, and political communication: Dispersion and deliberation. In *Political communication, 22(2),* 147-162.

Dotan, Y. (2010). Techniques for Authenticating Users of Massive Multiplayer Online Role Playing Games Using Adaptive Authentication. *U.S. Patent 8,370,389, issued February 5, 2013*.

Downe-Wamboldt, B. (1992). Content Analysis: Method, Applications, and Issues. In *Health Care for Women International 13(3),* 313-321

Drazewski, K., Galassi, A., Jablonowska, A., Lagioia, F., Lippi, M., Micklitz, H.W., Sartor, G., Tagiuir, G., & Torroni, P. (2021). A Corpus for Multilingual Analysis of Online Terms of Service. In *Association for Computation Linguistics*

Draz, M. (2018). Burning it in? Nietzsche, Gender, and Externalized Memory. In *Feminist Philosophy Quarterly*, 4(2).

Egliston, B. (2020). Quantified Play: Self-Tracking in Videogames. In *Games and Culture, 15(6),* 707-729.

Entertainment Software Association. (2019). U.S. Video Game Sales Reach Record-Breaking $43.4 Billion in 2018. *Entertainment Software Association*. Retrieved from https://www.theesa.compress-releases/u-s-video-game-sales-reach-record-breaking-43-4-billion-in-2018/ (September 9, 2021).

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*, 1-14.

Finkelstein, S. (2016). Algorithms are making us small-minded. *BBC.* Retreived from BBC.com, May 2022: https://www.bbc.com/worklife/article/20161212-algorithms-are-making-us-small-minded

Florencio, D. & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web (WWW '07)*.

Føllesdal, D. (2001). Hermeneutics. In *The International Journal of Psychoanalysis 82(2),* 375–79.

Foucault M (2012[1977]). *Discipline and Punish: The Birth of the Prison.* Vintage

Frederiksen, E. (2020). Amazon Says You Don't Actually Own Purchased Prime Videos. *GameSpot.* Retrieved from GameSpot, May 2022. https://www.gamespot.com/articles/amazon-says-you-dont-actually-own-purchased-prime-videos/1100-6483890/

Frik, A., Kim, J., Sanchez, J.R. & Ma, J. (2022). Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *proceedings of CHI Conference on Human Factors in Computing Systems*, 1-24.

Gadamer, H.G. (2006). Classical and philosophical hermeneutics. In *Theory, culture & society 23, no. 1 (2006)*, 29-56.

Galloway AR (2006). *Gaming: Essays on Algorithmic Culture.* University of Minnesota Press

Galloway AR (2012). *The Interface Effect.* Polity.

Garber, L. (2013). Game accessibility: enabling everyone to play. In *Computer, 46(06), 14-18*.

Gardner, D.L. & Tanenbaum, T. (2021). At the Edge: Periludic Elements in Game Studies. In *Game Studies 21(4)*

Gault, M. (2020). Newly Passed Right-to-Repair Law Will Fundamentally Change Tesla Repair. *Vice.* Retreived from Vice, May 2022. https://www.vice.com/en/article/93wy8v/newly-passed-right-to-repair-law-will-fundamentally-change-tesla-repair

GauthierDickey, C., Zappala, D., Lo, V., & Marr, J. (2004). Low latency and cheat-proof event ordering for peer-to-peer games. In *Proceedings of the 14th international workshop on Network and operating systems support for digital audio and video,* 134-139.

Gomez, J., Pinnick, T. and Soltani, A. (2009). KnowPrivacy. *UC Berkeley School of Information Report 2009-03710 October 2009.*

Good, N.S., Grossklags, J., Mulligan, D.K., & Konstan, J.A. (2007). Noticing notice: a large-scale experiment on the timing of software license agreements. In *Proceedings of the SIGCHI conference on Human factors in computing systems,* 607-616.

Grace, T., Larson, I., & Salen, K. (2022). Policies of Misconduct: A Content Analysis of Codes of Conduct for Online Multiplayer Games. In *Proceedings of ACM Human-Computer Interactions in Play, 2022*.

Grant, J. M., Mottet, L. A., Tanis, J. J., & Min, D. (2011). Transgender Discrimination Survey. National Center for Transgender Equality and National Gay and Lesbian Task Force: Washington, DC, USA.

Gregg, M. (2015). Inside the Data Spectacle. In *Television & New Media 16(1),* 37–51.

Grinvald L.C., & Tur-Sinai, O. (2019). Intellectual property law and the right to repair. In *Fordham L. Rev. 88 (2019),* 63.

Gruning, J. (2017). Models for Ownership: Implications for Long-term Relationships to Objects." In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems,* 2607-2613.

GWI. (2021). Social media marketing trends in 2021. Retrieved from https://www.gwi.com/reports/social

Haggerty, J., Hughes-Roberts, T., & Hagarty, R. (2015). Hobson's Choice: Security and Privacy Permissions in Android Devices. In *International Conference on Human Aspects of Information Security, Privacy, and Trust:* 506-516

Haggerty, K.D. & Ericson, R.V. (2000). The Surveillant Assemblage. In *The British Journal of Sociology 51(4),* 605–22.

Haimson, O.L., & Hoffmann, A.L. (2016). Constructing and enforcing" authentic" identity online: Facebook, real names, and non-normative identities. In *First Monday.*

Haimson, O.L., Brubaker, J.R., Dombrowski, L., & Hayes, G.R. (2016). Digital footprints and changing networks during online identity transitions. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 2895-2907.

Hassan, L. and Baltzar, P. (2022). Social aspects in game accessibility research: a literature review. In *DiGRA'22–Proceedings of the 2022 DiGRA International Conference: Bringing Worlds Together.* DiGRA online library.

Hsieh, H.F. & Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis. In *Qualiative Health Research 15(9),* 1277-1288

Jagannath, K. & Salen, K. (2022). Beyond Just Rules: Server Rules for Shaping Positive Experiences in an Online Play community for Youth. In *Proceedings of ACM Human-Computer Interaction in Play 2022.*

James, S., Herman, J., Rankin, S., Keisling, M., Mottet, L., & Anafi, M. (2016). The report of the 2015 US transgender survey. *Center for Victim Research*.

Jin, H., Shen, H., Jain, M., Kumar, S., & Hong, J.I. (2021). Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost. In *ACM Transactions on Computer-Human Interaction (TOCHI) 28, no. 5 (2021),* 1-55.

Juul, J. (2011). *Half-real: Video games between real rules and fictional worlds*. MIT press.

Kay, M. & Terry, M. (2010). Textured agreements: re-envisioning electronic consent. In *Proceedings of the sixth symposium on usable privacy and security,* 1-13.

Kretzschmar, M. and Stanfill, M. (2019). Mods as lightning rods: A typology of video game mods, intellectual property, and social benefit/harm. In *Social & legal studies, 28(4), 517-536*.

Krug, S. (2000). *Don't Make Me Think! A Commone Sense Approach to Web Usability*. Pearson Education India

Kushin, M.J. & Kitchener, K. (2009). Getting political on social network sites: Exploring online political discourse on Facebook. In *First Monday.*

Lämmel, P., Tcholtchev, N., & Schieferdecker, I. (2017). Enhancing cloud based data platforms for smart cities with authentication and authorization features. In *Companion Proceedings of the10th International Conference on Utility and Cloud Computing,* 167-172.

Lampe, C., Zube, P., Lee, J., Park, C.H., & Johnston, E. (2014). Crowdsourcing civility: A natural experiment examining the effects of distributed moderation in online forums. In *Government Information Quarterly 31, no. 2 (2014)*, 317-326.

Li, T., Reiman, K., Agarwal, Y., Cranor, L. F., & Hong, J.I.. (2022). Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In *proceedings of CHI Conference on Human Factors in Computing Systems,* 1-24.

Lillard. M., Perf. (1995). Emmanuel "Cereal Killer" Goldstein. In *Hackers.* United Artists.

Lippi, M., Palka, P., Contissa, G., Lagioia, F., Micklitz, H.W., Sartor, G., & Torroni, P. (2019). CLAUDETTE: An Automated Detector of Potentially Unfair Clasuses in Online Terms of Service. In *Artificial Intelligence and Law 27(2),* 117-139

Liu, Z., Wang, X., Li, X., & Liu, J. (2022). Protecting Privacy on Mobile Apps: A Principal–Agent Perspective. In *ACM Transactions on Computer-Human Interaction (TOCHI) 29, no. 1 (2022),* 1-32.

Ma, M. Agarwal, R. (2007). Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities. In *Information systems research 18, no. 1 (2007),* 42-67.

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., Eghtebas, C. and Kunze, K. (2022). "Nah, it's just annoying!" A Deep Dive into User Perceptions of Two-Factor Authentication. In *ACM Transactions on Computer-Human Interaction, 29(5), 1-32*.

Miesenberger, K., Ossmann, R., Archambault, D., Searle, G. and Holzinger, A. (2008). More than just a game: accessibility in computer games. In *HCI and Usability for Education and Work: 4th Symposium of the Workgroup Human-Computer Interaction and Usability Engineering of the Austrian Computer Society, USAB 2008, Graz, Austria, November 20-21, 2008. Proceedings 4, 247-260.* Springer Berlin Heidelberg.

Montfort, N. & Bogost, I. (2009). *Racing the beam: The Atari Video Computer System.* MIT Press.

Nejad, N.M., Scerri, S., & Auer, S. (2017). Semantic similarity based clustering of license excerpts for improved end-user interpretation. In *Proceedings of the 13th International Conference on Semantic Systems,* 144-151.

Nejad, N.M., Scerri, S., Auer, S., & Sibarani, E.M. (2016). Eulaide: Interpretation of end-user license agreements using ontology-based information extraction. In *Proceedings of the 12th International Conference on Semantic Systems,* 73-80.

Nissenbaum, H., 2009. Privacy in context. In *Privacy in Context*. Stanford University Press.

Obar, J.A. and Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. In *Information, Communication & Society, 23(1), pp.128-147*.

Papacharissi, Z. (2004). Democracy online: Civility, politeness, and the democratic potential of online political discussion groups. In *New media & society 6, no. 2 (2004),* 259-283.

Pegoraro, R. (2015). Who Really Owns Your iPhone? It May Not Be You. *Yahoo!finance*. Retreived from Yahoo!finance, May 2022. https://finance.yahoo.com/news/who-really-owns-your-iphone-it-may-not-be-you-129321095449.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACJRAkAHlM_8Yl8CEOJ_kZhyD1pZtnuDrr_CTPs_8sBbWmaOJPa1cUCGGOG-ddlgK_7zm4HWq6nCszQUNweZhoXjFxPe5m3CdnOK7EFcJU5CbanYTU-Snni8NJ6p0F1gXcwsmvOzllt4Emzip-9aKUv-6DZzVV9xOwTY8znY-jTe

Pfitzmann, A. & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity—a proposal for terminology. In *Designing privacy enhancing technologies*, 1-9.

Porter, J.R. and Kientz, J.A. (2013). An empirical study of issues and barriers to mainstream video game accessibility. In *Proceedings of the 15th international ACM SIGACCESS conference on computers and accessibility, 1-8.*

Postigo, H. (2008). Video game appropriation through modifications: Attitudes concerning intellectual property among modders and fans. In *Convergence, 14(1), pp.59-74.*

Rainie, L. & Anderson, J. (2017). Code Dependent: Pros and Cons of the Algorithmic Age. *Pew Research Center*.

Raji, I.D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). February. Saving face: Investigating the ethical concerns of facial recognition auditing. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 145-151.

Roth, Y. (2015). "No overly suggestive photos of any kind": Content management and the policing of self in gay digital communities. In *Communication, Culture & Critique, 8(3), 414-432.*

Ruiz, C., Domingo, D., Micó, J.L., Díaz-Noci, J., Meso, K., Masip, P. (2011). Public sphere 2.0? The democratic qualities of citizen debates in online newspapers. *The International journal of press/politics 16, no. 4 (2011)*, 463-487.

Ruoti, S., Roberts, B., Seamons, K. (2015). Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th international conference on world wide web*, 916-926.

Sadagopan, S.M. (2019). Facebook loops and echo chambers: How algorithms amplify viewpoints. Retrieved online from *the Conversation,* May 2022. https://theconversation.com/feedback-loops-and-echo-chambers-how-algorithms-amplify-viewpoints-107935

Said, K. and Kane, S.K. (2013). Button blender: remixing input to improve video game accessibility. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems, 43-48.*

Saldaña, J. (2015) *The Coding Manual for Qualitative Researchers.* Sage Publications Ltd.

Salen-Tekinbas, K. & Zimmerman, E. 2003. *Rules of play: Game design fundamentals*. MIT press.

Scheuerman, M.K., Wade, K., Lustig, C., Brubaker, J.R. (2020). How We've Taught Algorithms to See Identity: Constructing Race and Gender in Image Databases for Facial Analysis. In *Proceedings of the ACM on Human-Computer Interaction, 4(CSCW1)*, 1-35.

Seaver, N., 2017. Algorithms as culture: Some tactics for the ethnography of algorithmic systems. In *Big data & society, 4(2), p.2053951717738104.*

Seaver, N. (2019). Captivating Algorithms: Recommender Systems as Traps. In *Journal of Material Culture, 24(4)*, 421-436.

Scott, J.C. (1998). *Seeing like a State*. Yale University Press.

Seberger, J.S., Shklovski, I., Swiatek, E., Patil, S. (2022). Still Creepy After All These Years: The Normalization of Affective Discomfort in App Use. In *proceedings of CHI Conference on Human Factors in Computing Systems,* 1-19.

Sinclair, B. (2022). The Erosion of Ownership | 10 Years Ago This Month. Retreived online from *Gamesindustry.biz*, May 2022. https://www.gamesindustry.biz/articles/2022-04-06-the-erosion-of-ownership-10-years-ago-this-month.

Singh, S. (2019). Why Social Media is Making us Narrow-Minded. Retreived online from *Medium*, May 2022. https://medium.com/swlh/why-social-media-is-making-us-narrow-minded-ebc8471f0ec1

Sirivianos, M., Kim, K., Gan, J.W., Yang, X. (2014). Leveraging social feedback to verify online identity claims. *ACM Transactions on the Web (TWEB) 8, no. 2 (2014)*, 1-38.

Somayaji, A., Mould, D., Brown, C. (2013). Towards narrative authentication: or, against boring authentication. In *Proceedings of the 2013 New Security Paradigms Workshop,* 57-64.

Squires, B. (2021). You Don't Own the Digital Movies You Buy on Amazon Prime. Here's Why. Retrieved from *Looper*, May 2022. https://www.looper.com/493939/you-dont-own-the-digital-movies-you-buy-on-amazon-prime-heres-why/

Stamp, M. (2011). *Information Security: Principles and Practice*. John Wiley & Sons.

Star, S.L. (1999). The ethnography of infrastructure. In *American behavioral scientist, 43(3),*377-391.

Stenros, J. (2017). The game definition game: A review. In *Games and culture 12, no. 6 (2017),* 499-520.

Stylianou, K., Venturini, J., Zingales, N. (2015) Protecting User Privacy in the Cloud: An Analysis of Terms of Service. In *European Journal of Law and technology 6(3)*

Suits, B. (1990). *Grasshopper: Games, Life, and Utopia.* Jaffrey, NH: David R. Godine.

Svensson, S., Richter, J.L., Maitre-Ekern, E., Pihlajarinne, T., Maigret, A., Dalhammar, C. (2018). The emerging 'Right to repair'legislation in the EU and the US. In *Going Green CARE INNOVATION 2018*.

Szpytek, P.H.. 2021. Microsoft has made Game Ownership Tricky. Retrieved online from *GamerRant*, May 2022. https://gamerant.com/microsoft-xbox-game-ownership-digital-focus-debate-good-bad/

Tanenbaum, T.J. (2015). Hermeneutic Inquiry for Digital Games Research. In *The Computer Games Journal 4(1),* 59–80.

Tanenbaum, T.J. (2020). Publishers: let transgender scholars correct their names. *Nature 583, no. 7817 (2020),* 493-494.

Tanenbaum, T.J., Rettig, I., Shwartz, H.M., Watson, B.M., Goetz, T.G., Spiel, K., Hill, M. (2021). High Level principles for name changes in publishing. *Committee on Publication Ethics.*

Taylor, T.L. (2006). *Play between worlds: Exploring online game culture*. MIT press.

Taylor, T.L. (2009). The assemblage of play. In *Games and culture, 4(4), 331-339.*

Turow, J. (2003). Americans and Online Privacy: The System is Broken. In *Departmental Papers (ASC), University of Pennsylvania, Annenberg Schoolf of Communication.*

Vertesi, J. (2014) My Experiment Opting Out of Big Data Made Me Look Like a Crimminal. In *Time*. Retreived on 10/18/2022 from https://time.com/83200/privacy-internet-big-data-opt-out/

Vertesi J & Dourish P (2011) The Value of Data: Considering the Context of Production in Data Economies. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work.*

Waddell, F.T., Auriemma, J.R., & Sundar, S.S. (2016). Make it simple, or force users to read? Paraphrased design improves comprehension of end user license agreements. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* 5252-5256.

Waldman P. & Mulvany, L. (2020). Farmers Fight John Deere Over Who Gets to Fix an $800,000 Tractor. In *Bloomberg Business Week*. Retreived from https://www.bloomberg.com/news/features/2020-03-05/farmers-fight-john-deere-over-who-gets-to-fix-an-800-000-tractor (September 9, 2021).

Walker, J. (2012). Do We Own our Steam Games? Republished from Rock Paper Shotgun. Retrieved online form *Kotaku,* May, 2022. https://kotaku.com/do-we-own-our-steam-games-5883435

Wallace, R. (2014). Modding: Amateur authorship and how the video game industry is actually getting it right. In *BYu L. REv., 219.*

Wang, A.S., Pang, M., & Pavlou, P. (2017). Cure or poison? Impact of identity verification on the creation of fake posts on social media. In *Proceedings of ICIS 2017.*

Wardrip-Fruin, N. (2009). *Expressive Processing: Digital Fictions, Computer Games, and Software Studies*. MIT Press

Wardrip-Fruin, N. (2020). *How Pac-Man Eats.* MIT Press

Willson, M. (2017). Algorithms (and the) everyday. In *Information, Communication & Society* 20, no. 1 (2017), 137-150.

Willson, M. and Leaver, T. (2015). Zynga's FarmVille, social games, and the ethics of big data mining. In *Communication Research and Practice, 1(2), 147-158*.

Wu, Y., Edwards, W.K., & Das, S. (2022). "A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action. In *proceedings of the CHI Conference on Human Factors in Computing Systems,* 1-17. 2022.

Yuan, B., Folmer, E. and Harris, F.C. (2011). Game accessibility: a survey. In *Universal Access in the information Society, 10, 81-100.*

Zimmer, E., Burket, C., Petersen, T., & Federrath, H. (2020) PEEPLL: Privacy-Enhanced Event Pseudonymisation with Limited Linkability. In *Proceedings of 35th Annual ACM Symposium on Applied Computing:* 1308-1311

Zimmer, M. (2008). The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0. In *First Monday.*