



Volume 11 Issue 1



RESEARCH  
ARTICLE



OPEN  
ACCESS



PEER  
REVIEWED

# Addressing gendered affordances of the platform economy: the case of UpWork

**Elisabetta Stringhi** *University of Milan*

**DOI:** <https://doi.org/10.14763/2022.1.1634>

**Published:** 22 March 2022

**Received:** 17 December 2020 **Accepted:** 2 June 2021

**Competing Interests:** The author has declared that no competing interests exist that have influenced the text.

**Licence:** This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>  
Copyright remains with the author(s).

**Citation:** Stringhi, E. (2022). Addressing gendered affordances of the platform economy: the case of UpWork. *Internet Policy Review*, 11(1). <https://doi.org/10.14763/2022.1.1634>

**Keywords:** Digital platforms, Women, Platform economy, gender, Inequality, Cybercrime

**Abstract:** This study investigates UpWork affordances and their implications for female freelancers experiencing different forms of cyberviolence. Building up on a theoretical framework to situate the concept of affordances, gendered affordances and cyberviolence within a platform economy context, I use UpWork as a relevant case study to assess how online platforms that intermediate labour transactions present gendered affordances contributing to cyberviolence against women. I analysed the discussions of female users and freelancers in UpWork in line with the digital methods approach, by conducting a qualitative digital ethnographic analysis. These discussions serve as a foundation for a subsequent critical analysis of UpWork terms of service, to gain a wider understanding of how the digital platform controls information flows and models interactions between different categories of users. The findings suggest that UpWork affordances are gendered affordances, as they allow male users different conducts, as opposed to female freelancers, entrepreneurs, or users. I conclude that, while UpWork core features are allegedly neutral, they enable gendered affordances widening the gender gap in digital market transactions by facilitating the occurrence of cyber violence against women.

This paper is part of **The gender of the platform economy**, a special issue of *Internet Policy Review* guest-edited by Mayo Fuster Morell, Ricard Espelt and David Megias.

## Introduction

The purpose of this study is to explore the gendered affordances of the platform economy (PE) by using digital platform UpWork as a case study. Previously known as Elance-oDesk, Upwork is a digital platform that intermediates transactions between freelance workers and entrepreneurs. UpWork serves as a relevant case study to begin a discussion of the platform economy's gendered affordances that contribute to reproducing gendered cyberviolence, especially in labour relationships. I inquired about UpWork affordances and their implications for female freelancers experiencing different forms of cyberviolence. This study is structured as follows. In the first section, "Theoretical framework: situating gendered affordances within the platform economy", I will provide a theoretical framework to situate the concept of affordances, gendered affordances and cyber violence within a platform economy context. Next, I will describe the methodology used to conduct this study, by illustrating the digital methods and qualitative digital ethnographic analysis approaches in the "Methodology" section. Subsequently, I use this methodology as a foundation for the qualitative digital ethnographic analysis of the discussions of female users and freelancers in UpWork in section "A digital ethnography of UpWork's female freelancers". In this sense, I use UpWork as a relevant case study to assess how online platforms present gendered affordances contributing to cyber violence against women, hence precluding them from an active participation in the PE. These discussions are a foundation for a subsequent critical analysis of UpWork chore features and terms of service, to gain a wider understanding of the digital platform's design and politics, as I point out in section "Addressing the gendered affordances of UpWork TOS". In the final section "Main findings and future research", I conclude that said design and politics choices are gendered affordances backing cyberviolence performed against female freelancers or entrepreneurs, despite UpWork's commitment to create opportunities for all categories of users.

## Theoretical framework: situating gendered affordances within the platform economy

The platform economy is a disruptive phenomenon that re-shaped our societal and labour relationships radically (Cramer & Krueger, 2016; Drahokoupil, Fabo, 2016;

Degryse, 2016; de Groen, Kilhoffer, Lenaerts, Salez, 2017). As of today, there is not an agreed definition of the Platform Economy, which covers different business models. Therefore, “Platform Economy” is rather an *umbrella term* referring to a wide array of products and services (Roy, 2016). Digital platforms are key actors in the PE as they design, manage and shape the intermediation of the transactions between suppliers and consumers or between employer and employees. The surge of the PE due to several technological and social factors (Roy, 2016) brought about positive implications and, eventually, negative impacts, depending on their characterisation (Fuster Morell, Espelt, Renau Cano, 2020). Still, the PE is soaring dramatically, due to the Covid-19 pandemic impact on worldwide social organisation and market performance (Adobe, 2021; Arroyo, Payola, Molina, 2021; Iqbal, 2021).

Academic literature widely discussed the regulation of the PE, also known as the “Collaborative Platform Economy” or “Sharing Economy” (Botsman, Rogers, 2011; Hatzopoulos, Roma, 2017; Petropoulos, 2017). However, scholars investigated the role of the PE in exacerbating gender, race and class hierarchies and biases only in recent times (Edelman & Luca, 2014; Schoenbaum, 2016). Yet, few studies focused on the PE’s implications for the questions of identity, in particular, of gender identity and relationships, as follows. Initial inquiries revealed that, despite its original premises, the PE might reinforce gender biases and discrimination (Schoenbaum, 2016). As a result, such technologies play a powerful role in controlling information flows and modelling interactions between users. Notably, the specific properties and features of online platforms’ design and architecture may contribute to gender bias and discrimination, for instance by providing personal profiles and encouraging posting individual pictures (Edelman & Luca, 2014). As scholars highlight, trust is a key component of the PE (Botsman & Rogers, 2011; Edelman & Luca, 2014). Trust building may be also problematic from a gender viewpoint, as some economy and social psychology studies point out how women would be more risk averse and less likely to trust strangers, compared to men (Borghans et al., 2009; Chen, 2008; Sarin & Wieland, 2012; Booth, Cardona-Sosa & Nolen, 2014; Cipriani, 2017). While female consumers have positive views of the PE, despite the associated increased risks, findings reveal that there is indeed a gender disparity on the supplier side (Roy, 2016). To establish reputation and build trust, digital platforms present specific *affordances*: by way of illustration, creating personal profiles featuring first names, posting identifying pictures, hyper-linking to external social media accounts. Scholars consider that such *affordances* may trigger unintended consequences, such as racial discrimination (Edelman & Luca, 2014). From a gender perspective, the personalisation of the transaction emphasises the significance of the identity of the transacting parties, enhancing the likelihood of gen-

der discrimination (Schoenbaum, 2016).

First scholars who analysed the core characteristics of networked technologies claimed that these introduced new *affordances* for amplifying, recording and spreading information content and social acts, such as persistence, replicability, scalability and searchability of online content (Boyd, 2010). The concept of *affordances* emerged as a crucial analytical tool in the information and communication studies, science and technology studies, ecological psychology studies (Torenvliet, 2003; Parchoma, 2014), communication and design studies (Nagy & Neff, 2015; Evans et al., 2017). The term refers to a range of functions and constraints that an object provides for, and places upon, structurally situated subjects (Davis & Chouinard, 2016). This notion allows to acknowledge technological efficacy without accepting technological determinism (Neff et al., 2012). In other words, affordances are the dynamic link between subjects and objects situated within complex sociotechnical informational systems, such as digital platforms. To expand the category of technological affordance, intended as mere technological qualities, features or cues, authors also identify “*imagined affordances*” of digital platforms (Nagy & Neff, 2015). This latter notion aims at capturing the complex relationship of users’ perceptions, attitudes, and expectations; of technology’s materiality and functionality; and of designers’ intentions and perceptions. Davis & Chouinard (Davis & Chouinard, 2016) critically delineated the mechanisms of *affordance* that take shape through interrelated conditions, concluding that both said mechanisms and conditions represent a dynamic and structural model that addresses how artefacts afford, for whom and under what circumstances. Consequently, the analytical lens of *technological affordance*, or rather as *imagined affordance*, is essential for understanding how technological affordances enable different actions for different users, within a framework of cultural and institutional legitimacy (Davis & Chouinard, 2016).

Some studies addressed the gendered affordances of social media with different outcomes. Lingel and Golub investigated the social media practices of Brooklyn’s drag community, with a focus on the role of online platforms in the lives of drag performers, both as individual artists and as a queer community (Lingel & Golub, 2015). Online platforms included, to name but a few, Facebook, Instagram, Twitter, Tumblr, Pinterest, Grindr, YouTube. The researchers focused on the gendered affordances and politics in mainstream online social media platforms and the related implications for multifaceted identities, with a final discussion of alternate conceptualizations of authenticating online identities and an agenda for design policy in social media platforms. Duguay (Duguay, 2015) examined how queer women per-

formed sexual identity across social media platforms, by focusing on Instagram and Vine and, particularly, on women embodied self-representations either conforming to, either elaborating upon selfie and digital self-representation. Based on queer theory and actor network theory, the study gives insights into the role of platforms in identity performances, for a better understanding of online platforms constraints and affordances for queer representation. Subsequently, the same author (Duguay, 2016) examined the concept of context collapse within social platforms, namely how individuals intentionally redefined their sexual identity across audiences or managed unintentional disclosure. Both the social conditions of the online networks and the technological architecture of social media platforms modelled participants' gender identity disclosure decisions. The author shed light on stigmatised users' gender identity performances within social media platforms and the everyday identity implications. Cirucci (Cirucci, 2017) considers how Facebook users tend to adopt specific expectations and norms concerning the identification process. Some of the respondents believed that gender was an important issue while using the social platform, as Facebook explicitly requires users to define it. Therefore, the author concludes that prejudices learnt online by users are naturalised and reified through a digital performance modelled by Facebook's design.

*Gendered affordances* have both individual and collective implications as per how they model individual agency, as well as how they structure interactions between different kinds of users. Several critics pointed out how apparent neutral approaches to technological design reveal biased gendered assumptions and, subsequently, code, embed and perpetuate *gendered affordances* into digital platforms functioning (Broussard, 2018; D'Ignazio & Klein, 2020; Marwick, 2014; Massanari, 2015; Nakamura, 2014; Noble, 2018; Rosner, 2018). For instance, Bivens and Haimson document how most popular social media platforms as of 2016 required users to subscribe only after providing gender information as part of the signup process (Bivens and Haimson, 2016). Haimson and Hoffmann (Haimson and Hoffmann, 2016) consider that Facebook's algorithms disproportionately flag Native American names for violation, since said names often differ in structure and form from Anglo-Western names, which is demonstrative of how system design choice reflects the subject position of the system's designer. Besides, the authors highlight that the social media's real name policy endangers, rather than protects its most marginalised users. Concerning search engines, certain use of SEO techniques were revealed to result in distorting the representation of black women and girls as sexualised objects by delivering not credible and representative information. These search results are problematic, since there are no other alternatives to modify them through search refinement or changes to the search engine's default filtering

settings (Noble, 2018). Scholars who analysed the sex-for-rent advertising sponsored on Craigslist consider that the platform's core features allow different users to take different actions because of gendered social and cultural patterns at the disposal of users and technology designers (Schwartz & Neff, 2019). As per the sex-for-rent scheme observed on Craigslist, authors observed that harassment is frequently sexual, since perpetrators ask female users to perform sexual acts in exchange for payments. While the essence of the relationships between users remains unaltered, digital platforms provide distinct categories of users for distinct capacities to engage in them, within the creative and digital economies of the PE located in the wider social structures of gender inequality.

Scholars who investigated the topic of cyberviolence argue that online platforms present *gendered affordances* that contribute to the reinstatement of cyberviolence performed on a misogynist basis (Semenzin & Bainotti, 2020). By relying on data collected on Italian Telegram groups and channels, Semenzin & Bainotti investigated the sense of anonymity, the online platform's weak regulation and the possibility to create big male communities afforded by Telegram. The authors concluded that these core features were *gendered affordances*, since they modelled male users' harassing practises, thus contributing to cyberviolence performance. Yet, few studies investigated the *gendered affordances* of digital platforms in the PE context in connection with cyber violence (Schwartz & Neff, 2019; Siapera, 2019).

Schwartz and Neff (2019) suggest that *gendered affordances* may have four main consequences. First, they may suggest different actions to different users based on a gendered variation. Secondly, they may alter the variability in how users take up affordances. Third, they rely on precise cultural repertoires and macro relations between users and their social structures of gender, as highlighted by other authors as well (Zelizer, 2005 and 2012; Davis & Chouinard, 2016, p. 241; Evans et al., 2017). Lastly, *gendered affordances* may reinforce the social structures of gender inequality (Light, 2011). Gendered cyber violence generally refers to the performance of different acts of harassment, violation of privacy, sexual abuse and sexual exploitation and bias offences on a misogynist basis. As of today, there is not an agreed nor binding international legal definition<sup>1</sup>. Hateful speech, sexual harassment, intimidation, defamation, illegal access, illegal interference, identity theft, impersonation, denial of service, cyberbullying, cyberstalking, non-consensual dissemination of intimate images are types of cyber violence, to name but a few. From an intersectional viewpoint, perpetrators of gendered cyberviolence act pri-

1. Refer to the working definition provided in Cybercrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children, *Mapping Study on Cyberviolence*, T-CY(2017)10, Strasbourg, 9 July 2018, p. 5.

marily on a misogynist basis that, however, intertwines with other discriminatory attitudes. Women belonging to indigenous, ethnic and/or religious minority groups, LGBTQA+<sup>2</sup> women, women with disabilities, sex-workers are more at risk (Henry, Powell & Flynn, 2017). Similarly, women engaged in political activism or career, as well as female journalists, academics and women's rights defenders are sensitive targets. Women in the tech industry are potential objects of abuse, too. Chilling effects on users are shadow, yet manifest consequences of gendered cyber violence. After experiencing abuse or harassment in social media, 8% of women stopped posting content that expressed their opinions while 22% stopped sharing such content, thus self-censoring themselves (Ipsos Mori, 2017). However, according to Siapera (Siapera, 2019, p. 39) cyber misogyny (or online misogyny) precludes women from accessing the means of technological production, by confining them to few online spaces supposes insignificant for the technological future. By understanding cyberviolence in said materialistic terms, gendered victimisation aims at segregating and excluding women from an active participation in the PE (Massanari, 2015; Schwartz & Neff, 2019; Siapera, 2019). On this regard, the case of #GamerGate is acutely demonstrative, as Reddit's karma point system, aggregation of material across subreddits, ease of subreddit and user account creation, governance structure, and policies around offensive content served to ease performance of cyber violence against women working in the gaming industry (Massanari, 2015). Hence, *gendered affordances* of digital platforms may be drivers for gendered cyberviolence and, therefore, cause chilling effects on women's agency in the PE.

Building on this literature, *gendered affordances* constitute an analytical lens to investigate how to address gendered cyberviolence within the PE, as digital platforms' features and politics are at the core of and shape the social relations of the PE. Transacting online facilitates to perform different types of cyberviolence, especially whereas the digital platforms scarcely monitor and sanction such digital conducts. These affordances also widen the gender gap on the supplier side of the PE. Therefore, such *affordances* of digital platforms are *gendered*, as they profoundly affect female agency in the PE, as opposed to set goals of openness, fairness and equality.

2. "LGBTQA+ is an evolving acronym that stands for lesbian, gay, bisexual, transgender, intersex, queer/questioning, asexual, non-binary and pansexual used to describe experiences of gender, sexuality and physiological sex characteristics.



## Methodology

UpWork is a relevant case study to assess how online platforms that intermediate labour transactions present *gendered affordances* contributing to gender-based cyberviolence, hence preventing women from an active participation in the PE. The Digital Methods approach (Rogers, 2013) supported the analysis of this study, by considering the digital environments' affordances relevant, namely, by assessing to what extent digital devices and functions structure the communication flow and the social interactions therein (Rogers, 2013). Accordingly with the invitation to "follow the medium" and "follow the natives" (Caliandro, 2017), I collected a selection of UpWork female users' statements regarding experienced episodes of cyberviolence within the platform.

For this reason, I monitored the "Community Discussions" section of UpWork from October to November 2020. To refine the search, I conducted during that chosen time frame, I inserted appropriate key words in the platform's internal search engine, such as "harassment", "threat", and "stalking", to name but a few. In total, I collected 25 statements, which are comprehensive of the community's and/or the moderators' comments in some cases. To improve the contextualisation of chosen statements, I collected comments made by other users and/or moderators, for the sake of clarity and completeness. In addition, I collected statements by moderators to get an insight on moderation guidelines and practises within UpWork as well as to provide a comprehensive understanding of the ongoing social dynamics between different categories of users (moderators as opposed to freelancers). Collected statements are published in a timeframe between 2015 and 2020. These extracts serve as a foundation for a subsequent critical analysis on how the gendered affordances of UpWork supports cyberviolence.

The methodological approach consists in a qualitative digital ethnographic analysis (Caliandro & Gandini, 2017) to explore the discussions of female users who experienced episodes of gendered cyberviolence in a PE context. This implied a qualitative observation following the methods of covert ethnography (O'Reilly, 2008). First, it was necessary to gain a selection of female users' statements discussing experienced episodes of cyberviolence in a PE context. This was essential for analysing the social dynamics occurring between the affected users and the remaining community, to collect potential users' feedback on the platform's responsiveness. Besides, non-participant observation (Mills et al., 2010) avoids the Hawthorne effect in the data collection, since users may modify their behaviour if they are aware of being monitored (Merrett, 2006). Lastly, the affordances of digital platforms contain and drive the user's practice to self-categorise one's own



messages, resulting in the users' awareness of "acting in front of an invisible audience" (Caliandro, 2017). This consideration meaningfully applies to the present case, as users' comments are publicly available and accessible. However, ethical concerns for the participants' security, privacy, and safety significantly modelled the methodology. Therefore, following the statements' collection I collected data concerning freelancers', commenting users and moderators, namely geographic location, gender, job description, whether the profile was public, private or only available to UpWork users, whether the profile was "Active", "Ace contributor", "Community guru", as well as form of experienced cyberviolence for freelancers. These data are reported in three different tables joint to this essay (Table 1, Table 2, Table 3). Mostly, statements are female freelancers' first-person testimony of experienced cyberviolence within the platform (see Table 1). Several accounts are private, hence in most cases it was not possible to infer other data concerning freelancers, such as country and job description. Anyhow, most freelancers who provided a geographic location are based in the US, as indicated in the freelancer's profile. This should not, however, be understood as an exhaustive indication of the freelancer's identity, which is often revealed through personal profile pictures. To avoid potential identification of users, said pictures were clearly not included in this essay. Within the observed data set, freelancers' age appears not to be a relevant factor. Nevertheless, this data set as illustrated in Table 1 should be considered just as a partial representation of the wider phenomenon occurring within UpWork. Most users who commented on the female freelancers' excerpts were male and had public profiles, hence providing further details concerning geographic location and job description, as shown in Table 2. Moderators' gender sampling and job description varies, as exhibited in Table 3.

Following this, I applied de-anonymisation techniques to the statements. For example, but without limitation, I proceeded to remove names, places, dates, univocal information as well as I replaced names with ID numbers (as shown in Table 1, Table 2 and Table 3, see annex) and used terms while leaving unchanged the general sense of phrasing, to avoid possible re-identification of users. Thus, I verified whether, by inserting the collected statements or relevant parts thereof in a search engine, it was still possible for a user to find them through a reasonable effort. In this sense, anonymization and de-anonymization techniques prevented from collecting further information than necessary and mentioning personal details that could potentially re-identify the participants.<sup>3</sup>

3. The information collected from each participant individual contribution is associated with a non-identifying ID, applying a random function. Access to this correlation is exclusive to the research's author/s.

## A digital ethnography of UpWork's female freelancers

In most statements, two types of cyberviolence appear recurring: cyberstalking and harassment. In some cases, it is hard to trace a neat line between one kind of cyberviolence and another, as these practises often combine. As female freelancers witness, the perpetrator repeatedly, unwantedly, and disruptively intrudes in their private e-mails and social media accounts outside of UpWork, irrespective of contract inception or termination.

#ID248366: *"I had wrote [sic] this proposal for a job, even though I had just gained two long term clients, [...] Regardless, I am going about my day and I get a message from [...], IMMEDIATELY asking for my number, still unable to give any info on the project. There was no way I was giving my phone number, and his profile is most likely fake, so I blow it off. I figure if the says "contact if interested" then that's all but I had this feeling in my gut just they [sic] way he messaged me – AND now he wont [sic] stop WHO THE HELL IS THIS GUY?????"*

#ID934828: *"Client invited me to bid on his job. He was looking for a \*language\* teacher. I submitted my proposal. We chatted in [sic] Whatsapp because Upwork chat on mobile didn't work. He then messaged and called me at 11pm. I did not answer, but got a bad gut feeling. I withdrew [sic] my offer citing personal reasons. In the next few days, he continued to message and call me. I had to block him on Whatsapp. I can take screenshots to prove it. He's like a crazy internet date! How do I report him so he can't harass other freelancers?"*

#ID997894: *"Though I told him we could work possibly in the future for another job he was just out of control bombarding me with messages [...]."*

Besides, female freelancers describe how harassment is often of a sexual nature, because perpetrators offer targets a payment in return for performing sexual acts. This recurrent practice seems to be in line with the sex-for-rent scheme that scholars observed on Craigslist (Schwartz & Neff, 2019). In our cases, however, sexual harassment mostly involved the sending of picture or, even, the use of a webcam, mainly to acquire sexually explicit imagery. This may lead to further online gendered victimisation: sextortion and the non-consensual dissemination of intimate imagery. Nevertheless, the participants acknowledged the severe violation of their own *sexual privacy* (Citron, 2019), thus refused to comply with such proposals:

#ID476543 *"Because I am not "like that" it took a while to understand what he was*

*really saying. He had to spell it out for me. Basically, I was to be his cam girl. [...] He would make obscene gestures with his tongue on the camera. I got to the point when I refused to be on camera, just audio. Because even though I didn't want to do anything, he would still stare at me and those gestures."*

*#ID698373 "[...] I just got a [sic] invitation for a job where someone is asking me to dress in lingerie and answer his phone and emails over WebCam. How is this allowed?? I feel like it's really inappropriate to have those type of job postings coming to me. Isn't there some sort of safeguard against what it is to me a type of sexual-harassment [sic]. Has this happened to anybody else?"*

Moreover, participants acknowledged to have experienced other types of cyberviolence, including cyberbullying, hate speech and threats. In the latter case, cyberstalking and/or cyberbullying often accompany threatening messages addressed to affected subjects. Such violent communication includes threats to start litigation, to damage one's reputation, even to one's physical integrity and wellbeing, as the below statements denounce:

*#ID364485: "This is his message to me when he read my feedback: "Consider this your warning. Do anything more to hurt my reputation and I will make sure any of your future employer/client who google \*\* Name and Surname \*\* will find information that paints a very negative picture of you."*

*#ID365884: "Quotes client sent me:*

*"where do you live in ....?"*

*I'm guessing it's in a 20 mile radius \*work address on linkedin\**

*"... It looks like \*employer\* and \*employee\* are only a few miles apart. It looks like a nice area. do you have a family?"*

*"You don't know what threatening is ... we will soon find out how much you are willing to endure to steal money that isn't yours".*

Moreover, perpetrators address targeted users with denigrating, humiliating and offending discourse against not only their gender identity, but also their racial and/or religious background, as the following statement highlights:

*#ID939866: "He started to saying [sic] bad things about my nationality and religion*

*[...] He has sent me harassing [sic] messages despite the fact that I still apologized for any delay I caused. I am literally feeling frightened. [...] I desperately need upwork help.,”*

Other statements involved the performance of various forms of cybercrime acts by perpetrators. By way of illustration, cybercriminal conducts included phishing, illegitimate or unfair use of data and abusive access to data processing or telecommunications systems. In practice, these conducts often result in a data breach from a cybersecurity perspective.

*#ID282747: “I installed a security plugin and found out the “error.txt” was uploaded when he wanted to “show me” something and I was no longer able to login but found a matrix like screen and the words “you have been hacked”. A friend [sic] of mine overwrote everything and changed all password because he had excess to everything.”*

Overall, female users search for the community’s opinion and suggestion on how to properly deal with their cases, as they are often unaware of the specific platform’s guidelines and reporting mechanisms. Generally, female freelancers appeared to be keen to emphasise with the affected subjects, whereas male users showed a tendency to trivialise the abusive and/or violent conducts.

Answer 1 #ID 228456:

*“[...] There are a billion freelancers on Upwork...just ignore this dude and move on. Also, “stalking” is a very strong expression here...its [sic] not like he unexpectedly showed up at your place. There are people who suffer from real stalkers who makes their lives miserable, this is not that.”*

Answer 2 #ID 228457:

*“I agree with #ID 228456.Irritating, indeed. “Stalking”? I’m not certain about that term. Just block them. Your Upwork Messenger tool has an easy menu setting for blocking any user from interacting with them all. So do your other communication tools [...].”*

Minimisation of online abusive and/or violent conduct that disproportionately targets women is commonplace (Chemaly, 2019). For example, Lumsden and Morgan (Lumsden & Morgan, 2017) conceptualise the advice given to victims of online

abuse “do not feed the troll” as a “silencing strategy”, to preventing victims from challenging and/or resisting sexist cyber abuse. Adhering to the “do not feed the troll” message trivialises the impact of online abuse and also implies that victimised users shall be complicit with the performed violence, or “symbolic violence” as another author puts it (McRobbie, 2004). Similarly, victim blaming and slut shaming were viewed as commonplace in an analysis involving young people and their exposure to rape culture on social media. (Sills et al., 2016). According to Linabary and Batti, many women challenge the framing of online spaces as “non-serious” spaces or spaces that do not represent the “real world” to challenge hegemonic narratives of cyber violence that shout down women’s experiences of abuse (Linabary and Batti, 2019). UpWork’s freelancer community might be in line with this trend. In some cases, female freelancers admitted to having themselves violated the platform’s Terms of Service (henceforth, ToS). Consequently, the community often commented that violating the ToS somehow encouraged perpetrators to commit such wrongful conducts. Thus, the community was inclined to hold the freelancers responsible for the abusive and/or violent behaviour of perpetrators. Shifting the liability from the perpetrator to the offended subject occurs systematically when discussing episodes of gendered victimisation. Examples of minimisation and victim blaming are evident in the following excerpts, where UpWork’s community downplays the culpability of cyberviolence, even imputes it to the female freelancers.

*#ID 228458:< “I suppose that’s part of the reason why it’s a violation of Upwork’s TOS to give out personal contact information before you reach an agreement with a customer. If you flag him, then you are acknowledging to Upwork that you breached the TOS. Consider it a lesson learned and be pleased Upwork didn’t hit you for breaching its policies.”*

During the study, it was also possible to witness the recurrence of chilling effects on female freelancers’ active participation in the economic transactions, due to the experienced types of cyberviolence within the platform. Three excerpts are demonstrative of said consequences of gender-based victimisation:

*#ID282747: “The tough truth is that I am a struggling freelancer who looked-for some support on my website and have been damaged now a lot. Will not use Upwork ever again.”*

#ID365884: “What can I do about this kind of conduct? After filing a dispute, because the customer didn’t pay me for job, he was furious (plausibly [sic] since considers he’s right), but I didn’t expect him to physically threaten my well-being. I don’t even want to freelance anymore due to this.”

#ID857382: “Hello, I cannot manage to terminate my profile. I am no longer willing to be here since one of the customers I met was incredibly unprofessional and is now stalking me on my social media profiles. [...]”

Regarding the role of UpWork in adequately monitoring and addressing these types of cyberviolence, the analysis of the collected statements revealed important flaws and inefficiencies. Usually, moderators ask reporting female UpWork users in the UpWork “Community Discussions” to keep the details of these episodes of cyberviolence private, to prevent related public discussion. The below extract illustrates the described dynamic.

#ID859443: “I am sharing here this because I don’t appear to get any joy with anyone from UpWork elsewhere. 1. A customer refuses to pay and is abusive and aggressive. 2. I open a dispute and that customer harasses and abuses me. 3. I accidentally close the dispute which UpWork will not open again. 4. The customer next reports me and UpWork warns me. 5. When I reply and attempt to report the said client for further harassment I am told that I have a flag on my profile and not to do it again. 6. There is no mention of said client or any action being taken against him. 7. No one will say to me what I am expected to have done wrong. This is absolutely revolting and UpWork need to take some action now and stop freelancers being treated like this and also treating them like this. PS: I also need evidence of what I have allegedly done wrong

#ID368997: Hi #ID859443, I apologize for your unpleasant experience. I verified your ticket and I can understand that our team is communicating with you and responding all of your questions. Please keep communicating with our team on this support ticket, so we can avoid unnecessary delays and keep all the conversation in one place. If you have any further questions please add them to your ticket and our team will support you. We cant [sic] discuss private particulars publicly in the Community. Thank you!

In addition, moderators refer to the platform’s guidelines, “safety tips” and ToS, beyond providing practical steps to solve the issue at stake.

*#ID368998: "Hi #ID698373, Please ask your customer to confirm their billing method and report them to Customer Support if they suggest to work with you and pay you outside Upwork, or any other inappropriate offer. Don't accept an agreement before a customer confirms their billing method and ensure to review the working conditions and terms in details beforehand, and transcribe them in the message room. Please check the safety suggestions we disclosed here in order to avoid problematic offers."*

While I generally observed that moderators answer female users promptly, it is possible to infer a lack of clear, steady, certain and fair response to reported episodes of cyber violence from the gathered conversations.

Example 1:

*#ID939866: "I am dissatisfied [sic] since no action has been taken by Upwork, although I have delivered screenshots of customer harrasing [sic], threatening, blackmailing & name calling me. Those kind of users [sic] should not be accepted on a professional platform like Upwork."*

Example 2:

*#ID859443: "My issue is that the customer is sending a new communication with further threats (suing for slander for example) every few hours but Support team is answering only once a day. [...] but I basically don't know how to respond to his threats while I wait for assistance's reply as he seems hurried and impatient to suit."*

*#ID 228459: #ID368999, Maybe you could recommend to the commands that be that it is abusive to freelancers to require them to negotiate in good faith with a customer who is harassing or threatening them. The dispute procedure should have a method to address this that doesn't involve a freelancer to keep communicating with somebody engaging in wrong conduct [sic].*

*#ID368999: #ID228459, The support assesses the communication and if it's found that the customer breached Upwork ToS and used abusive words, actions are taken. Sadly, I can't disclose any additional information about #ID859443's report and dispute."*

Generally, female freelancers are dissatisfied with the reporting mechanism, and particularly so with the human-review team assigned to their case. In many cases, this is due to the unresponsiveness of the platform's support team. However, statements also expose lack of specific training not solely on how to address the matter of cyber violence, but also, even more worryingly, the issues of cybersecurity. In



worst cases, female freelancers find themselves locked out of their personal accounts, due to the platform's inadequacies.

#ID282747: *"I have got in touch with Upwork already but they consider this matter as over. The person I was communicating with did not much acquaintance about IP addresses and I inquired if she could let me talk to somebody else..however that never occurred and she closed the issue. I still consider that [amount of money] for this minor task was a decent plus. Upwork did not block him and he appears to work as usual. I think he is still attempting to log into my website to erase his hints. Is there a system to get in touch overseers directly? thank u [sic]"*

#ID368997: *Hi #ID282747, I apologize for the lead time in getting back to your report. I've reviewed your ticket and consider our team established that, given the proof you delivered, we can't proceed against the user you flagged. Please pursue the same request and give any further information that would allow our team to proceed, since we need to get convincing proof before actioning an account.*

#ID282747:> *"Update: Upwork has blocked me now. I have been keeping in touch with them since [sic] [month] and requested them to deal with the payment problem but I have only been getting pre-recorded responses. I have told them that I will make a refund and the customer rep did not deal with this. [...] I am receiving reactions like "you should have told somebody" "You should have flagged it". [...] Is there a way to have my account back? Any good suggestions for other plat-forms? Upwork has the worst customer service. Still expecting a reply."*

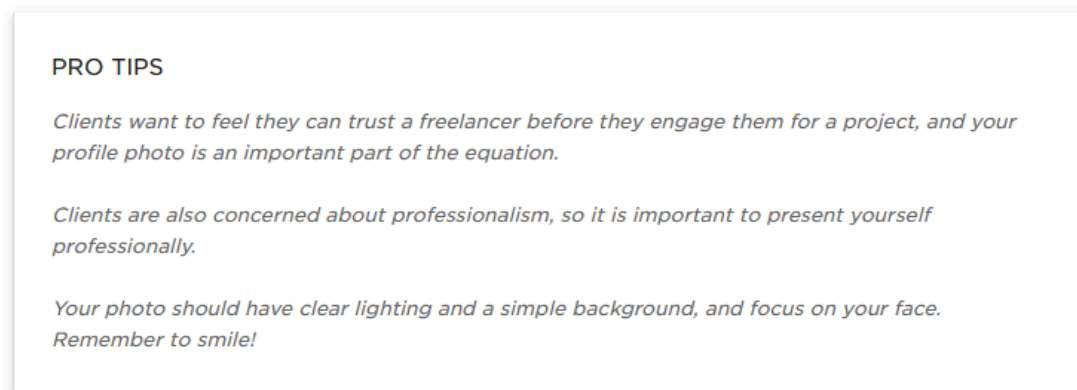
Overall, gendered cyberviolence seems a recurrent practice within UpWork. As some female freelancers considered, the platform itself seems to, somehow, "encourage" such types of online gendered victimisation. This is due to a complex combination of the features and architecture of the platform's design and functioning with the perceptions, attitudes, and expectations of users. By examining UpWork through the analytical lens of *affordance*, it is possible to frame the collected statements in the following terms: UpWork's affordances (or *imagined affordances*) enable different actions for different users in a wider landscape of cultural and institutional legitimacy (Davis & Chouinard, 2016). I state that UpWork's affordances are *gendered affordances*, as they allow male users different conducts, as opposed to female freelancers. Further research would be needed to assess whether *gendered* affordances significantly affect other online platforms intermediating labour transactions (<sup>4</sup>).

4. Further research would be needed on this regard. It is possible to observe a trend, which may be worthwhile analysing, in PeoplePerHour platform. For instance, consider visiting the following thread: <<https://support.peopleperhour.com/hc/en-us/search?utf8=%E2%9C%93&query=harass->

## Addressing the gendered affordances of UpWork ToS

The combination of UpWork's core features and functionalities with the platform's loose ToS contribute to the reinstatement of cyberviolence performed on a misogynist basis against female freelancers or entrepreneurs, despite the commitment to creating economic opportunities "equally available to all qualified talents in our community" (5).

First, users seeking freelancer services are not required to verify their own account, therefore it is easy for clients to create accounts without providing for further self-identification. This is particularly useful for users who attempt or manage to perpetrate cyberviolence offences, as it impedes affected users to identify and report them. Besides, freelancers are encouraged to create a personal profile that displays name, family name, even personal profile pictures. On this latter regard, the platform's ToS dispose that using a profile photo that misrepresents one's identity or represents someone else constitutes fraudulent or misleading use or content. In line with scholars who observed a platform-driven enhancement of discriminatory attitudes and practices (Edelman & Luca, 2014), this feature facilitates gender-based victimisation.



**FIGURE 1:** Picture from UpWork website section "Profile Pictures".

In addition, the platform's policy does not provide for a detailed section on cyberviolence. The ToS include different forms of cyberviolence in the "Prohibited Site Uses" section. UpWork broadly (and vaguely) defines "Unsolicited Contact", which affected users can report by filling out an online form, without referring to

ment>.

5. The statement is available at the following URL: <<https://www.upwork.com/legal#nondiscrimination>>.

cyberstalking. Accordingly, UpWork’s staff will investigate and take appropriate action.

---

#### What is unsolicited contact?

Unsolicited contact is when an Upwork user discovers information on the platform and uses it to contact another person for their own purposes outside of Upwork’s platform. This contact can be to solicit circumvention or for another reason.

Recipients of unsolicited contact have not requested or invited this contact from other users, and should **report it** directly to Upwork Trust and Safety.

---

**FIGURE 2:** Picture from UpWork website section “Unsolicited Contact”.

---

Within the “Safety Section”, Upwork encourages users to flag any content or conduct that violates the ToS, that seems suspicious and inappropriate and/or that constitutes threats or harassment. As shown above, a recurrent practice within UpWork, which is also in line with the sex-for-rent scheme observed on Craigslist (Schwartz & Neff, 2019), is sexual harassment involving requests to female freelancers to send pictures and/or use a webcam to provide sexually explicit imagery in exchange for money. Hence, the platform offers a flagging mechanism. Users can flag freelancer profiles, freelancer portfolios, job postings and messages, too. In case of doubt, users can submit a request to the Customer Support team for “Circumvention Reporting”. In addition, users can report discrimination or harassment to a specific e-mail address. However, UpWork does not publish insight in the content-moderation guidelines, nor communicates indicative time-frameworks of the support team’s responsiveness. In the light of the above-reported users’ considerations, the platform’s support team, which mostly consists of human-review expertise, lacks proficiency in assisting offended users effectively and expeditiously. Hence, enforcement of such ToS is problematic, as UpWork does not provide affected users efficient reporting mechanisms. Besides, there are no publicly available explanations on which decision-making criteria govern how human-review actions and, subsequently, terminates violative accounts. As the policy terms specify, the platform does not assume any obligation to investigate potential violation of the ToS, neither to implement removal requests.

---

#### 4.2 ENFORCEMENT

We reserve the right, but do not assume the obligation, to investigate any potential violation of this Section 4 or any other potential violation of these Site Terms of Use and to remove, disable access to, or modify any content on the Site. Our failure to act with respect to a breach by you or others does not waive our right to act with respect to subsequent or similar breaches. We do not guarantee we will take action against all breaches of these Terms of Use or the User Agreement.

---

**FIGURE 3:** Picture from UpWork website section “Legal Enforcement”.

---

In this respect, transparency is at stake as well. Further aggregated, systematic data on response to cyberviolence and affected users’ feedback on the platform’s action is key for empowering all involved stakeholders, namely, female freelancers. From a preventive viewpoint, there is no commitment to implement automatic removal and filtering of inappropriate and/or abusive content contained, for instance, in job offers and messages. Yet, few female freelancers raised the question of ToS automatic enforcement for prevention purposes. For example, Twitter recently launched a filter to prevent users from sending unsolicited sexually harassing pictures. Similar mechanisms would prevent various types of online gendered-victimisation, i.e. webcam-for-money job offers and/or threatening messages. Redress mechanisms present significant flaws, too. Affected freelancers who lost job opportunities or suffered damages due to cyberviolence experienced within the platform are not entitled to any form of compensation, nor other kind of restore. Lastly, UpWork does not offer prioritised communication and cooperation channels with law enforcement agencies: instead, it only strongly recommends users to report “violations” in the interior reporting mechanisms. From a user-friendliness viewpoint, all forms and tools are in English, which is contradictory to the proclaimed “legal accessibility” policy.

Addressing UpWork gendered affordances and correlated implications for female freelancers is essential for establishing a due diligence mechanism towards women experiencing different forms of cyberviolence in this P.E. context. In this sense, the UN Report (*Cyber Violence Against Women and Girls: A WorldWide Wake-Up Call*, 2015) lays down five key due diligence principles for states and digital platforms to prevent and tackle the systemic concern of gendered cyberviolence: prevention, protection, prosecution, punishment and providing redress. However, the UN “Guiding Principles on Business and Human Rights” (*Guiding Principles on Business and Human Rights*, 2011) adapted to the P.E. context provide for meaningful solutions to improve ToS, conduct and accountability of platforms towards female users (Athar, 2015). Embedding gender in generic digital platform design and architecture that precludes women from accessing market opportunities or, as (Sia-pera, 2019) critically considers in materialist terms, “technological means of pro-

duction”, is a first key step to address the gendered affordances enabling gendered cyberviolence. Scholarly debates about whether online markets reduce the scope of discrimination are vibrant. Yet, digital transactions can limit the flow of undesirable or unnecessary data, namely, the disclosure of information about user identity. Nevertheless, the potential benefits of digital transactions crucially depend on market design (Edelman & Luca, 2014), which notably results in affordances enabling unintended consequences, like cyberviolence as the above statements illustrate. Although designers of online reputation systems pursue the goal of trust building and accountability by disclosure of additional personal information (Dai et al., 2014; Luca & Zervas, 2016), on the downside, they heighten the likelihood of gendered cyberviolence. To address this affordance, UpWork may limit employers’ access to information on a prospective employee, in accordance with anti-discriminatory law practices applicable to the hiring process (Schoenbaum, 2007). Self-disclosure and review by other users may be available to employers following this first stage. In addition, UpWork may require users seeking freelancer services to verify their own identity compulsorily, for example, by matching official identification with online identities. Moreover, UpWork may implement automatic removal of personal contacts (email addresses, phone numbers or social media accounts) before parties begin the transaction, to prevent potential victimisation. These proposed adjustments could be the first key steps in addressing digital platforms’ affordances, especially, gendered imagined affordances. The latter ones include a perception of anonymity and impunity by male perpetrators, too. As entrepreneurs and freelancers transact online, UpWork could monitor their behaviours to assess whether users disproportionately act on gendered preferences, for example, by negatively reviewing female freelancers (Schoenbaum, 2007), without prejudice to data protection standards. Lacking adequate ToS design and implementation, digital platforms facilitate abusive conducts motivated by misogynistic attitudes. Yet, how digital platforms respond to violent self-generated content by users, as well as to safety concerns, seems insufficient. However, digital platforms (UpWork included) are unlikely to face accountability for the unintended consequences of their affordances, cyberviolence included. Digital platforms would address them only because of ethics, rather than profit or law (Athar, 2015; Edelman & Luca, 2014). A lack of due diligence liability and market incentives impedes further advancement in this area. Insofar, digital platforms are not legally bound within the EU legal framework to prevent cyberviolence as defined in this study, excepted for removing illegal online content as mandated under the eCommerce Directive (Directive 2000/31/EC) and countering illegal hate speech online as recommended by the EU Code of conduct on countering illegal hate speech online (European Commission, 2016). Meanwhile, online platforms are bound to counter

discrimination depending on applicable and sectorial national law, such as labour law, by way of illustration. Overall, ToS reflect this fragmented liability landscape, as currently written policies explicitly address only certain matters, i.e. copyright infringements, but not others, including cyberviolence and cyber misogynist content. However, by referring to the cited UN Guiding Principles, accountability for not adequately preventing and tackling cyberviolence represents the next step in compelling digital platforms to due diligence towards female users, beyond the current available measures inclusive of takedown procedures for unlawful content and account termination for misconduct. Since 2016, the European Commission has collected data during monitoring exercises to check progress made to enforce the aforementioned EU Code of conduct, which approximately covers 96% of the EU market share of online platforms that may be affected by hateful content (Statcounter, 2019). According to the European Commission, IT companies joining the EU Code of conduct achieved a decrease in hate speech notices, due to compliance strategies (European Commission, 2019). However, said monitoring action did not comprise action taken to address cyber violent content against female users within a P.E. context. Public research and data are needed on this regard, to increase transparency towards affected stakeholders. Insofar, platform policy took some steps towards countering hate speech, such as reviewing and enforcing ToS prohibiting said content, swiftly removing or disabling access to it, providing training to internal staff, working in partnership with civil society and trusted flaggers, using automatic detection technologies, to name but a few (European Commission, 2019). However, more research and data collection would be useful to monitor other digital platforms apart from main social media and networks. Suggested best practices by the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) include recommendations that State parties to the Istanbul Convention shall implement, among many, the below preventive measures:

i) Encourage the ICT sector and internet intermediaries, including social media platforms, to make an active effort to avoid gender bias in the design of smart products, mobile phone applications and video games, as well as the development of artificial intelligence and - respectively - to create internal monitoring mechanisms towards ensuring the inclusion of victim-centric perspectives as well as to advocate stronger awareness of the perspective and experiences of female users, in particular those exposed to or at risk of intersecting forms of discrimination. Internet intermediaries as well as technology companies should be incentivised to co-operate with NGOs working on violence against women in their awareness-raising and other efforts; (GREVIO, 2021, p. 24).

Therefore, beyond relying on platform self-regulation, public policy should design new accountability frameworks and auditability standards to encourage – if not even bind – digital platforms to address the unintended consequences of *gendered affordances*.

## Main findings and future research

Policymaking should consider embedding gender in digital platform design as a first key step towards addressing gendered affordances in the PE. Other individual categories may be considered to further reducing cyberviolence against women, including LGBTQA+ women, black women, disable women, to name but a few. Otherwise, alleged neutral design choices for trust building and accountability would further strengthen the chilling effect on women’s active participation and, therefore, widen the gender gap in digital market transactions, due to the resulting gendered affordances. This study should serve as a starting point for further discussions in the field. Future research should widen the data set by including a larger collection of participants, by among other investigating the gendered affordances of other digital platforms in the P.E. Upcoming reflections should develop the gender-by-design principles for practical implementation in platforms’ design, architecture and liability. However, analysis should also balance competing interests by covering other arising concerns for over-removal of lawful self-generated content, reliance on automatic filtering rather than human-based support, and users’ privacy interest before law enforcement agencies.

## Appendix

Table 1

The below table shows the witnessing freelancers’ assigned ID number, origin, gender, type of experienced cyberviolence, type of profile, availability of the profile, job description.

**TABLE 1:** Witnessing freelancer information

ASSIGNED ID NUMBER	ORIGIN	GENDER	FORM OF EXPERIENCED CYBERVIOLENCE	PROFILE TYPE	PROFILE AVAILABILITY	JOB DESCRIPTION
#ID248366	US	Female	Cyberstalking	Ace contributor	Public	Social media
#ID934828	US	Female	Cyberstalking	Active	Public	Translator
#ID997894	n.a.	Female	Cyberstalking	Active	Private	n.a.



ASSIGNED ID NUMBER	ORIGIN	GENDER	FORM OF EXPERIENCED CYBERVIOLENCE	PROFILE TYPE	PROFILE AVAILABILITY	JOB DESCRIPTION
#ID476543	n.a.	Female	Sexual harassment	Active	Private	n.a.
#ID698373	n.a.	Female	Sexual harassment	Ace contributor	Only available to UpWorks' customers	n.a.
#ID364485	n.a.	Female	Threats	Ace contributor	Only available to UpWork's customers	n.a.
#ID365884	US	Female	Threats	Active	Public	UX designer
#ID939866	n.a.	Female	Hate speech (racist motive)	Active	Private	n.a.
#ID282747	n.a.	Female	Unlawful access to IT systems	Active	Private	n.a.
#ID857382	n.a.	Female	Cyberstalking	Active	Private	n.a.
#ID859443	n.a.	Female	Threats	Active	Private	n.a.

Table 2

The below table shows commenters' assigned ID number, origin, gender, type of profile, availability of the profile, job description.

**TABLE 2:** Commenter information

ASSIGNED ID NUMBER	ORIGIN	GENDER	PROFILE TYPE	PROFILE AVAILABILITY	JOB DESCRIPTION
#ID 228456	Switzerland	Male	Ace contributor	Public	Copywriter
#ID 228457	US	Male	Community guru	Public	Database designer
#ID 228458	US	Male	Community guru	Public	Writer
#ID 228459	US	Female	Community guru	Public	Marketing writer

Table 3

The below table shows moderators' assigned ID number, origin, gender, type of profile, availability of the profile, job description.

**TABLE 3:** Moderator information

ASSIGNED ID NUMBER	ORIGIN	GENDER	PROFILE TYPE	PROFILE AVAILABILITY	JOB DESCRIPTION
#ID368997	n.a.	Male	Community manager	Private	n.a.
#ID368998	n.a.	Female	Community manager	Private	n.a.
#ID368999	n.a.	Male	Community manager	Private	n.a.

---

## References

Adobe. (2022). *2021 Digital Economy Index* [Report]. <https://business.adobe.com/ca/resources/digital-economy-index.html>

Arroyo, L., Payola, M., & Molina, E. (2021). *Economía de plataformas y COVID-19: Una mirada a las actividades de reparto, los cuidados y los servicios virtuales en España y América Latina*. Inter-American Development Bank. <https://doi.org/10.18235/0003020>

Athar, R., & Padte, R. K. (2015). *From impunity to justice: Improving corporate policies to end technology-related violence against women* (End Violence: Women's Rights and Safety Online). Association for Progressive Communications. <https://www.genderit.org/node/4255/>

Bivens, R., & Haimson, O. L. (2016). Baking Gender Into Social Media Design: How Platforms Shape Categories for Users and Advertisers. *Social Media + Society*, 2(4), 205630511667248. <https://doi.org/10.1177/2056305116672486>

Booth, A., Cardona-Sosa, L., & Nolen, P. (2014). Gender differences in risk aversion: Do single-sex environments affect their development? *Journal of Economic Behavior & Organization*, 99, 126–154. <https://doi.org/10.1016/j.jebo.2013.12.017>

Borghans, L., Golsteyn, B. H. H., Heckman, J., & Meijers, H. (2009). *Gender Differences in Risk Aversion and Ambiguity Aversion* (No. w14713; p. w14713). National Bureau of Economic Research. <https://doi.org/10.3386/w14713>

Botsman, R., & Rogers, R. (2010). *What's mine is yours: The rise of collaborative consumption* (1st ed). Harper Business.

Broussard, M. (2019). *Artificial unintelligence: How computers misunderstand the world* (First MIT Press paperback edition). The MIT Press.

Bucher, T., & Helmond, A. (2018). The Affordances of Social Media Platforms. In J. Burgess, A. Marwick, & T. Poell, *The SAGE Handbook of Social Media* (pp. 233–253). SAGE Publications Ltd. <https://doi.org/10.4135/9781473984066.n14>

Caliandro, A. (2017). Digital Methods for Ethnography: Analytical Concepts for Ethnographers Exploring Social Media Environments. *Journal of Contemporary Ethnography*, 089124161770296. <https://doi.org/10.1177/0891241617702960>

Caliandro, A., & Gandini, A. (2016). *Qualitative research in digital environments: A research toolkit*. ROUTLEDGE.

Chemaly, S. (2019). Foreword. In D. Ging & E. Siapera (Eds.), *Gender Hate Online* (p. ). Springer International Publishing.

Chen, J. (2008). *Gender Differences in Risk Taking: Are Women more Risk Averse?* University of Tilburg. <http://homepage.uvt.nl/~s865056/thesis.pdf>

Ciprani, G. P. (2017). *Gender differences in risk aversion: Evidence from repeated multiple-choice exams* (Report No. 21; Working Paper Series). Department of Economics, University of Verona. <http://dse.univr.it/home/workingpapers/wp2017n21.pdf>

Cirucci, A. M. (2017). Normative Interfaces: Affordances, Gender, and Race in Facebook. *Social Media + Society*, 3(2), 205630511771790. <https://doi.org/10.1177/2056305117717905>

- Citron, D. K. (2019). Sexual Privacy. *Yale Law Journal*, 128, 1870–1960.
- Commission, E. (2019). *Information note—Progress on combating hate speech online through the EU Code of conduct 2016-2019*.
- Council of Europe. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women*. <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>
- Dai, W., Jin, G. Z., Lee, J., & Luca, M. (2014). Optimal Aggregation of Consumer Ratings: An Application to Yelp.com. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2518998>
- Davis, J. L., & Chouinard, J. B. (2016). Theorizing Affordances: From Request to Refuse. *Bulletin of Science, Technology & Society*, 36(4), 241–248. <https://doi.org/10.1177/0270467617714944>
- De Groen, W. P., Kilhoffer, Z., Lenaerts, K., & Salez, N. (2017). The Impact of the Platform Economy on Job Creation. *Intereconomics*, 52(6), 345–351. <https://doi.org/10.1007/s10272-017-0702-7>
- Degryse, C. (2016). Digitalisation of the Economy and its Impact on Labour Markets. *Working Paper ETUI, WP*. <https://www.etui.org/publications/working-papers/digitalisation-of-the-economy-and-its-impact-on-labour-markets>
- D'Ignazio, C., & Klein, L. F. (2020). *Data feminism*. The MIT Press.
- Drahokoupil, J., & Fabo, B. (2016). The Platform Economy and the Disruption of the Employment Relationship. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2809517>
- Duguay, S. (2015). Is being #instagay different from an #lgbttakeover? A cross-platform investigation of sexual and gender identity performances. *SM&S: Social Media and Society 2015 International Conference, Ted Rogers School of Management*. <https://eprints.qut.edu.au/85139/>
- Duguay, S. (2016). “He has a way gayer Facebook than I do”: Investigating sexual identity disclosure and context collapse on a social networking site. *New Media & Society*, 18(6), 891–907. <https://doi.org/10.1177/1461444814549930>
- Edelman, B. G., & Luca, M. (2014). Digital Discrimination: The Case of Airbnb.com. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2377353>
- European Commission. (2016, June 30). *Code of conduct on countering illegal hate speech online*. [https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online\\_en](https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en)
- European Union. (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on electronic commerce”)*. Document 32000L0031. <http://data.europa.eu/eli/dir/2000/31/oj>
- Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating Affordances: A Conceptual Framework for Understanding Affordances in Communication Research: EXPLICATING AFFORDANCES. *Journal of Computer-Mediated Communication*, 22(1), 35–52. <https://doi.org/10.1111/jcc4.12180>
- Fuster Morell, M., Espelt, R., & Renau Cano, M. (2020). Sustainable Platform Economy: Connections with the Sustainable Development Goals. *Sustainability*, 12(18), 7640. <https://doi.org/10.3390/su12187640>
- Haimson, O. L., & Hoffmann, A. L. (2016a). Constructing and enforcing “authentic” identity online:

Facebook, real names, and non-normative identities. *First Monday*. <https://doi.org/10.5210/fm.v21i6.6791>

Haimson, O. L., & Hoffmann, A. L. (2016b). Constructing and enforcing “authentic” identity online: Facebook, real names, and non-normative identities. *First Monday*. <https://doi.org/10.5210/fm.v21i6.6791>

Henry, N., Powell, A., & Flynn, A. (2018). *Not Just “Revenge Pornography”: Australians’ Experiences of Image-Based Abuse A SUMMARY REPORT*. <https://doi.org/10.13140/RG.2.2.29903.59045>

Iqbal, M. (2021). *Zoom Revenue and Usage Statistics (2021)*. Business of Apps. <https://www.businessofapps.com/data/zoom-statistics/>

Light, A. (2011a). HCI as heterodoxy: Technologies of identity and the queering of interaction with computers. *Interacting with Computers*, 23(5), 430–438. <https://doi.org/10.1016/j.intcom.2011.02.002>

Light, A. (2011b). HCI as heterodoxy: Technologies of identity and the queering of interaction with computers. *Interacting with Computers*, 23(5), 430–438. <https://doi.org/10.1016/j.intcom.2011.02.002>

Linabary, J. R., & Batti, B. (2019). “Should I Even Be Writing This?”: Public Narratives and Resistance to Online Harassment. In D. Ging & E. Siapera (Eds.), *Gender Hate Online* (pp. 253–276). Springer International Publishing. [https://doi.org/10.1007/978-3-319-96226-9\\_13](https://doi.org/10.1007/978-3-319-96226-9_13)

Lingel, J., & Golub, A. (2015). In Face on Facebook: Brooklyn’s Drag Community and Sociotechnical Practices of Online Communication: IN FACE ON FACEBOOK. *Journal of Computer-Mediated Communication*, 20(5), 536–553. <https://doi.org/10.1111/jcc4.12125>

Luca, M., & Zervas, G. (2016). Fake It Till You Make It: Reputation, Competition, and Yelp Review Fraud. *Management Science*, 62(12), 3412–3427. <https://doi.org/10.1287/mnsc.2015.2304>

Lumsden, K., & Morgan, H. (2017). Media framing of trolling and online abuse: Silencing strategies, symbolic violence, and victim blaming. *Feminist Media Studies*, 17(6), 926–940. <https://doi.org/10.1080/14680777.2017.1316755>

Marwick, A. (2014). Gender, sexuality, and social media. In H. J & S. TM (Eds.), *Routledge Handbook of Social Media*. Routledge.

Massanari, A. (2017). #Gamergate and The Fapping: How Reddit’s algorithm, governance, and culture support toxic technocultures. *New Media & Society*, 19(3), 329–346. <https://doi.org/10.1177/1461444815608807>

McRobbie, A. (2004). Notes on ‘What Not to Wear’ and Post-Feminist Symbolic Violence. *The Sociological Review*, 52(2\_suppl), 99–109. <https://doi.org/10.1111/j.1467-954X.2005.00526.x>

Merrett, F. (2006). Reflections on the Hawthorne Effect. *Educational Psychology*, 26(1), 143–146. <https://doi.org/10.1080/01443410500341080>

Mills, A. J., Durepos, G., & Wiebe, E. (2010). *Encyclopedia of case study research*. SAGE Publications. <http://knowledge.sagepub.com/view/casestudy/SAGE.xml>

Mori, I. (2017). *Online abuse and harassment*. <https://www.ipsos.com/sites/default/files/ct/news/documents/2017-11/online-experiences-tables-2017.pdf>

Nagy, P., & Neff, G. (2015). Imagined Affordance: Reconstructing a Keyword for Communication

Theory. *Social Media + Society*, 1(2), 205630511560338. <https://doi.org/10.1177/2056305115603385>

Nakamura, L. (2014). Gender and Race Online. In M. Graham & W. H. Dutton (Eds.), *Society and the Internet* (pp. 81–96). Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199661992.003.0006>

Neff, G., Jordan, T., McVeigh-Schultz, J., & Gillespie, T. (2012). Affordances, Technical Agency, and the Politics of Technologies of Cultural Production. *Journal of Broadcasting & Electronic Media*, 56(2), 299–313. <https://doi.org/10.1080/08838151.2012.678520>

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

O'Reilly, K. (2009). *Key concepts in ethnography*. SAGE.

Papacharissi, Z. (Ed.). (2010). Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications. In *A Networked Self* (0 ed., pp. 47–66). Routledge. <https://doi.org/10.4324/9780203876527-8>

Parchoma, G. (2014). The contested ontology of affordances: Implications for researching technological affordances for collaborative knowledge production. *Computers in Human Behavior*, 37, 360–368. <https://doi.org/10.1016/j.chb.2012.05.028>

Petropoulos, G. (2017). *An economic review of the collaborative economy in Bruegel policy contribution* (5 (Policy Contribution No. 2)). <http://hdl.handle.net/10419/173101>

Rogers, R. (2013). *Digital methods*. The MIT Press.

Rosner, D. (2018). *Critical fabulations: Reworking the methods and margins of design*. The MIT Press.

Roy, S. (2016). *The Impacts of Gender, Personality and Previous Use on Attitude towards the Sharing Economy and Future Use of the Services* [California State University, Fresno]. [https://dspace.calstate.edu/bitstream/handle/10211.3/179585/ROY\\_Sandip.pdf?sequence=1](https://dspace.calstate.edu/bitstream/handle/10211.3/179585/ROY_Sandip.pdf?sequence=1)

Sarin, R. K., & Wieland, A. M. (2012). Gender Differences in Risk Aversion: A Theory of When and Why. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2123567>

Schoenbaum, N. (2007). It's Time that You Know: The Shortcomings of Ignorance as Fairness in Employment Law and the Need for an "Information-Shifting" Model. *Harvard Journal of Law & Gender*, 30(99), 54.

Schoenbaum, N. (2016). Gender and the Sharing Economy. Flourishing families in context: A new lens for urban law. *Gender and the Sharing Economy*, 43, 1023.

Schwartz, B., & Neff, G. (2019). The gendered affordances of Craigslist "new-in-town girls wanted" ads. *New Media & Society*, 21(11–12), 2404–2421. <https://doi.org/10.1177/1461444819849897>

Semenzin, S., & Bainotti, L. (2020). *The use of Telegram for the non-consensual dissemination of intimate images: Gendered affordances and the construction of masculinities* [Preprint]. SocArXiv. <https://doi.org/10.31235/osf.io/v4f63>

Siapera, E. (2019). Online Misogyny as Witch Hunt: Primitive Accumulation in the Age of Techno-capitalism. In D. Ging & E. Siapera (Eds.), *Gender Hate Online* (pp. 21–43). Springer International Publishing. [https://doi.org/10.1007/978-3-319-96226-9\\_2](https://doi.org/10.1007/978-3-319-96226-9_2)

Sills, S., Pickens, C., Beach, K., Jones, L., Calder-Dawe, O., Benton-Greig, P., & Gavey, N. (2016). Rape

culture and social media: Young critics and a feminist counterpublic. *Feminist Media Studies*, 16(6), 935–951. <https://doi.org/10.1080/14680777.2015.1137962>

Statcounter. (2019). *Social Media Stats Europe*. GlobalStats. <https://gs.statcounter.com/social-media-stats/all/europe>

Tandon, N., & Pritchard, S. (2015). *Cyber Violence Against Women and Girls: A WorldWide Wake-Up Call* (Discussion Paper 2.0). [https://www.broadbandcommission.org/wp-content/uploads/2021/02/WGGender\\_Executivesummary2015.pdf](https://www.broadbandcommission.org/wp-content/uploads/2021/02/WGGender_Executivesummary2015.pdf)

Torenvliet, G. (2003). We can't afford it!: The devaluation of a usability term. *Interactions*, 10(4), 12–17. <https://doi.org/10.1145/838830.838857>

United Nations. (2011). *Guiding principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (HR/PUB/11/04). New York.

V., H., & S, R. (2017). Caring for sharing? The collaborative economy under EU law in. *Common Market Law Review*, 54(1), 81–127.

Zelizer, V. A. (2012). How I Became a Relational Economic Sociologist and What Does That Mean? *Politics & Society*, 40(2), 145–174. <https://doi.org/10.1177/0032329212441591>

Zelizer, V. A. R. (2005). *The purchase of intimacy*. Princeton Univ. Press.

Published by



ALEXANDER VON HUMBOLDT  
INSTITUTE FOR INTERNET  
AND SOCIETY

in cooperation with



CREATE



centre  
— internet  
— et  
— societe



R&I IN3  
Internet  
interdisciplinary  
Institute

Universitat Oberta de Catalunya



UNIVERSITY OF TARTU  
Johan Skytte Institute of  
Political Studies