TO BE OR NOT TO BE ON THE INTERNET: UNPACKING ONLINE ANONYMITY

Lina Eklund[1,2], Emma von Essen[2,3], Fatima Jonsson[2,3] and Magnus Johansson[1, 2]
[1]Uppsala University, [2]SIRG, [3]Stockholm University

SIRG
Research Reports
SIRR, 2018:1

Abstract

In this paper we present a new way of understanding online anonymity. Building on previous research we propose that three structures—technical, legal, and commercial—make up the base for how three facets—factual, social, and physical—of online anonymity can be realised in interactions online. Indeed, we argue that plurality of the concept, anonymities, instead of anonymity might be key in moving research on the matter forward. We present a model where our structures and facets together to build up the phenomenon of online anonymities, which can be seen as processes across time guided by regulations on both a legal and commercial scale as well as the technological structure, which relies heavily on perceptions and interpretations of being anonymous along factual, social, and physical lines. In the end we analyse three empirical examples based on our own research, where we attempt to show how the model can be useful in empirical research.

Introduction

"On the Internet, nobody knows you're a dog."

Image 1: The New Yorker July 5 1993, *(Vol.69 (LXIX) no. 20) Paul Steiner.*

Anonymity on the internet has become a contentious issue; it protects freedom of speech on one hand yet hampers accountability of e.g. crime or bullying on the other. Online anonymity is by some seen as an important freedom, which needs to be protected from, foremost, meddling nation states and corporate interests (Castells 2002; Lessig 2006). At the same time, others are arguing for increased regulation to protect youth and other groups at risk from exploitation, antisocial, and fraudulent behaviours (Citron 2014). Crudely, the polarized debate stands between the proponents of the 'real name internet' of e.g. Facebook (Froomkin 2017), and the anonymous or pseudonymous internet of Reddit (boyd 2014). These positions mirror the common understanding of anonymity as a dichotomy—you are anonymous or you display "yourself".

It is, however, not as simple as the comic strip "…,nobody knows you are a dog" indicated in the early, hopeful days of the internet. Researchers before us have argued that a dichotomous view of anonymity is too limiting and that we need a new understanding of anonymity on the internet (e.g. Nagel and Frith 2015; Kennedy 2006; Nissenbaum 1999). Being nameless does not cover what it means to hide ones identity online (Kennedy 2006). Anonymity online is as complex as the construction of people's multifaceted identities (Nagel and Frith 2015). Online anonymity is a process that exists on different levels and is regulated and defined by various actors and that while empirical studies show this, theoretical development lag behind. There exists no coherent framework for understanding online anonymity, indeed we argue here that the conceptual vagueness which now define the use of the term makes a coherent understanding of online anonymity difficult and limits progress in the study of online social life. This study aims to fill that gap. We 1) draw on the multidisciplinary literature concerning online anonymity and online behaviours 2) derive at a multi-layered conceptual model for

studying online anonymity, and 3) explore the complexity as different facets of anonymity interact and intersect by drawing on three brief empirical examples: reputational feedback on an online auction site, social interaction in an online game, and hate groups on an online forum. We approach the question of online anonymity from our respective social science fields of sociology, economy, and computer and system sciences. We believe that online anonymity is in its essence a multifaceted phenomenon that can best be understand in an inter-disciplinary approach. To highlight the complexity of online anonymity, we argue that it is key to discuss anonymity online using the plural—anonymities.

The structure of the paper is as follows: we first outline our process, discussing the delimitations of our inter-disciplinary approach, we then move on to discuss our analysis of previous research which we have structured according to our attempt at analysing and offering a structure for the studying of online anonymity. We suggest that three structures—technical, legal, and commercial—make up the base for how three facets—factual, social, and physical—of online anonymity can be realised in interactions online. Last, we present our model and provide three empirical examples from our own research where we show how the model can enhance the understanding of anonymities and behaviour online.

A brief note on delimitations and method

We concentrate on the state of research from our three disciplines of sociology, economics, and computer and systems sciences. We subscribe to an idea of online anonymity as contextual, depending on not only social configuration but also platforms and situation of use, yet we still believe in the measurability of our subject of study. Our goal is an interdisciplinary conceptual model useful across the social sciences yet in the limited scope of an article and through the sacrifices that by necessity had to made in order to bridge between fields, we have made delimitations, which may not suit all fields or questions. We are aware that many terms have different meanings in different research fields and that there are theories and concepts which we had to exclude, however, we have tried our best to allow for the various strengths of our fields to make up for their respective lack. We focus on anonymity from the point of individual end-users and their actions and delimit our engagement with related concepts such as privacy; concealing private information while revealing your identity (in economics the concepts are used interchangeably, see discussion Acquisti, Taylor, and Wagman 2016). Our goal is a usable model which can inform research by bringing clarity to the, we argue, now muddled concept of online anonymity. Scholars are welcome to engage with, adapt, remix and expand on our contribution under the creative common terms Attribution and ShareAlike.

We have attempted to take on the emerging issue of understanding online anonymities by mapping the past and charting out the future (Webster and Watson 2002). Our approach is a qualitative literature review, informed by theorizing. As Webster and Watson (2002) argue, theorizing is crucial for any good review, yet a complex and abstract skill. We have thus

chosen to draw on Swedberg's (2011) theorizing method. As online anonymity is studied in multiple fields and under many guises our approach, we felt, had to look at many fields of research. Our work then became to summarize, coalescence and synthesise the work that has been done. Due to the fractured nature, and multiple meanings of online anonymity we choose a qualitative, ad-hoc strategy where we engaged with previous research using an inductive strategy where we as Webster and Watson (2002) detail, started with key journals (e.g. New Media and Society, Computer and Human Behaviours, American Economic Review) in our fields and completed with searches in the main search engines Web of science, google scholar, and ACM. We used inductive sampling based on the searches and our previous knowledge. Our reading progressed based on the references from searches and literature lists. We read, took notes, and summarized. Our goal was to capture the main trends, debates, and theories, as Swedberg candidly names it, "Anything goes!" (2011: 11). We strived for saturation and thus read until no new concepts, theories, or arguments emerged. In line with Swedberg's (2011) theorizing methodology we started with empirical facts and (1) observed the field (2) name the patterns we found (3) built a model where the patterns we found is made clear and (4) iterated through reading and discussing until we reached a complete model.

Note that we foremost engage with work on anonymities from the authors' main fields of study; sociology, economics, and computer and system sciences. It is thus more than likely that we have missed arguments and aspects from other fields of research. However, our goal is not an all-encompassing meta-theory of online anonymities but to unpack the concept and suggest ways for researchers to move forward in their respective fields when studying anonymities online.

A multidimensional model of online anonymity

Our engagement with previous research has convinced us that rather than talking about online anonymity we should talk about anonymities. Plurality when studying online anonymity might be key to understand the disperse ways in which the concept has been used so far. Online anonymity does not take one simple form but is a multifaceted phenomenon. We argue that three structures—legal, commercial, and technological—and three facets—factual, social and physical—are important to consider for online anonymity. We will first detail the three structures, then move onto the facets.

Structures of anonymity

We see legal, commercial, and technological structures as creating limitations and possibilities for anonymities on the internet. A structure is here seen as an observable pattern, both giving form to and regulating social behaviour. Structures thus both allow and restrict the actions of agents, in short they offer opportunities for action but not unbounded possibilities. Governments and commercial agencies use various means to structure how users can perform

anonymity online, in other words, laws guide what individuals and organizations such as companies can do. Of course, structures matter online as elsewhere, but also because the point in time has passed when we believed that behaviour on the internet was impossible to control (Lessig 2006). Governments have for the past decade placed new online technologies under the rule of law. This has partly included restraining anonymous communication, where both governmental and commercial interests are at work controlling the legal aspects of online anonymity (Froomkin 2017). Laws concretely concern both the right to be anonymous when for example voting or whistleblowing, and govern the use of identifiers connected to data such as personal information, credit card information or the use of IP addresses. Second, commercial entities use various means of regulating anonymity, such as consent through End-User-License-Agreements (EULA) to enable them to use data and identifiers. Third, we have the technological structure and architecture of the internet and its applications, such as the TCP/IP protocol which specifies end-to-end communication works. The technological structure constitutes the key to how it is possible to execute control (Lessig 2006). The three structures of anonymity share that individuals, organizations, and governments all in practice appropriate, subvert, hinder, and assimilate to these structures. The structures are thus not deterministic, yet aids in shaping and allowing certain types of anonymity.

Legal structure

National and international legal systems usually treat anonymity as means to protect personal identity connected to (personal) information (in Swedish and European law), yet there exists no *single* legal concept of anonymity; it differs between sectors as well as countries. Governments has to balance security and efficiency; protecting the freedom of speech while curbing criminal activity. Today governments issue control online to a large extent through chokepoint regulations, i.e. targeting intermediaries, such as Internet Service Providers (ISP), requiring for example retention and transmission of data (identifying end-users). According to Benkler (2006), this type of policy is effective because it takes into account that the internet depends on network effects—the largest social network services and search engines becomes target of these chokepoint regulations. Online interaction and communication crosses national borders and legal regulations requires international cooperation. In 2001, US and European countries signed "the Council of Europe Convention on Cybercrime" to facilitate cooperation to fight computer-related crime. Some countries have used the convention as grounds to require intermediaries to retain data on their customers (Froomkin 2017). However, the relationship between EU and that of its member states' laws on retention is still unclear and this creates uncertainty regarding the legal rights to be anonymous for end-users. A recent example is the case of the Swedish ISP Bahnhof vs. the Swedish government. In 2009, Bahnhof, by purpose, failed to store IP addresses of customers in order to defeat the government's new EU based law on data retention connected to illegal file sharing (International Property Rights Enforcement Directive, IPRED). In 2014, European Court of Justice (ECJ) struck down the EU Data Retention Directive for being in opposition to Human Rights laws. The Swedish government claimed that its new IPRED law on data retention were not in conflict with Human Rights, and mandated IPSs to retain data longer than data

protection law allows. Bahnhof has opposed this interpretation of the Swedish law. They only store data for six months as required by data protection law and only transmit customer data if there is a serious crime involved. In 2017 the ECJ ruled in favour of Bahnhof.

Both individuals and organisations resist and subvert the law, yet do so within this structure. Legal ruling, both on a state and intra-state level, thus affect how one can and cannot be anonymous on the internet.

Commercial structure

Regulations of anonymity online do not only come from governmental attempts to enforce possible accountability; there are also commercial interests (e.g. (Froomkin 2017; Acquisti, Brandimarte, and Loewenstein 2015). Under the rule of law, EULAs specifies under what conditions the end-user can use the software or website. As a structure it is, however, problematic as end-users often clicks accept without reading or understanding the agreement. Many EULAs include giving the right to the software owner to alter, use, and share content individuals create, including photos and location. Information on individual behaviour has become a valuable economic asset for both public and commercial purposes (Spiekermann et al. 2015). The use of customer data can cut costs and increase sales, through e.g., providing targeted products or services to customers and potential customers. Identifying customers directly or indirectly by use of personal information, can ease billing, or prevent un-identified individuals to harm systems. For example, one of the largest social network sites Facebook, requires their users to identify themselves not only in relation to the platform, but also between end-users. Many news sites and blogs require a Facebook account to comment and take part in the public debate, as a way of identification. E-commerce sites such as eBay Sweden require individuals to disclose social security numbers when opening an account, but this information is not disclosed between users. Another set of examples are hardware suppliers that incorporate possibilities for identification in the product such as thumb print readers (an example is the debated concept of trusted computing.). For the past ten years, a decrease in diversity in the market of hardware (e.g. iPhone) and of social network services (e.g. Facebook) has taken place. Less diversity, i.e. centralization to fewer actors, does not only ensure economic interests it also makes it easier to regulate (Froomkin, 2017). However, many users actually engage with resisting commercial interests, by e.g. installing add-blockers or using private browsing.

Data is not only used by each data holder separately it is usually combined across sources. Without understanding the consequences of the future downstream uses of the data, it is impossible for the end user to weight costs and benefits of directly revealing identity or indirectly by sharing information (Skopek 2015). Individuals self-selecting anonymity, by not agreeing to the EULA, involves trade-offs; e.g. not being able to use a platform. Thus commercial applications online provide structure to how end users can/cannot be and act on the internet.

Technological structure

Simplified, we understand technological structure as the software and hardware of the Internet which allows computer-mediated interactions. It is in part both the conventionalized set of principles and values, and the development of architecture and applications enabling and limiting programmers in developing and designing user spaces as well as new technology (e.g. Lessig 2006; Flanagan, Howe, and Nissenbaum 2008).

Technological development can be used for 'good' and 'bad' purposes and have unintended consequences (Castells 2002) also when it comes to anonymity online. How applications enable or anonymities of individual users is much in the hands of programmers and firms who develop them. A classic example is the design difference between the early versions of Internet at University of Harvard and University of Chicago. At Chicago, the administrator designed free access to the network—you could just connect your machine. At Harvard, the administrator built a layer on top of the protocol[1] that required the user to have a registered, licensed, and approved computer to access the network. At Harvard user identities were thus known and all actions could be tracked back to the root of the network, at Chicago it could not. At Harvard the structure enabled user accountability, and user behavior could be regulated. For end-users these types of structures are most often hidden, and it is in everyday use that the structure of the application used determines the visible allowances for example, how end-users can create multiple accounts to disguise their identity at Twitter. This opportunity is now sometimes used for inflating numbers of sympathizers for various oppositional opinions, a clear unintended consequence of the design.

Structures are not neutral, however, they are made in social contexts by individuals who are in turn social beings. One key issue is the gender bias in technology, where programmers, designers, and application developers are primarily men. A consequence is that online applications might be more suited to traditional masculine uses (Rosser 2005) and women's contributions to software development is seen as of lesser value if they are known to be women (Terrell et al. 2017). The gendered nature of design is further visible in how applications often only (this seems to be changing somewhat) have two options for gender toggles, woman/man. Structures such as these affect how people can/cannot present themselves on the internet and this affect anonymity as well as sustains a binary definition of gender.

The technical architecture structure how the internet works and in contribution with platform design lay the ground for how users can be anonymous online.

---

[1] The internet protocol suite is the communication model used on the Internet and other networks. It provides end-to-end communication that includes layers describing how data should be packetized, addressed, transmitted, routed and received.

Summing up structures

Our three structures—legal, commercial, and technological structure—endogenously make interactions and behaviors online possible; the development of technical possibilities of anonymities and the private and public controlling of anonymities. Larsson et al (2012) provides an example of this endogeneity, where legal structures spur the development of new technology for circumventing the law. They found that the more enforcement restricting anonymity, the larger the call for technical solutions for being anonymous online within the file sharing community (ibid.). The technical structure provides ways for how the internet can be regulated by governments and how companies can build products for it, but laws, business interests, and varying uses also feedback into how the internet's structure evolve. We do thus not see any of these structures as necessarily more important than any other, yet they might be so for understanding certain specific case studies. The various power dynamics in play between these regulatory structures will vary and a more detailed debate is simply outside the scope of this study. These opportunities and restrictions can at all times be broken, objected to, and subverted. As structures they are not deterministic but constantly negotiated, changed, and evolving via intended and unintended consequences and actions.

Facets of anonymity

We now move on to a discussion of our three main facets of anonymity—factual, social, and physical facet. We imagine online anonymities as a multidimensional assembly where each facet represents a perspective that can be more or less relevant in the context at hand, as it is constructed by and embedded within socially, embodied, and technological experiences, relationships, implementations, and services. Analytically, these three facets of anonymity can be studied and analysed separately. Nevertheless, together they offer a multidimensional image of online end-user anonymity.

Factual anonymity

Factual anonymity is about non-traceability, or hiding one´s legal identity and other identity related information. Factual anonymity pertains to traceable information about individuals' digital activities shown online, i.e. surname, first name, social security number, or identity number. It can also include digital identifiers such as IP-address and other quasi-identifiers that together can indicate a legal person. Factual anonymity is how anonymity, often, has been defined and measured in most fields (see Pinsonneault and Heppel 1997; Marx 1999). Factual anonymity thus oscillates between three forms: being unknown (traditional notion of anonymity), pseudonymity (having at least a semi-stable pseudonym that can be followed across one or multiple platforms), and nonymity (being completely known on a factual level).

Platforms that offer factual anonymity are still present online, there has however since the early 90's been a shift in online life towards less factual anonymity. For example, on old bulletin boards alias and pseudonyms where common, while with current social network services we see a marked shift towards legal names. This has been called the real names internet (Formkin 2017) (boyd 2014). For example, while MySpace favoured handles, Facebook, Google +, and Blizzard have gone from aliases to real names or e-mails as user profiles on their platforms. Many applications also offer users to log into their platform through a Facebook account, and some apps even require login via Facebook, such as the dating site Tinder. These applications thus draw on Facebook's requirements concerning user's factual nonymity. One argument in the development towards real names is that it can help promote trust, cooperation and accountability (Millen and Patterson 2003). Messages that are factually anonymous has been shown to be less trustworthy (Rains 2007). While there often are, several choices for who can see what identity information on for example Twitter or Facebook, users seldom make an active choice, and end up with the default option of revealing all identity information to all users. Previous literature in behavioural economics have found that default options are important in many setting (see discussion in Mullainathan and Thaler 2000).

Many studies have explored whether users trust sites for shopping and handling their identifier data (factual data), such as real id's, credit card info etc. Acquisti et al (2015) further discuss the uncertainty regarding the consequences of this type of data collection—usually a situation of asymmetric information; the data holder knows more about the collection and usage of data compared to the sharing individual. It is possible for private and public entities to identify individuals without explicitly asking for their identification. All information individuals reveal online can be used to trace a person's legal identity. Today there are plenty of techniques of collecting, storing, curating, analysing, and drawing sensitive inferences from Big Data shared by individuals online.[2] The legal possibilities of data collection and usage are under constant change and actual data collection is often invisible. This generates uncertainty about how much individuals should share, and how much factual anonymity that can be achieved. Expectations of anonymity plays in here, identity might be easily traceable for someone with the necessary skills, yet individuals often believe that they are factually anonymous.

Factual anonymity thus pertains to all information about individuals (and also to potentially other legal units such as organizations) linked to them as legal entities.

---

[2] A related debate is that algorithms involved when analysing BigData from end-users, force anonymity into societal decision making processes. The mathematical models decide who gets fired or hired, with lack of transparency, and no chance to appeal. In circumstances where many individuals might prefer nonymity, the models treat individuals anonymously used under the name of fairness (O'Neil 2016).

Social anonymity

Social life on the Internet is made up by a vast number of different online spaces, where individuals and groups participate, connect, interact, exchange information, and communicate. In these spaces, gender, age, race, ethnicity, sexual orientation, disabilities, and other social identities are more or less visible and identifiable. This is partly due to the design, technical functionalities and limitations and partly due to individual users´ preferences and reasons to hide, obscure or make visible their social identity. In the early days, the Internet was framed as a giant community, characterized by democratic values, freedom of speech, and personal freedom. On the Internet users could switch gender, age, or ethnicity in the brave new cyberspace. Many believed that everyone could choose identity markers such as gender, age, or ethnicity as they please in in cyberspace ("identity tourism", as Lisa Nakamura phrased it, 2002). Even though gender swapping by role playing or crossdressing goes back to the renaissance online networks supposedly allowed people to do this on a larger scale than before the internet due to the possibility of being what we here dub socially anonymous online. However, the understanding of the Internet as a space for self-construction where people explored new, fluid social identities, was soon questioned (Bruckman 1996). Today studies show that most people (though not all) stick with their offline social identities such as gender and that people who conceal their identity or crossperform are often met with suspicion or even hostility (Kendall 1998).

Thus, it can be said that our social identities offline also matter online. That means that those who have power offline, tend to also have power online. Traditional social group belongings shape how we act towards each other and some are among the most basic categories we use to structure the world (in most societies the social category of gender is key for how society is structured). In this light the classic online chat question, ASL(R/P) (age/sex/location, race/picture) speaks to user's desire to fix their interactional partners along these lines. Writing on a message board using a factual anonymous handle the individual can nonetheless reveal key social identity features which will affect interaction with others. Knowing someone's social group belongings can matter in various ways depending if they are similar or dissimilar to an imagined "us" and depend on the power and agency associated with these group memberships.

Research has established that similarities in social identity helps build closeness and establish relationships (McPherson, Smith-Lovin, and Cook 2001). In social psychology it has been argued that a desire for comparison and self-affirmation leads people to prefer friends who are similar to themselves (Festinger 1954). Such group identifiers—or memberships—offer individuals a sense of belonging in the social world; as defined in social identity theory (Tajfel and Turner 1979). An example is, revealing social features online will reduce uncertainty and create affinity and a sense of cohesion among individuals (Beltagui and Schmidt 2015; Eklund 2015). The consequence is that despite the opportunities of the internet to connect people all across the world, people in their every-day interaction end up in social communities where people are similar to themselves across social identity factors.

Social identities are never neutral or unbiased, they are assigned with certain ideas, values, prejudices, and characteristics. Revealing them can give rise to stereotyping which reduces people to essential characteristics and abilities, it functions as a mechanism to exercise symbolic power, e.g. limit women who play games (Vermeulen and Looy 2016). We know from studies on online life that there are different expectations put on individuals labelled or identifying as men, woman, white, black, Asian etc. (Kendall 1998; Nakamura 2002; Turkle 1995). Literature across fields indicate that individuals receive different treatment depending on their gender or race identity online as well as offline (see sociological and economic reviews by Pager and Shepherd 2008; Heckman 1998). Not revealing e.g. gender could therefore work as a strategy to avoid sexual harassment (Eklund 2011). Although, hiding social identity initially can in some situations lead to future punishments (von Essen and Karlsson 2013).

Social identities are more or less accepted in relation to the dominant cultural norms and values in a specific social context and therefore individuals belonging to minorities have motives for staying socially anonymous. For example, women in online gaming might gain from coming across as men. In-group and out-group behaviours can be explained through the social norms that regulate how a community acts, where norms can be seen as utterances of and "oughtness" to act in certain ways, with a possibility of sanctions relating to how transgressions towards the community norms are judged (Verhagen and Johansson 2009). Social anonymity thus pertains to individual's social identities and how much of these are known/not known to interactional partners. Which social identity factors that matters will vary depending on the specific online venue in question.

Physical anonymity

So while online life has traditionally been seen as non-physical—or disembodied—online social spaces are not disconnected from the physical. We cannot leave our 'meat' behind; we are embodied when we interact online (Sundén 2003). Physical anonymity pertains to this, how digital interaction is embodied, but so in various complex ways that act on a micro level and is structured around embodiment and emotion. Physical anonymity is made up out of several layers of physical anonymity where embodiment can take many forms, from sharing bodily experience in online forums, to visual representations of the body, to our physical bodies being tracked online. Emotion concerns how we attempt to draw on and display emotions when limited in our communicative range and how people online manage emotions in order to appear as credible individuals online to drawing on emotions to get to know people and be known in turn.

While online interactions are always also embodied experiences, the level to which bodies are present or visible varies. For example, some users discuss (shared) bodily experiences on forums for illnesses or other physical issues (Daniels 2009) and thereby bring the body into focus. At the same time our bodies and physical reactions are often by default hidden from others in online interaction. In textual interaction we cannot establish eye-contact or shake

each other's hands. Social psychology studies have repeatedly shown how body language affect our interpretation of messages (Duclos et al. 1989) e.g. how smiling might make something seem funnier (Strack, Martin, and Stepper 1988). The lack of such bodily cues, e.g. eye-contact in most online interaction has been considered a chief factor behind online disinhibition (Lapidot-Lefler and Barak 2012), a lack of restraint manifested in various behavioural patterns, such as impulsivity and disregard of others. Unless brought to bear our bodies are not as readily available as they are in offline interaction. We can more easily attempt to hide them and our physical and emotional reactions in social interaction. It is moreover easier to avoid emotional work online as we can stay clear of conversations we are not interested in (Turkle 2012) and we can more easily control which emotions we show in order to manage how we appear to others (Garde-Hansen and Gorton 2013).

Social presence is a key concept when attempting to understand physical anonymity. The term has, in resaerch, been used when discussing interpersonal communication, it classifies how socially present our communcational partners appear to us, or in other words how aware we are of them when using various communication media (Short, Willliam and Christie 1976). Traditionally face-to-face communication has been seen to generate the most social presence and text communication the least. A voice over IP service such as Skype would generate more social presene than a text conversation, as more social ques such as facial experssions are avaliable. Yet, Walther (1992) showed that during e-mails between conference participants participants began developing impressions of other participants based on their written communication and these impressions coudl develop into a sense of intimacy and identification between participants; in other words led to greater perceptions of social presence (ibid.). Moreover, it has been suggested that experiences of social presence and closness during communication can lead to emotional connections (Gooch and Watts 2015). Although there is a reduced set of physical interactions online such as lack of bodily smells, facial expressions, verbal talk, social technological services and functionalities offer ways for embodied interactions and identity cues, such as virtual bodies in the forms of graphical avatars in online worlds, emoticons, video chat programmes, etc. (Daniels 2009) and frequency of mesages can be a way to create co-presence or immediate intimacy.

Another layer of embodiment online is how our physical bodies are being tracked and identified via our online activities. Embodiment in this context is seen as the fusion of technology and (the material) human body (Featherstone and Burrows 1995). With the advance of more sophisticated technological implementations of SNS sites, such as mobile tracking and facial recognition, users' activities and behaviours online have become valuable and significant behavioural identifiers for commercial stakeholders. People like to check in to places, to announce where they are located to their friends.

Some negative aspects of embodied anonymity are cases where other users take control over and reveal individuals physical presence online. Doxing is a key negative form of 'outing' someone's bodily location on the internet. Revenge porn is another, creating discomfort that pictures exist online, even when their name and factual information has long since

disappeared. Using fake or overly edited pictures of one self in for example online dating sites is considered "wrong" by most as we are not being true "about who we are", showing how our bodies matter online.

Emotions are contextual physical and mental expressions that enter every aspect of human life. They are often hard to interpret so depending on the technology we communicate through. The lack of emotional cues online is a well-known communicative problem and concretised in the prevalent use of emoticons to augment meaning in textual interaction (Rezabek and Cochenour 1998). At the same time studies increasingly shows how emotions matter online in how users engage in emotion work in order to manage their emotions (Menking and Erickson 2015). Another aspect is how emotions spread online, by talking about emotional experiences they spread and intensify (see Rimé 2009 for a review). The social context guides which emotions are expected and thus accepted. For example, at websites for mothers and fathers displaying the correct emotions for children is key, whereas in the activity of trolling it is all about rousing emotions in others, while not becoming emotional. Trolls then practice emotional anonymous. Of course trolls have emotions, the goals of a good troll are simply to keep them anonymous in online interaction. There are different cultures of emotions online, and our body and emotions are part of how we are known to others online (Sadowski 2016a). Showing emotions can thus also be used as a bridge between people. We saw this most recently in hashtag campaigns such as #metoo, where women's collective emotions of being sexually harassed created affinity and became the basis for political campaigns in some countries and sectors (Sadowski 2016b).

As how we interact online keep evolving so does the nature of anonymity online and nowhere is that more visible than when discussion physical anonymity. The body is today a prominent presence online which many expose in extreme detail on platforms such as YouTube or Instagram. Here interaction with a follower base can be very physical and personal, while still happening under a user name, this type of interaction is clearly not "anonymous" yet without an understanding of physical aspects of anonymity would appear so. Physical anonymity thus pertains to individual's bodies and emotions and how much of these are known/not known to interactional partners.

Summing up facets of anonymity

Factual anonymity is how we often see anonymity online studied, yet we argue that this is online one facet of what it means to be known and unknown online. While factual anonymity is indeed important it is not everything. Social identities also disclose "who we are" even if disconnected from our legal name etc and some social identities are accepted more and some are accepted less in dominant normative contexts. In reality we expect all facets to interlink and this is especially clear in that legal names often contain social group identifiers. Pictures of people also contain information of some, but not all, social groups people both belong and are excluded from. While the myth of the disembodied internet still seems to dominated some

understanding of internet life increasing evidence rather point to how bodies are communicative resources in online life, both their presence and their absence. When we interact online, various ways of communicating will be more or less rich and communicative cues expressed in body language can be, willingly or unwillingly, shared via text, voice, or visuals. Thus the facets will affect each other but some will likley be more important in some contexts and times.

## A conceptual model of structures and facets of online anonymity

We have explored three main structures and three main facets of importance to online anonymity in our engagement with previous literature. All of these or only one dimension at a time, which are not fixed and therefore can change, changes the opportunity for or nature of anonymity. In practise the facets are not separate but parts of the process of online anonymity. We do not consider them dichotomies, either together or in isolation, they are not mutually exclusive or part of a single continuum, but rather an assemblage of anonymities resulting in a multidimensional anonymity process. While this argumentation might, on some points, overlap with post-structuralism we still take our point of departure in our belief that you can study and measure anonymity online. However, this debate is outside the scope of this paper. We see anonymity on the internet as a flexible process, not a state. Time matters, users move between various states of anonymity at various time points and in different venues and social groups online. Figure 2 details our conceptual model, which can be used when studying online anonymity.

It is beneficial to think of online anonymity as an assemblage of different facets of identifiability made possible by our three main structures. We are using the term assemblage here loosely based on Deleuze and Guattari's (1987) work to indicate how studies could benefit from focusing on anonymity as constructed through the fluid exchangeability of multiple facets and their connectivity. Seeing anonymity in this light focuses on the relations between actors, rather than the state of actors themselves; anonymity as a relational process. Paying attention to relations offers a more dynamic perspective where we can see the unfolding of the social world (Emirbayer 1997). This allows us to understand anonymity not as a state, but as an assemblage, further dependent on subjective interpretation of the social situation. It might indeed matter more whether I perceive myself as anonymous, than whether I actually am anonymous (Kennedy 2006). There is thus both an effective, and an affective quality to online anonymity.

Various structures are part of the assemblage of online anonymity. We have here identified three key one, but other subjects might want to highlight others. These structures both allow and restrict opportunities for the anonymities. As structures they give shape to how anonymity takes place online, yet they are not deterministic, the structures are resisted, subverted, and appropriated at all times. Online anonymity is thus situated as well as relational. In other words, it is dependent on the platform we use, on our interactions with this platform and other

users/agents, as well as the legal system we reside in. Online anonymity thus comes to be in the relations between ourselves, other users, platforms, and other potential agents.

Figure 2: visual representation of the online anonymities model showing three structures and three facets, all changeable over time. The overlap in the middle symbolises the fictive condition of total anonymity.
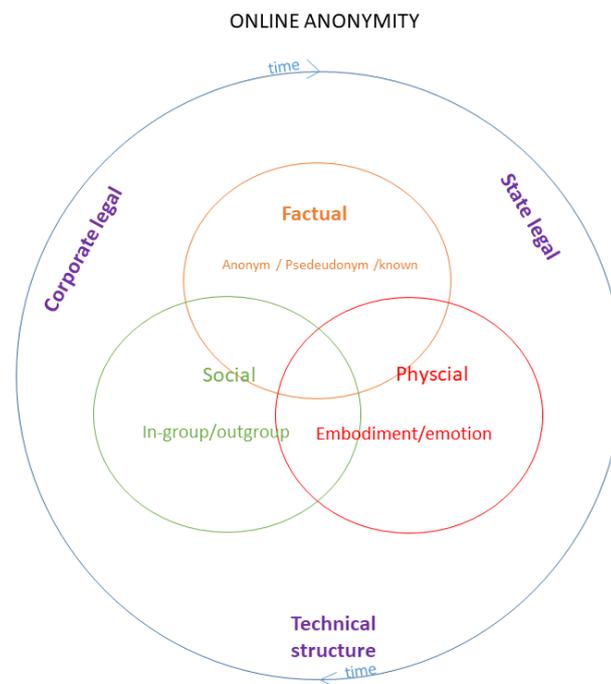
ONLINE ANONYMITY

We believe that this conceptual model of anonymity, where anonymity is understood in this multifaceted sense, has the potential to guide research forward on social aspects of online life. Online anonymity is made up of the three anonymity facets, for a researcher this means that we need to state which aspect of anonymity we are studying, in order for others to situate our research and relate it to studies before and after ours.

Empirical examples

An individual can be more or less anonymous along facets of factual, social, and physical lines. In addition, the legal and commercial level together with the technical structure shape the opportunities for these facets. In the empirical examples below we show that online anonymity work on different facets and levels, and that various anonymities are at stake

depending on social and platform context as well as time. We use fictional individuals who are ideal cases (Weber 1904) based on our own empirical research as we attempt to show how the model can be used.

Example 1: Reputation on online auction sites

Alireza creates an account on the online auction site Swedish eBay intending to sell his used computer games. To minimize fraud eBay's user terms and conditions require factual nonymity between user and platform. Knowing his names might sound foreign in Sweden Alireza rightly fears price discrimination. To get a fair price he thus chooses a pseudonym revealing no social identifier in his interaction with potential buyers. His pictures only show the games themselves. The physical anonymity when buying and selling online makes trust harder, i.e. by not being able to shake hands or judge trustworthiness face-to-face. In this respect, eBay has created a reputation system that encourages trust and sustains trade. Reputational feedback is cumulatively attached to the username; which users cannot change. Many users bid on Alireza's games. After auctions end, but before payment, eBay automatically reveals Alireza's factual identity to buyers, in order to arrange for payment and exchange of goods. Some buyers react negatively due to stereotypes connected to Alirezas name which has been revealed to them. As a consequence, they give him negative feedback.

In this example we can see how factual anonymity matters both between platform and end-user and between seller and buyer. However, social anonymity comes to play in user names and product descriptions and we can understand the reputation system as way to overcome limits due to physical anonymity.

Example 2: Social interaction in online gaming

Anna, a Swedish gamer, creates an account for an online game, she registers her credit card and home address etc. She is thus factually known vís-a-vís the game company. She names her avatar using a pseudonym well-known from other games she has played. Her in-game name Stjärna (meaning Star) has no relation to her legal name. After a few months of playing she joins a clan made up of other Swedes, it feels easier as they have so much in common already. She is open about being a woman "IRL", and participates frequently in voice-chat. At the same time, she is not open about identifying as queer, as she is uncertain how this would be received by her in-game-friends. She is thus partially socially anonymous, while perhaps not appearing so to others. During play emotions run high, elation and happiness when they win and anger and frustration when they lose. Through these, affinity and community is created in these shared emotional experiences. When competing against others Anna engage in bad talking opponents and shaming losers, the norms of the space permit it and she doesn't know these people, or have to look them in the eyes anyway.

In this example we see how, while Anna is factually anonymous towards other users, however, "who she is" is till know, or believed to be known, and shared social identity as Swedes create affinity. Displaying emotions, not being emotionally anonymous, further contributes to these gamers feeling like they know each other. At the same time, Anna is

factually, socially and physically anonymous to most opponents that she only meets in brief encounters. This makes it easier to engage in harassment, which is further not frowned upon (much) in the space.

Example 3: Online hate on Flashback

Flashback is a Swedish online forum, defined by the slogan "Real freedom of expression" (author's translation). A user creates an account under a disposable e-mail and takes care to hide the IP-address from the site owners, making the user factually anonymous. The user joins the thread "Keep Sweden Swedish" under the newly minted pseudonym Ultimatulelover1. Ultimathule is a Swedish 90's rock band known for its dubious connections to neo-Nazis, the name thus signals a certain age and demographic, the band's fans where mostly white men from the countryside of Sweden young during the 1990's. This gives the user instant credibility in the forum thread composed of individuals mostly sharing the same social identity. The user is not socially anonymous. Ultimathulelover1 chooses a profile picture of what is understood to be his own naked torso, showing a tribal tattoo and posing with his arms crossed over his chest, army cargo pants showing. By relinquishing physical anonymity the user further signals identity, in this particular instance gaining credibility even though factual identity is hidden. In the forum emotions are key in building community, feeling the right things at the appropriate moments is central in building affinity between members. At the same time, the factual anonymity makes the user feel safe to engage in hate speech among likeminded, illegal according to Swedish law. While the user is factually anonymous, and taking care to continue to be so, Ultimatulelover1 is still "known" to their interactional counterparts in the forum where Ultimatulelover1 is socially and physically "known", or at least believed to be.

In this empirical example, we see how the end-user, while remaining factually anonymous, still is not actually anonymous in the sense we think about anonymity in an everyday sense. The person in the example, is known as they reveal themselves along social and physical lines. It also becomes clear that anonymities are social in the sense that it is in the interpretation of interactional parties that we can determine if someone is or is not anonymous.

In all of our empirical examples we illustrate how fractured and multiple anonymity can be online and how we can benefit from a plural perspective when talking about being known, or not, on the internet. The examples are brief and thus not all encompassing but intended to illustrate how our model can take into account some of the complexity of online life.

Conclusions

The traditional way of defining anonymity as being nameless is not enough when talking about anonymity on the internet due to the complex nature of online interactions. Instead, we

argue that we should talk about anonymities, which can be seen as processes across time guided by regulations on both a legal and commercial scale as well as the technological structure, which relies heavily on perceptions and interpretations of being anonymous along factual, social, and physical lines. We thus define anonymity as an assemblage of anonymity facets along factual, social, and physical lines structured by technological, legal, and commercial structures.
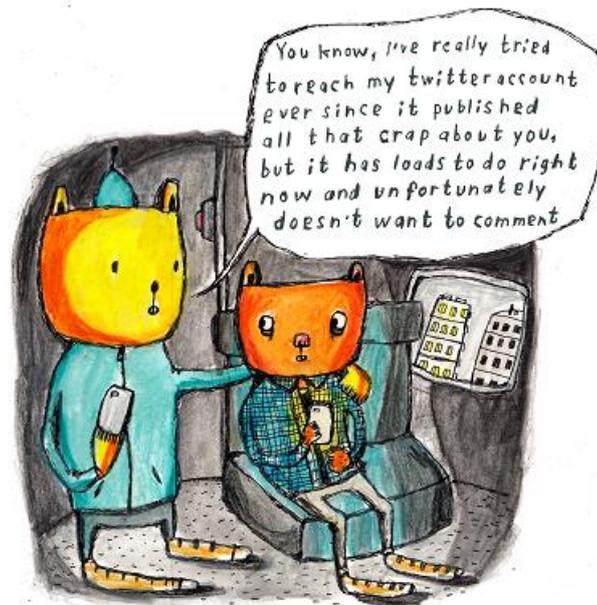

Image 2: *Sara Granér, 2017*

We asked Swedish comic artist Sara Granér to illustrate our results on how we understand anonymity and online life. Her comic, shown above, highlight how online life while perceived as isolated blend into the offline and have consequences beyond what we might have imagined. Also how we might feel anonymous while perhaps only being so along one facet. We can be both anonymous and known at the same time. Plurality of anonymity promises to explain many of the paradoxes of online life. We can be physically anonymous and thus feel "hidden" while still spreading hateful comments using our factual name via our social network account. We can feel exposed by the spread of a naked picture of ourselves even if it lacks our head or other factually identifiable features. We can make forum friends under pseudonyms and feel like they know us, even while never sharing "real names". Our approach also holds promise for rethinking regulation of anonymity online. Many have called for less anonymity in order to curb online hate and harassment, perhaps the most important issue we need to solve online today. Thinking of anonymities instead of anonymity opens up the possibility of trying to regulate different facets than the factual, as reducing the opportunity to be factually anonymous has drawbacks linked to democracy and freedom of speech. Instead we could aim to reduce physical anonymity, as less physical anonymity has the potential to

increase a sense of awareness of other users as full human beings and thus create empathy and a sense of consequences.

Finally, we want to stress that anonymity on the internet is as complex and multifaceted as our identities and with this study we want to challenge researchers from all disciplines to treat it as such.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information | Science." *Science* 347 (6221): 509–14.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. 2016. "The Economics of Privacy." *Journal of Economic Literature* 54 (2): 442–92. https://doi.org/10.1257/jel.54.2.442.

Beltagui, Ahmad, and Thomas Schmidt. 2015. "Why Can't We All Get Along? A Study of Hygge and Janteloven in a Danish Social-Casual Games Community." *Games and Culture*, June, 1555412015590062. https://doi.org/10.1177/1555412015590062.

Benkler, Yochai. 2006. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

boyd, danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. 1 edition. New Haven: Yale University Press.

Bruckman, Amy. 1996. "Finding One's Own Space in Cyberspace." In *MIT Technology Review. January 1996, P. 50*. CUMINCAD. http://papers.cumincad.org/cgi-bin/works/Show?59c3.

Castells, Manuel. 2002. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. OUP Oxford.

Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Harvard University Press.

Daniels, Jessie. 2009. "Rethinking Cyberfeminism(s): Race, Gender, and Embodiment." *Women's Studies Quarterly* 37 (1/2): 101–24.

Deleuze, Gilles, and Felix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia*. Translated by Brian Massumi. 2 edition. Minneapolis, Minn.: University of Minnesota Press.

Duclos, Sandra E., James D. Laird, Eric Schneider, Melissa Sexter, Lisa Stern, and Oliver Van Lighten. 1989. "Emotion-Specific Effects of Facial Expressions and Postures on Emotional Experience." *Journal of Personality and Social Psychology* 57 (1): 100–108.

Eklund, Lina. 2011. "Doing Gender in Cyberspace: The Performance of Gender by Female World of Warcraft Players." *Convergence: The International Journal of Research into New Media Technologies* 17 (3): 323–42. https://doi.org/10.1177/1354856511406472.

———. 2015. "Bridging the Online/Offline Divide: The Example of Digital Gaming." *Computers in Human Behavior* 53 (December): 527–35. https://doi.org/10.1016/j.chb.2014.06.018.

Emirbayer, Mustafa. 1997. "Manifesto for a Relational Sociology." *American Journal of Sociology* 103 (2): 281–317. https://doi.org/10.1086/231209.

Essen, Emma von, and Jonas Karlsson. 2013. "A Matter of Transient Anonymity: Discrimination by Gender and Foreignness in Online Auctions." SIRR Working paper series. Department of Sociology, Stockholm University.

Featherstone, Mike, and Roger Burrows. 1995. "Cultures of Technological Embodiment: An Introduction." *Body & Society* 1 (3–4): 1–19. https://doi.org/10.1177/1357034X95001003001.

Festinger, Leon. 1954. "A Theory of Social Comparison Processes." *Human Relations* 7: 117–40. https://doi.org/10.1177/001872675400700202.

Flanagan, M, D. C. Howe, and Helen Nissenbaum. 2008. "Embodying Values in Technology: Theory and Practice." In *Information Technology and Moral Philosophy*, edited by Jeroen van den Hoven and John Weckert, 322. Cambridge University Press.

Froomkin, A. Michael. 2017. "Lessons Learned Too Well: Anonymity in a Time of Surveillance." *Arizona Law Review* 59: 95–160.

Garde-Hansen, J., and K. Gorton. 2013. *Emotion Online: Theorizing Affect on the Internet*. Springer.

Gooch, Daniel, and Leon Watts. 2015. "The Impact of Social Presence on Feelings of Closeness in Personal Relationships." *Interacting with Computers* 27 (6): 661–74. https://doi.org/10.1093/iwc/iwu020.

Heckman, James J. 1998. "Detecting Discrimination." *Journal of Economic Perspectives* 12 (2): 101–16. https://doi.org/10.1257/jep.12.2.101.

Kendall, Lori. 1998. "Meaning and Identity in 'Cyberspace': The Performance of Gender, Class, and Race Online." *Symbolic Interaction* 21 (2): 129–53. https://doi.org/10.1525/si.1998.21.2.129.

Kennedy, Helen. 2006. "Beyond Anonymity, or Future Directions for Internet Identity Research." *New Media & Society* 8 (6): 859–76. https://doi.org/10.1177/1461444806069641.

Lapidot-Lefler, Noam, and Azy Barak. 2012. "Effects of Anonymity, Invisibility, and Lack of Eye-Contact on Toxic Online Disinhibition." *Computers in Human Behavior* 28 (2): 434–43. https://doi.org/10.1016/j.chb.2011.10.014.

Larsson, Stefan, Måns Svensson, Marcin de Kaminski, Kari Rönkkö, and Johanna Alkan Olsson. 2012. "Law, Norms, Piracy and Online Anonymity: Practices of De-identification in the Global File Sharing Community." *Journal of Research in Interactive Marketing* 6 (4): 260–80. https://doi.org/10.1108/17505931211282391.

Lessig, Lawrence. 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. 2nd Revised ed. edition. New York: Basic Books.

Marx, Gary T. 1999. "What's in a Name? Some Reflections on the Sociology of Anonymity." *The Information Society* 15 (2): 99–112. https://doi.org/10.1080/019722499128565.

McPherson, Miller, Lynn Smith-Lovin, and James M. Cook. 2001. "Birds of a Feather: Homophily in Social Networks." *Annual Review of Sociology* 27 (January): 415–44.

Menking, Amanda, and Ingrid Erickson. 2015. "The Heart Work of Wikipedia: Gendered, Emotional Labor in the World's Largest Online Encyclopedia." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 207–210. CHI '15. New York, NY, USA: ACM. https://doi.org/10.1145/2702123.2702514.

Millen, David R., and John F. Patterson. 2003. "Identity Disclosure and the Creation of Social Capital." In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, 720–721. CHI EA '03. New York, NY, USA: ACM. https://doi.org/10.1145/765891.765950.

Mullainathan, Sendhil, and Richard H. Thaler. 2000. "Behavioral Economics." Working Paper 7948. National Bureau of Economic Research. https://doi.org/10.3386/w7948.

Nagel, Emily van der, and Jordan Frith. 2015. "Anonymity, Pseudonymity, and the Agency of Online Identity: Examining the Social Practices of R/Gonewild." *First Monday* 20 (3). http://firstmonday.org/ojs/index.php/fm/article/view/5615.

Nakamura, Lisa. 2002. *Cybertypes: Race, Ethnicity, and Identity on the Internet*. Routledge.

Nissenbaum, Helen. 1999. "The Meaning of Anonymity in an Information Age." *The Information Society* 15 (2): 141–44. https://doi.org/10.1080/019722499128592.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. 1 edition. New York: Crown.

Pager, Devah, and Hana Shepherd. 2008. "The Sociology of Discrimination: Racial Discrimination in Employment, Housing, Credit, and Consumer Markets." *Annual Review of Sociology* 34 (1): 181–209. https://doi.org/10.1146/annurev.soc.33.040406.131740.

Pinsonneault, Alain, and Nelson Heppel. 1997. "Anonymity in Group Support Systems Research: A New Conceptualization, Measure, and Contingency Framework." *Journal of Management Information Systems* 14 (3): 89–108. https://doi.org/10.1080/07421222.1997.11518176.

Rains, S. A. 2007. "The Impact of Anonymity on Perceptions of Source Credibility and Influence in Computer-Mediated Group Communication: A Test of Two Competing Hypotheses." *Communication Research* 34 (1): 100–125. https://doi.org/10.1177/0093650206296084.

Rezabek, Landra, and John Cochenour. 1998. "Visual Cues in Computer-Mediated Communication: Supplementing Text with Emoticons." *Journal of Visual Literacy* 18 (2): 201–15. https://doi.org/10.1080/23796529.1998.11674539.

Rimé, Bernard. 2009. "Emotion Elicits the Social Sharing of Emotion: Theory and Empirical Review." *Emotion Review* 1 (1): 60–85. https://doi.org/10.1177/1754073908097189.

Rosser, Sue Vilhauer. 2005. "Through the Lenses of Feminist Theory: Focus on Women and Information Technology." *Frontiers: A Journal of Women Studies* 26 (1): 1–23. https://doi.org/10.1353/fro.2005.0015.

Sadowski, Helga. 2016a. *Digital Intimacies : Doing Digital Media Differently*. Linköping: Linköping University Electronic Press, 2016. http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-132634.

———. 2016b. "From #aufschrei to Hatr.org: Digital–material Entanglements in the Context of German Digital Feminist Activisms." *Feminist Media Studies* 16 (1): 55–69. https://doi.org/10.1080/14680777.2015.1093090.

Skopek, Jeffrey M. 2015. "REASONABLE EXPECTATIONS OF ANONYMITY." *Virginia Law Review* 101 (3): 691–762.

Spiekermann, Sarah, Alessandro Acquisti, Rainer Böhme, and Kai-Lung Hui. 2015. "The Challenges of Personal Data Markets and Privacy." *Electronic Markets* 25 (2): 161–67. https://doi.org/10.1007/s12525-015-0191-0.

Strack, Fritz, Leonard L. Martin, and Sabine Stepper. 1988. "Inhibiting and Facilitating Conditions of the Human Smile: A Nonobtrusive Test of the Facial Feedback Hypothesis." *Journal of Personality and Social Psychology* 54 (5): 768–77. https://doi.org/10.1037/0022-3514.54.5.768.

Sundén, Jenny. 2003. *Material Virtualities: Approaching Online Textual Embodiment*. Vol. 13. Peter Lang Publishing. http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0820462047.

Swedberg, Richard. 2011. "Theorizing in Sociology and Social Science: Turning to the Context of Discovery." *Theory and Society* 41 (1): 1–40. https://doi.org/10.1007/s11186-011-9161-5.

Tajfel, Henri, and John C. Turner. 1979. "An Integrative Theory of Intergroup Conflict." *The Social Psychology of Intergroup Relations* 33 (47): 74.

Taylor, T. L. 2002. "Living Digitally: Embodiment in Virtual Worlds." In *The Social Life of Avatars*, edited by Ralph Schroeder BA MSc, 40–62. Computer Supported Cooperative Work. Springer London. https://doi.org/10.1007/978-1-4471-0277-9_3.

Terrell, Josh, Andrew Kofink, Justin Middleton, Clarissa Rainear, Emerson Murphy-Hill, Chris Parnin, and Jon Stallings. 2017. "Gender Differences and Bias in Open Source: Pull Request Acceptance of Women versus Men." *PeerJ Computer Science* 3 (May): e111. https://doi.org/10.7717/peerj-cs.111.

Turkle, Sherry. 1995. *Life on the Screen*. Simon and Schuster.

———. 2012. *Alone Together: Why We Expect More from Technology and Less from Each Other*. Paperback 1. publ. New York, NY: Basic Books.

Verhagen, Harko, and Magnus Johansson. 2009. "Verhagen, Harko, and Magnus Johansson. "Demystifying Guilds: MMORPG-Playing and Norms." In . London, United Kingdom. http://www.digra.org/wp-content/uploads/digital-library/09291.50401.pdf.

Vermeulen, Lotte, and Jan Van Looy. 2016. "'I Play So I Am?' A Gender Study into Stereotype Perception and Genre Choice of Digital Game Players." *Journal of Broadcasting & Electronic Media* 60 (2): 286–304. https://doi.org/10.1080/08838151.2016.1164169.

Walther, Joseph B. 1992. "Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective." *Communication Research* 19 (1): 52–90. https://doi.org/10.1177/009365092019001003.

Weber, Max. 1904. "'Objectivity' in Social Science." In *Classical   Sociological   Theory   2nd   Edition*, edited by Gerteis, Moody, Pfaff, and Virk. Vol. 2007. Oxford: Blackwell.

Webster, Jane, and Richard T. Watson. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly* 26 (2): xiii–xxiii.