Opt Out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm

Fiona Westin
Carleton University
Ottawa, Canada
fiona.westin@carleton.ca

Sonia Chiasson
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

ABSTRACT

This paper explores how the design of online technology influences social factors and manipulates users' online privacy behaviours. In short, users reveal information and participate in online activities even when reluctant due to the influence of dark patterns. We propose *FoMO-Centric Design* as a paradigm for explaining how dark pattern-infused design may lead users to reluctantly behave in a less secure or privacy-preserving way than their attitudes reflect. We review the literature for evidence pointing to the existence of such design and for potential explanations for how it works. We then discuss the implications, present a list of preliminary recommendations, and offer an agenda for the research community based on our findings.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Privacy, Social Factors, Fear of Missing Out, Privacy Paradox, Social Media, Dark Patterns

ACM Reference Format:
Fiona Westin and Sonia Chiasson. 2019. Opt Out of Privacy or "Go Home": Understanding Reluctant Privacy Behaviours through the FoMO-Centric Design Paradigm. In *New Security Paradigms Workshop (NSPW '19), September 23–26, 2019, San Carlos, Costa Rica.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3368860.3368865

1 INTRODUCTION

When considering how to improve security and privacy practices online, usability and informational factors may come to mind; "Is the user informed of potential risks? Are tools designed in a way that makes it easy for the user to mitigate these risks?" Say the answer to both of these questions is "yes"– this should, theoretically, mean the user is free to behave in accordance with their security and privacy attitudes. But what if that is not the case?

The Privacy Paradox [9], which acknowledges the discrepancy between users' privacy attitudes and behaviours, is a well-known phenomenon within the privacy community: users frequently report high concern for privacy, but then behave in ways that disregard privacy. Similar observations apply to users' security behaviours. There are a range of theories [9] attempting to explain this gap, but thus far none have been universally accepted, or able to explain every situation in which the discrepancy arises. In particular, there appears to be a lack of research relating to why users voluntarily proceed with risky behaviours while simultaneously feeling uncomfortable in the act.

This type of behaviour, wherein a person chooses an action against their preferences, is a phenomenon Cassidy calls "participatory reluctance" [17]. We explore the prevalence of participatory reluctance in relation to privacy behaviours. To do this, we look at security and privacy behaviours through the lens of *Fear of Missing Out (FoMO)* [58]. The ubiquity of FoMO resulted in its addition to the Oxford English Dictionary in 2013 [54]; in the same year, a study showed 56% percent of adults reported suffering from FoMO [47]. We hypothesize that this social-media-propagated phenomenon leads users to share more data than they are truly comfortable doing, in order to gain short-term social benefit and avoid negative social consequences, such as perceptions of being reclusive. This over-sharing can have significant security implications since the shared information can be used against the user in various security attacks, for example, by allowing an attacker to infer answers to security questions.

Central to our framework for examining this phenomenon is the concept of design patterns and, specifically, the sub-concept of dark patterns. While design patterns themselves typically have beneficial outcomes for those involved by providing clear guidance on how to solve certain problems, dark patterns tend to manipulate. Our understanding of the term "manipulation" might be aided here by Susser et al.'s [70] definition: "hidden influence–the covert subversion of another person's decision-making power."

Dark patterns have recently been highlighted in the media in relation to social media [10] and are the subject of a US Government bill. Given this recent attention, we believe that a closer examination of exactly how users are manipulated towards privacy-adverse behaviors is warranted. It is through this lens that we present the propagation of the formerly mentioned FoMO-related behaviour as dark pattern-driven design, calling it "FoMO-centric design." We identify *FoMO-centric design* as a collection of manipulative strategies within system design that benefit from users' desires to be accepted socially. By exploiting FoMO-associated behaviours and motivations, *FoMO-centric design* sways users to reluctantly behave in ways that compromise their own privacy-preserving standards and leave them, and whole systems, vulnerable to security threats.

NSPW '19, September 23–26, 2019, San Carlos, Costa Rica

ACM ISBN 978-1-4503-7647-1/19/09…$15.00
https://doi.org/10.1145/3368860.3368865

To lay a solid foundation for understanding FoMO-centric design, we first conduct a literature review covering key related concepts: Fear of Missing Out (FoMO), the Privacy Paradox, Participatory Reluctance, and Dark Patterns. We further cover research that displays evidence of FoMO-centric design at work. Finally, we end with a reflection and discussion, and provide preliminary recommendations and a research agenda for future work in the area.

2 BACKGROUND

2.1 Fear of Missing Out

Przybylski et al. [58] were the first researchers to operationalize the construct *Fear of Missing Out (FoMO)*. They define FoMO as "a pervasive apprehension that others might be having rewarding experiences from which one is absent" and say it is characterized "by the desire to stay continually connected with what others are doing." According to Przybylski et al., this "self-regulatory limbo" [58] results from situational or chronic deficits in the satisfaction of three basic psychological needs — competence, autonomy, and relatedness — required for effective self-regulation and psychological health, according to the Self-Determination theory [26]. Przybylski et al. found a "robust" link between FoMO and high levels of social media engagement.

Since this work, other researchers have touched on the subject of FoMO through topics including academic motivation [6], iPhone separation [21], and attachment style [12].

2.2 Design patterns

Design patterns were introduced by Alexander [5] as a set of flexible solutions to defined recurring architectural problems. Patterns are created through "describ[ing] the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice." Since the publication of Alexander's work, the concept of patterns has gained traction in the fields of computer science and software design, including the branches of security [43] and privacy [60].

Design patterns stand out in their ability to identify recurring real-world problems and provide a roadmap for clear, implementable solutions to those problems. These solutions may be grouped into categories of patterns; within the privacy community, categories which have received dedicated attention include user control [22] and transparency [65]. While the presentation of patterns vary in their levels of organization and implementability, effort has been made to assimilate privacy patterns into a more defined, consistent "language" structure [23]. Security design patterns have received more widespread attention (e.g., [52, 84]) and patterns exist to address many typical security problems.

2.3 Dark patterns

A design pattern only succeeds in being a design pattern insofar as it achieves its original, constructive purpose. When a pattern fails to achieve its goal, or results in unintended consequences, it is a pattern misapplied, and thus becomes an *anti-pattern* [27]. Dark patterns [16], on the other hand, begin with malicious intent and successfully end in its planned consequences. To borrow from Fogg's definition of *planned effects* vs. *side-effects*, "Intentionality is what distinguishes between a *planned effect* [(intentional)] and a *side effect* [(unintentional)] of a technology" [33]. The negative effects of dark patterns are planned. These are, at their heart, the design patterns of manipulation.

Dark patterns take advantage of humans' psychological propensity for certain thought patterns and behaviours in order to trick and manipulate users into taking an action they would've otherwise been unlikely to take. This is distinct from the purpose of persuasive design, which aims to influence positive changes in users' behaviours, in line with their interests [33]. Bösch et al. [14] adopt Kahneman's [40] language of "System 1" (automatic, unconscious) and "System 2" (deliberate, conscious) thinking, saying that dark patterns tend to prompt and maximize the former.

While this psychological manipulation by dark patterns has been acknowledged, few patterns explicitly address social factors contributing to the exploitation of users, with only two notable instances. The first is Bösch et al.'s *Address Book Leeching*. This pattern functions on the basis of humans' "fundamental need to belong" [14], a motivation which they propose may be strong enough to counteract potential privacy concerns. The second instance is the "Social Proof" category created for a number of dark patterns found by a group at Princeton after their recent crawl of 11,000 shopping websites [45].

With a marked research gap concerning social factors as a driving force behind certain privacy dark patterns, and an apparent link between FoMO and System 1 thinking, we set out a new framework for understanding instances of socially-driven dark pattern manipulation: FoMO-centric design. We note that there are likely many forces contributing to these dark patterns, but we focus our attention on FoMO for this paper. We briefly address other possible influences in Section 5.5.

3 FACTORS CONTRIBUTING TO FOMO-CENTRIC DESIGN

We define *FoMO-centric design* as a collection of manipulative strategies that exploit FoMO-associated motivations and behaviours. These typically derive benefit from negative effects on the privacy and/or security of users. Some strategies result in immediate, direct behaviours by users, while other strategies are longer-term and more subtle. Users may use FoMO-centric technologies voluntarily, but this does not mean they are naive to their negative effects: they may feel exploited and continue to participate regardless.

Intuitively, we understand that FoMO likely plays a key role in users acting contrary to their privacy or security desires. But what evidence is there for such a phenomenon in existing literature? And what evidence exists to explain why it happens? We conducted a literature review to find out.

3.1 Literature survey methodology

We collected papers for our literature review by searching the ACM and IEEE digital libraries, and Google Scholar for various combinations of the key words and terms: *privacy*, *social pressure*, *online sharing*, *privacy paradox*, *social media/network*, *problematic smartphone use*, *internet addiction*, *Fear of Missing Out/FoMO*, *social norm*, *affect*, *performative privacy*, *shame*, and *security* and then snowballing relevant sources from the references of those papers until no new papers were found. From this collection, we selected

the most relevant in informing our discussion of FoMO. Through our central searches and snowballing we collected approximately 80 papers and 20 newspaper articles, websites and blog posts that appeared relevant based on a first pass. A second pass allowed us to reduce our set of papers for careful analysis to those directly relevant to our discussion of FoMO-centric design. We then added supporting papers as necessary to expand on certain indirectly related subjects, resulting in a total of 150 sources analyzed, and 85 sources used and cited in this paper.

Collating the results of our literature survey, we find that research relating to FoMO largely falls under two broad categories: *user behaviours and motivations* that lead to FoMO, and *design features* of social media platforms that encourage feelings of FoMO.

The elements contributing to each factor are summarized in Table 1. We address each factor in the following sections.

4 FACTOR 1: USER BEHAVIOURS AND MOTIVATIONS

4.1 Short-term benefits prioritized

The Privacy Paradox [63] is a widespread phenomenon in which the privacy behaviours of users who are self-reportedly highly privacy concerned do not reflect that concern. It was first popularized in an online context in 2000 [63] and has since been reported in a wealth of studies (e.g., [50, 57, 71, 75, 85]).

There is no consensus on what causes this phenomenon; theories range from knowledge deficiencies to the optimistic bias theory and beyond. In 2017, Barth et al. [9] published a systematic literature review organizing privacy paradox theories into main categories and sub-clusters. Our interest in this paper lies in the "Biased-risk assessment within the risk-benefit assessment" sub-cluster– and more specifically, the "(Immediate) gratification" sub-cluster II, as we believe it appears to relate most closely with motivations driving FoMO. It explains that the promise of immediate benefits prompts individuals to behave in ways which may be detrimental to their long term interests. Acquisti et al.'s [3] paper on privacy and rational decision-making found that even when users are sufficiently informed of benefits and risks, they often choose short-term benefits over long-term privacy benefits. Time-inconsistent discounting says that people tend to overrate the present compared to the future [3]. With respect to social media, this suggests that users value the immediate benefit of sharing more than possible future privacy benefits. Acquisti et al. speak to privacy trade-offs being "inherently intertemporal"; that "disclosing data often carries an immediate benefit," but that the costs are "often uncertain, and are generally incurred at a more distant point in time" [4].

4.2 Social isolation avoided

The term "participatory reluctance" was coined in 2016 by Cassidy [17]. This concept challenges typical binary presentations of connection and disconnection in social media– that is, the idea that if a user uses a site it is because they want to, and that otherwise they would discontinue use of the site. Cassidy found that users of gay social media site Gaydar continued to use the site despite voicing strong objections to both its interface, which promoted a stereotypical view of gay men, and its resulting perceived user base. Cited as a significant factor in users' decisions to stay on the site was the "lack of genuine alternatives in terms of niche SNSs [Social Network Sites] designed for the gay male community" [17].

This lack of alternatives meant that Gaydar had gained a kind of "essential" quality for gay men. Despite the fact that users felt "othered" and "isolated" using this website, they felt the alternative (not using the website) would be worse; "akin to choosing to isolate oneself from the gay community." While users were encouraged to "go home" if they didn't like the site, Cassidy points out that leaving the "metaphorical 'club' of Gaydar [...] really does mean effectively going home." The website's only competitors consisted of much the same kinds of experiences that users hated so much in Gaydar. As a result, "users continued maintaining profiles on Gaydar, despite their relationships with the site often being defined by abhorrence– both of the site itself and its imagined audience" [17].

Users of Gaydar were technically free to not use the website, or to "go home", so to speak, but they chose to stay out of fear of isolating themselves further. This is important to keep in mind when we consider whether users are always comfortable with a "voluntary" choice. As shown, hidden factors can be at play.

Since the publication of Cassidy's paper, the concept of participatory reluctance has been discussed in relation to disconnective practices [77] of millenials [28] and politically active youths [20], posting decisions for mixed audiences [59], queer identity on social media [29, 61], and manipulation and "price" in social media [55].

Participatory reluctance might be explained in part by a commitment-based model, which says that users can get "locked in" to a website when there are no competitive alternatives, and that time spent on the site can constitute "sunk costs" which dissuade users from switching (especially if alternatives are not as good) [44]. Nusair et al. [51] found that "calculatively committed Gen Y users stay in a relationship with travel related OSNs [Online Social Networks] because of the lack of alternatives and the switching costs associated with leaving the relationship."

4.3 Community norms established

Online culture has significant impact on users' behaviour and self-regulation. Tufekci [74] proposes that the cultural norms of online environments produce a certain level of "minimum [self-]disclosure" that users feel pressured to follow. She found disparities in the percentage of privacy-concerned participants who used their real names on Myspace (63%) and Facebook (95%). Participants reported an *expectation* of using their real name on Facebook. This community norm can most likely be attributed to the site's real-name policy [31], which penalizes users for using names which are deemed implausible or fake. Facebook CEO, Mark Zuckerberg, acknowledges evolving "social norm[s]" of privacy [7], but frames Facebook's privacy practices as "reflect[ing] what the current social norms are", rather than playing a role in influencing those norms.

Communities perpetuate norms once they are established. In the case of Gaydar, reluctant users continued to maintain the culture that had given them such low expectations to begin with. Cassidy describes this as the "cyclical" nature of a "culture of participatory reluctance"; "[Users] are engaging in an already existing dialogue", and feel obliged to "keep a particular narrative going" [17].

Failing to keep that narrative going may result in negative evaluation — and users are afraid of it. Wolniewicz et al. [83] discovered

Table 1: Factors contributing to FoMO-centric design

Category	Subcategory	Description	References
User behaviours and motivations	Short-term benefits	Users choose short-term benefits over long-term privacy benefits.	[3]
	Social isolation avoided	Users will continue to choose an option that makes them uncomfortable if the alternative appears more socially isolating.	[17]
	Community norms	Users are motivated to behave in accordance with community norms.	
		(1) Once behaviours surrounding community norms have been established, they become cyclical, even if users are unhappy with those norms.	[17]
		(2) Users fear social fallout from failing to meet these norms, including that of "minimum disclosure."	[74]
		(3) Users react negatively to seeing profiles that hide social features, when they were expected to be visible.	[68]
		(4) Users with high privacy concerns were usually peer pressured into adopting social media.	[2]
	Social capital	Impression management and gaining social capital are primary reasons for using social media.	[72]
		(1) Users feel experiences lose their value if they are not digitally shared, including the sharing of one's location.	[11]
Design	Attention-economic logic	Services rely on users to "reproduce" their attention-economic logic.	[39]
		(1) This is attained by designing to "grab" the user in such a way that they provide maximum engagement, and feeds users' desires to produce and attain affective intensity.	[39]
	Service denial	Users with high privacy-preserving standards are often seen as "unprofitable" and denied service.	
		(1) In these cases, users' only option to both get service and preserve privacy is through the use of 3rd-party solutions.	[35]
	Infrastructure informs community	Community norms arise from technologies' digital infrastructure. The framework provided for a community informs its expectations.	[17]
		(1) Social media produces an environment that "equates sociality with sharing."	[56]
	FoMO and SNS use link	Social media use and FoMO are "robustly" associated.	[58]
		(1) Users feel that changing ICT use that undermines or depletes their values and resources, including privacy concerns, is beyond their control.	[11]
		(2) Users feel a sense of "creepiness" when using social media, but feel that is the price to pay for use	[55]
		(3) Users express wishes for outside forces to prevent them from using ICTs in problematic ways	[11]
		(4) Users high in FoMO are more likely to partake in risky behaviours relating to social media use including checking Facebook while driving	[58]

a strong correlation between FoMO, social smartphone use, and fears of negative evaluation. A fear of negative social effect from failing to meet the community norm of minimum disclosure may be justified; Strater et al.'s [68] participants reacted negatively when viewing partially complete Facebook profiles which hid displays of social connections such as the Friends list and the Wall. Acquisti et al. [2] found that a driving force behind the disparity between privacy concerns (which were generally high) and behaviours relating to joining and using Facebook was peer pressure.

In relation to their empirical study of peer effects in voluntary disclosure, Böhme et al. [13] discuss the "self-reinforcing" nature of peer dynamics influencing users' privacy attitudes. They suggest that interventions such as privacy-friendly UI design and user education may not in themselves be enough "to reverse dynamics of descriptive social norms."

4.4 Social capital desired

Social capital is the "resources available to people through their social interactions" [76]. Individuals who are more connected to others have increased opportunities for various supports, job-seeking, or favours. Through the use of social media, users strengthen bonds with others and can increase their social capital [30].

The desire for social capital can lead users to disregard privacy concerns. For example, Tang et al. [72] discuss *social-driven location sharing*, sometimes known as large-group or one-to-many sharing. This form of location sharing, usually done over social media, is presented in contrast to *purpose-driven location sharing* and is driven by impression management and the building of social capital.

Even when users indulge in partial location blurring for privacy purposes, they prefer to keep it minimal, so that it does not negatively interfere with any potential social benefit. "By opting to share a place name that is somewhat precise [...] participants can still appear as though they are actively involved in contributing to their social network's overall social capital. If they opt to share an overtly vague place label (e.g., 'Pennsylvania'), then it may comes across as though they are intentionally being socially reclusive" [72].

Interestingly, Tang et al.'s work finds it is not uncommon for users to lie about their location to make more positive impressions on those in their network. This raises the question: if the user actually *is* in a place they consider to be impressive, do they feel more pressure to share that location, for the sake of social capital? This would fall in line with Bednar et al.'s finding that users feel an experience is worth less if it has not been digitally shared [11].

5 FACTOR 2: DESIGN FEATURES

As stated in the introduction, we define FoMO-centric design as "a collection of manipulative strategies within system design that benefit from users' desires to be accepted socially. By exploiting FoMO-associated behaviours and motivations, *FoMO-centric design* sways users to reluctantly behave in ways that compromise their own privacy-preserving standards." Systems qualifying as FoMO-centric display one or both of the following characteristics:

(1) direct social benefit from using features that may compromise aspects of privacy or security (e.g., location sharing)
(2) indirect social benefit from sharing information with company or service (e.g., being allowed to join, install, or use certain features of app or website by accepting permissions for data collection, or directly providing data such as via forms), which ultimately results in social approval from peers

5.1 Attention-economic logic

Most social media platforms are "free" for end-users to use, but as Paasonen explains, "the price paid for using social media is that of time, attention and data, while affective ripples, releases and reattunements are that which is both generated and gained in the exchange" [55]. Sites are engineered to continuously "grab" users in such a way that they provide the maximum engagement. This, of course, is all part of an attention-economic logic: users' attempts to continuously create and attain affective intensity "binds us to a communicative capital that desires and demands affective responses in order to perpetuate, to *reproduce*, its economic logic" [39]. Personal data gained from this attention grabbing are considered "business assets" for targeted advertising and trading with third companies– a central theme of privacy economics [4].

Designs that appeal to users' tendency to choose short-term benefits and desires to gain social capital, will result in users prioritizing those items, especially when made to choose between them and long-term privacy benefits. If services manage to balance just the right level of "creepiness" and resource depletion with fostered values and rewards, they can create enough ambivalence in users towards the service that they will continue coming back for more, even continuing behaviour the user has already identified as problematic. This feeds into the cycle of participatory reluctance and perpetuates community norms of use, which users feel pressured to follow. At this point, quitting the service may not be seen as an option, as it could be considered akin to isolating oneself socially.

Reluctantly shared information can directly affect security, for example, when used to deduce answers to security questions, used as bait for spear-phishing, or used in other identity theft attacks (as recognized in relation to privacy economics [4]). Information harvested from social media is particularly suited to automated social engineering attacks as it is easy to process [42]. This allows for automated user profiling, large-scale email address validation, and additional personal information collection [8]. "Social" phishing attempts using data mined through social media were found to be 67% effective, compared to the 16% effectiveness of regular phishing [38]. Sensitive data shared through social media may also be exploited through vulnerabilities in inter-application communication [19].

FoMO-fueled insecure decisions also ostensibly occur in activities such as the downloading of software, movies, and/or music from questionable sources. Wang et al. [79] found users were more likely to download illegally when they "did not want to be termed afraid of risk." Research on adolescents [62] has found the greatest predictor of their risky online behaviours is injunctive peer norms. Along these lines, it is reasonable to venture that users might also disable security features because they "get in the way" of an activity they perceive their peers to be participating in or approving of, or click on potentially malicious links within emails or websites (such as in the case of social phishing), for reasons relating to FoMO. In

some ways, the incentives for resisting FoMO are even less tangible for users when dealing with security decisions; users may understand that they are giving up their privacy, but a risk of being attacked is easier to brush off, particularly if they have previously performed similarly risky behaviour with no perceived near-term negative effect.

In other words, it is in companies' interests to design their apps and websites to create and perpetuate behaviours that are brought out by FoMO, as such, essentially perpetuating FoMO itself. It is this kind of design that we suggest to be predatory and suggests that dark patterns are at play. Whether intentional or not, it preys on a kind of ambivalence and participatory reluctance — users know their values are undermined by the social tool they are using [11], but their ambivalence effectively causes them to continue using it [55]. External malicious actors can then benefit from this reluctantly provided information and dependency by launching socially engineered attacks.

5.2 Service denial

Oftentimes, users' access to services is reliant on the leniency of their privacy preferences. An extreme example of this is the install-time permissions model used by Android until recently. In this "ultimatum" model (as Wijesekera et al. [82] put it), all permissions are requested before installation. If the user does not agree to required permissions (which are often privacy-sensitive), the app cannot be installed. Essentially, the user is punished and denied service for having higher-than-desired privacy standards. This happens as well, though perhaps to a lesser degree, in Android's more recent *ask-on-first-use* model, which takes the user's original decision out of context and applies it to all future requests [82].

Denying service to those uncomfortable with the given privacy standards will likely result in users compromising their standards. When users are facing pressure to conform to community norms and to avoid potential social fallout, giving them an ultimatum to either conform wholly and immediately to given privacy parameters or get out does not provide the user with a fair chance to consider privacy or security implications. This is *especially* true if the user is already experiencing high levels of FoMO and feeling both "out of control" of their behaviour and more likely to take risks in the name of social capital. Parallel user behaviours occur where users are pushed towards insecure decisions such as creating accounts on systems to gain access to content/services that should not really need explicit user accounts, or having users agree to legalese terms of service that promise that they will undertake unreasonably complex security precautions.

Service denial is recognized as a dark pattern in the form of Bösch et al.'s *Forced Registration* [14], but they do not relate it to social implications, instead focusing on the *instant gratification* a user gets upon registering to reach their "goal".

Some researchers, such as Guha et al. [35], have explored whether it is possible for a user to use social media websites while maintaining both privacy and full access to services. Many online providers, in lieu of re-engineering their services to protect privacy, choose to simply deny service to users who desire more stringent privacy options, since these users are, in the eyes of the providers, "unprofitable" [35]. Guha et al.'s proposed solution is "NOYB", or "None of Your Business," which allows users more control over their information by using encryption to disallow it from being read by unauthorized parties, without interfering with functionality [35].

However, it seems unlikely that most users would be willing to expend the additional effort (or even have the knowledge) required to use third-party plugins, such as NOYB [35], to preserve both their privacy and access to the service. The fact that these third-party solutions exist in the first place is symptomatic of a larger problem regarding the service's handling of users' privacy.

5.3 Infrastructure informs community

Cassidy [17] argues that a site's digital infrastructure has a major role to play in how people choose to interact with the site and those on it. As illustrated in his study of Gaydar, the cyclical nature of participatory reluctance culture can make it difficult or impossible for users to break out of the cycle and interact with the website in a different way that they might prefer.

By design, privacy-conscious individuals are at a disadvantage using social media from the outset. Papacharissi et al. [56] state that social media creates an "environment that equates sociality with sharing" where a reduced online presence can result in social cost. "[N]etworked social environments make it challenging for individuals to be private in spaces that were designed for sharing, not privacy" [56].

Users may be marketed the illusion that they have independent will to stray from the status quo if they dislike it, but the status quo can have a tremendous impact on users' behaviours. Those with high levels of FoMO, who are especially concerned with how they are viewed by others [83], may be especially susceptible to acting within the status quo. Crucially, that status quo does not arise spontaneously. It begins with how the website, app, or other technology is presented to its audience. If we create an environment where sociality and sharing are synonymous, users *will* share more, because they do not want to be seen as unsociable [39, 72]. Designers have a responsibility to avoid designs that take advantage of users' weaknesses for economic, or other, benefit.

5.4 FoMO and Social Media use

Using a 10-item self-report scale developed to measure low, medium, and high latent levels of FoMO across individuals, Przybylski et al. [58] found that participants who scored low on items of competence, autonomy, and relatedness reported higher levels of FoMO. These participants also reported lower general mood and lower levels of life satisfaction. Correlations were found between high levels of FoMO and interaction with Facebook at "key" times of day, including during university lectures and while driving. Overall, they found FoMO "robustly" associated with social media engagement, and presented FoMO as a "mediator" connecting psychological needs deficits to social media engagement [58].

Through a series of semi-structured interviews, Bednar et al. [11] created a list of values fostered, values undermined, and psychological and societal resources depleted by ICTs (Information and Communication Technologies). Values fostered by ICTs included convenience, efficiency, information accessibility, belongingness, and joy. Undermined values, on the other hand, included friendship (resulting from reduced in-person contact, boredom from digital

overexposure, and friends being distracted by their phones when met in person), and knowledge (through loss of competence with constant access to a search engine, fear of getting lost without a map app, and general feelings of becoming "more stupid"). Psychological resources depleted included an impediment of control and autonomy through addiction; stress, social pressure, distractions, and feelings of wasted time. Societal resources depleted consisted of concerns of information privacy– many users were aware that social platforms "spy" on them and sell their data to third parties, a biased view of reality, and problems associated with the powerful position of ICTs in society [11].

Users noted considerably more disadvantages than advantages to using ICTs, yet continue to use them. Bednar et al. put it succinctly: "Our interview partners are fully aware of [negative effects], but feel incapable of reacting. They expressed the wish to stop, reduce, or change their use, but they do not feel in control of their own behavior" [11]. Paasonen [55] reports a kind of "ambivalence" caused by FoMO and participatory reluctance, making users feel helpless as they continue to use social media in the face of "creepiness" invoked by awareness of data leaks: there is a sense by users that this is simply the price to pay for using the service. And the more users continue to helplessly use the service, the more helpless they are when data leaks do happen; a greater amount of information shared with the service means a greater risk to security when that information is revealed to unintended parties.

Feeling they were "missing out" on the offline world as a result of their dependency, Bednar's participants expressed wishes for social media or smartphones to be abolished, harder sanctions for privacy violations, and even spending more time in nature [11].

Even when seemingly given free range over their behaviours, users still feel constraints on how they can act. Socially-speaking, this is clear in relation to pressure to adhere to community norms and avoiding isolation. Seeking short-term benefits over long-term privacy benefits may also be closely linked, either directly or indirectly, when the benefit is of a social nature. While these characteristics are not necessarily linked directly to FoMO, we suspect their effects would become stronger in individuals with high levels of FoMO. Users high in FoMO are likely to partake in detrimental and risky behaviours, and may put impressing others above their privacy. Finally, users may not feel that changing any of the above behaviour is within their control. Especially noteworthy is that users would like to change their behaviours, but would like external help. This suggests that *built in* measures to help discourage problematic usage would be appreciated by users.

Unfortunately, evidence suggests that this type of problematic usage of social media may be by design (i.e., a dark pattern rather than an anti-pattern), and thus, design changes would need to be accompanied by an attitudinal and directional shift from those responsible for social media platforms.

5.5 Other design considerations

Our reasoning behind the existence of FoMO-centric design focuses on the benefits associated with privacy- and security-compromising user behaviours as laid out above. However, these factors may not be the *only* reason these patterns are implemented, or why they work. Other design considerations including economic, marketing, purchasing, deceptive sales tactics, network economics, and privacy economics could reasonably be at play.

Cost-benefit models of understanding decisions by users, such as those seen in economics, posit a consumer voluntarily trading privacy for some benefit, often assuming a balanced relationship between user and technology. While privacy economics acknowledges the fact consumers may not be aware of *future* uses for their data [4], they do not necessarily focus on solutions to tackling the problem of user manipulation.

While helpful in informing our understanding of the competing priorities when it comes to motivations for using such patterns, they are out of scope of this paper as they do not directly contribute to explaining why or how these patterns may be, directly or indirectly, privacy and security threats by ways of manipulation.

6 DISCUSSION

6.1 Are we okay with this?

Twenty years ago, then-CEO of Sun Microsystems was quoted as saying, "You have zero privacy anyway. Get over it" [67]. Fortunately, not all authorities on technology share this attitude. To the contrary, some are making efforts to alter how technology design is approached, to put the benefit back in favour of the consumer.

Former Google Design Ethicist Tristan Harris has founded the Center for Humane Technology [36] to combat technology's "hijacking our minds and society." He says that today's technology is designed to amplify and exploit users' vulnerabilities to make them act impulsively, against their better judgement. A motivating factor is "Loss-aversion" [49]— in other words, FoMO. To combat it, users must be given the confidence that they are able to disconnect more often *without* missing anything vital. This could be accomplished through the introduction of "useful friction" [49] into technology to slow down users' thinking process and give them the chance to make rational, considered decisions about their technology use– rather than those based on the kind of "fight or flight" response that current technology provokes. Harris is joined by former employees of Google and Facebook; intimately familiar with the inner workings of these companies, they are determined to "correct a wrong" by raising awareness and advocating for change to bring control back to the consumer [15].

Even current employees are speaking out against industry malpractice: Apple CEO Tim Cook published an article in Times Magazine in January 2019 [24] calling for comprehensive federal privacy legislation to "protect and empower the consumer", and regain the "vanishing ability to control our own digital lives."

This comes at a time when "digital wellness" public awareness is at an all-time high; publications such as Cal Newport's *Digital Minimalism* [48] (Newport has been called the "Marie Kondo of Technology") arms readers with techniques for "digital decluttering"; so-called "digital detox" programs have also been increasing in popularity [64]. Responding to such pressure, Apple and Google have released updates to alleviate users of some of this hijacking: iOS 12's Screen Time function [81] allows the user to set "downtime" and time limits on apps, as well as content and privacy restrictions; Android 9 Pie offers an "app timer", "do not disturb" mode, and a "wind down" feature, which gradually eliminates blue light and colour before a user-specified bedtime [37].

As laudable as such measures might be, they have been criticized as the "Marlboro Lights of the tech industry" [41], a stopgap measure shifting the blame from ingrained product design to case-by-case consumer use. While on the surface digital wellness features might help users combat FoMO, they are more of a band-aid for the problem than a real solution. If anything, the fact that such additional settings are needed for imposing limits on product use is proof that the core product itself is flawed. To truly stop disadvantaging users and manipulating them into making privacy choices they do not want, technology's design must be based on a model that benefits them in the long term, rather than takes advantage of their impulses. A product that affords impulsive use will continue to afford impulsive use, even after we put a timer on it.

Of course, it is unfair to suggest designers be held solely accountable for users experiencing FoMO while using their products, since a range of outside factors affect users' experiences. However, as evidenced in this literature survey, the design of a product can aggravate cases of FoMO by provoking FoMO-related emotions (or encouraging deficits in competence, autonomy, and relatedness) and rewarding FoMO-related behaviours, contributing positively to a cycle of FoMO and product use. It is up to designers, therefore, to lessen this effect as much as possible by being held accountable for possible FoMO-traps or dark patterns in their designs, especially where privacy-sensitive data is at stake.

6.2 Preliminary Recommendations

Research in this area is still in early stages, but we set out our initial thoughts about how to move away from FoMO-centric designs and into an environment where users have autonomy over their online privacy-related choices. A failure to act will mean that users will continue to be exploited, because designs based on dark patterns will become more common and more aggressive to win out in an attention-economic system. In this sense, there needs to be a shift in the ecosystem itself at a larger scale, including getting major players on board. We recognize that these recommendations are broad and that they face many challenges to implementation. FoMO-centric designs are prevalent because they work; they achieve direct benefits for the other actors in play (and in some sense for the user as well, although at an increasingly high price). Figuring out how to address the complicated dynamics is a challenge, but we believe that a first step is recognizing and identifying the patterns as problematic in the space of security and privacy, followed by engagement by all stakeholders to work towards more transparent solutions.

Promote privacy-centric designs. As a community, we should promote and create a culture of wanting to give people control over their privacy rather than manipulate them into privacy behaviours that make them uncomfortable. This is a long-standing argument by the privacy community and the basis of the Privacy-by-Design (PbD) [18], but is worth re-iterating. Previous critiques of PbD have complained of the framework being "vague" [78] and too open to interpretation. To combat this, we argue that *explicitly* identifying FoMO-centric designs and proposing concrete privacy-centric alternatives is essential to addressing this problem.

Concrete design recommendations might be achieved through extrapolating Harris' concept of "useful friction." This falls in line with a solution mentioned by Susser [69] in relation to manipulative adaptive choice architectures, where he says that in order to mediate the "invisible influence" of technological mediation, it must be revealed– even, when necessary, "compromising user experience in the name of user welfare and autonomy." For example, this might be accomplished by placing at the forefront details about how data shared on social media is being used by the platform, and ideally providing users with some control.

DuckDuckGo is an example of a search engine that prioritizes user privacy. The platform has gained popularity with users wary of the tracking and targeting done by its competitors. A quick search, however, reveals that not all users appreciate the trade-offs; they want both a customized, personalized experience *and* privacy, which is not necessarily feasible. The important consideration, however, is that users should be empowered to *choose* for themselves how much privacy they desire and what trade-offs are acceptable, recognizing that different users will have different thresholds.

Increase public awareness of FoMO-centric design and dark patterns. Making it easier to publicly report or flag instances of dark patterns relating to privacy concerns and FoMO-centric designs would help bring to the forefront these deceptive practices. Raising awareness among the general public would enable more critical assessment by users with regards to their online practices and privacy decisions. Additionally, providing a forum for discussing privacy compromising decisions by companies can occasionally give rise to high-profile movements such as #DeleteFacebook following the Cambridge Analytica scandal [34].

We strongly caution, however, that the solution to this problem is not solely one of "educating the user." Considering how Phishtank [53] enables and encourages everyone to report instances of phishing sites, we envision a collaborative site where instances of FoMO-centric design can be reported and discussed. While these sites generally attract professionals or enthusiasts, it would provide a starting point for discussion and for the development of more general public awareness campaigns.

Legislate against the use of identified dark patterns. In April 2019, two US Senators tabled a bill [46, 80] intended to protect users against specific dark patterns. The bill signifies a positive first step but is far from a solution to the overall problem. It addresses very specific types of dark patterns ("to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data" [80]) and only prohibits designs that have a "purpose or substantial effect of cultivating compulsive usage" [80] for children under the age of 13. Furthermore, it only applies to online services with more than 100 million users. In our interpretation, only the most overt types of FoMO-centric designs would be covered, and only for very large organizations operating within the US. Clearly, additional work is needed to more broadly address this problem, both in terms of the types of practices covered and in international reach.

The US legislation comes in the wake of the EU General Data Protection Law (GDPR) in May 2018. The introduction of the GDPR enables combating privacy intrusive exploitation of users. However, the Norwegian Consumer Council audited major technology companies' settings and found that even after the regulation was

implemented, companies continued to use dark patterns to nudge users into sharing the maximum amount of data [25].

Past critiques of PbD have suggested that enforcing better privacy practices ignores economic needs [66], but Ontario Privacy Commissioner and PbD founder Ann Cavoukian counters by suggesting that protecting user privacy up front saves companies more than dealing with the aftermath of a data breach or privacy infraction [32]. The reality is likely less clear-cut than either position.

Educate designers and developers on dark patterns and the design patterns that combat them. Designers and developers must first be aware of what to look out for to design in a productive way. Education about such dark patterns should be included in computer science and software development curriculum. Avoiding such designs should be discussed as a matter of professional ethics, and ideally embedded in companies' Code of Conduct by which all employees should abide. In fact, if we look at the ACM Code of Ethics and Professional Conduct [1], a computing professional should, among others, "contribute to human well-being," "avoid harm," "be honest and trustworthy," and "respect privacy." We argue that dark patterns, including FoMO-centric designs, violate this code, and that individuals have a responsibility to actively avoid their use.

Combat monopolies. Maintaining, or increasing, diversity in users' options in terms of comparable service and quality is important to curbing the "opt in or go home" phenomenon. This is a concern with company mergers and acquisitions, where increasingly users are at the mercy of a smaller number of companies – and whatever limited privacy options (and dark patterns) they provide.

6.3 Research Agenda

Besides the above recommendations, we propose a research agenda addressing the issues for FoMO-centric design and privacy.

Understand FoMO and online privacy. We suggest conducting empirical user studies on the effect of specific design decisions on FoMO-related emotions experienced by users during privacy behaviours. Our literature review has established a deep, cyclical interconnection between FoMO-related behaviours and design features. A study with experimental and control groups and pre-session measures of user FoMO-levels, as well as in-session observed behaviours, should help differentiate between behaviours encouraged by FoMO-centric design versus by "plain FoMO" — that is, FoMO behaviours existing independent of design. Because FoMO is linked to deficits in basic psychological needs [58], we can assume it exists even in the absence of FoMO-centric design — however, our goal is to show that FoMO-centric design *aggravates*, *amplifies*, and *takes advantage of* FoMO. We further suggest a closer exploration of the link between FoMO and "System 1" [40] (automatic, unconscious) thinking as they relate to privacy behaviours. These would provide a stronger psychological basis for combating the effects of FoMO-centric design and for proposing alternatives.

Characteristics of social media are of particular interest, but FoMO-centric designs relating to other forms of media (e.g., IoT devices, wearables) are also worth understanding since they may also employ dark patterns relating to user privacy. FoMO-centric dark patterns are noteworthy across all types of media, and their effects may differ. There is also room for broader reflection on the ethical and moral implications of FoMO-centric design, the psychological and social constructs that have led us to this point, and what this means for society moving forward.

Specify FoMO-centric dark patterns. Now that we have put forth the motivations, behaviours, and general design features surrounding FoMO-centric design, specific FoMO-centric dark patterns should be defined, in keeping with design pattern conventions (i.e., following the template visible on the privacypatterns.org website [23]), and clearly identifying the ways in which FoMO-centric design presents itself. We argue that the definition of dark patterns should include explicit discussion of the psychological factors involved (a practice followed by Bösch et al. [14]), to provide context and broader understanding of the manipulation.

Propose corresponding privacy-preserving design patterns. Establishing appropriate privacy-preserving patterns is essential to moving forward and providing viable alternatives to those wishing to avoid FoMO-centric dark patterns. This task would initially require innovation and creativity to shift thinking beyond seeing users and their data as a commodity. The resulting patterns would need to be tested to ensure their robustness.

Improve the presentation of current privacy patterns and dark patterns. Many privacy patterns suffer from being presented in an overly abstract or fragmented way that does not make them clearly implementable. Improving the presentation of existing privacy patterns would increase the likelihood that they are implemented correctly, rather than resulting in "anti-patterns." We further believe more concrete, tangible examples of designs are needed. One effective approach could be providing side-by-side comparisons of two similar designs, one FoMO-centric and one not, to better illustrate how these principles apply to the real world.

Empower users against FoMO-centric design. Recognizing that there are many reasons why FoMO-centric designs exist, we cannot rely on the benevolence of service providers in eliminating all such patterns. In such cases, we should devise ways to empower users who wish to protect themselves. This may be through the use of third-party tools, or through awareness and education. For example, tools might facilitate participation in more privacy-preserving ways, might facilitate self-monitoring/reflection with respect to FoMO, or might enable retrospective data management.

6.4 Post-Workshop Reflection: Are Dark Patterns Always "Bad"?

During the NSPW session, discussion of the ethics of using dark patterns gave rise to the following question: are there some cases in which dark patterns *can* be used ethically? An example of this might be targeted dark pattern use by police to aid in their apprehension of a suspected criminal. Here, the dark pattern would be used for the "greater good" of maintaining societal order. Another example might be businesses using dark patterns for monetary gain or to keep up with competition. In this case, although the end goal is self-interested, it is not malicious towards the user — that is, the business may have no plans to turn the gathered data against the user. If the end goal is to succeed in honest work, be it business, law enforcement, or otherwise, is dark pattern use really so bad?

To answer this, let us return momentarily to the definition of a dark pattern, which at its core is a design intended to trick the user into doing something they would not otherwise do. "Entrapment" is the term used by law enforcement when a government agent designs a crime and induces (through means including persuasion) a person to commit that crime when the person would have been unlikely to do so otherwise [73]. Entrapment is, in many jurisdictions, a complete defense against criminal liability.

For clarity's sake, we can distinguish entrapment from arguably less problematic cases of agents going undercover to gain trust with the purpose of gathering incriminating evidence of a suspect. This latter case assumes that the evidence emerges without inducement and that the suspect acts as they otherwise would. Analogously, a design that allows for a less secure or privacy-preserving action but that does not manipulate or trick the user into taking it does not constitute a dark pattern.

When considering the ethical implications of dark patterns, we should be cautious of evaluating them solely on the merits of their end-goal. Rather, it is the loss of individual autonomy promoted by dark patterns that we should carefully consider when deciding their ethical status.

7 CONCLUSION

In this paper, we explored how the design of systems can manipulate users' online privacy behaviours and negatively affect their security. We focused on dark patterns stemming from the FoMO-related susceptibilities of users, causing them to reluctantly behave in less privacy-preserving ways than they would prefer. We found evidence of the existence of such design, as well as possible explanations for how it works, based on the psychological constructs involved. We believe that such systems prey on users' subconscious fear of missing out and manipulate individuals into giving up more of their privacy than is comfortable. We provided a list of preliminary recommendations and a research agenda. Our takeaway: When we make users choose between social benefits and privacy, we are not truly providing a choice. This ultimatum should be brought to the forefront so that everyone involved recognizes the manipulation and we can work towards more positive alternatives.

REFERENCES

[1] ACM Code 2018 Task Force. 2018. ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics.

[2] Alessandro Acquisti and Ralph Gross. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *Privacy Enhancing Technologies*, George Danezis and Philippe Golle (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 36–58.

[3] A. Acquisti and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security Privacy* 3, 1 (Jan 2005), 26–33. https://doi.org/10.1109/MSP.2005.22

[4] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of Economic Literature* 54, 2 (2016), 442–92.

[5] Christopher Alexander. 1977. *A pattern language: towns, buildings, construction*. Oxford university press.

[6] Dorit Alt. 2015. College students' academic motivation, media engagement and fear of missing out. *Computers in Human Behavior* 49 (2015), 111–119.

[7] Anita Balakrishnan, Sara Salinas, and Matt Hunter. 2018. Mark Zuckerberg has been talking about privacy for 15 years - here's almost everything he's said. *CNBC* (Mar 2018). https://www.cnbc.com/2018/03/21/facebook-ceo-mark-zuckerbergs-statements-on-privacy-2003-2018.html

[8] Marco Balduzzi, Christian Platzer, Thorsten Holz, Engin Kirda, Davide Balzarotti, and Christopher Kruegel. 2010. Abusing Social Networks for Automated User Profiling. In *Recent Advances in Intrusion Detection*, Somesh Jha, Robin Sommer, and Christian Kreibich (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 422–441.

[9] Susanne Barth and Menno D.T. de Jong. 2017. The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and Informatics* 34, 7 (2017), 1038 – 1058.

[10] Diane Bartz. 2019. U.S. senators introduce social media bill to ban 'dark patterns' tricks. https://www.reuters.com/article/us-usa-tech/us-senators-introduce-social-media-bill-to-ban-dark-patterns-tricks-idUSKCN1RL25Q.

[11] K. Bednar and S. Spiekermann. 2018. *Aware but not in control: A qualitative value analysis of the effects of new technologies*. IFIP Advances in Information and Communication Technology, Vol. 537. 202–218 pages. www.scopus.com

[12] David Blackwell, Carrie Leaman, Rose Tramposch, Ciera Osborne, and Miriam Liss. 2017. Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction. *Personality and Individual Differences* 116 (2017), 69–72.

[13] Rainer Böhme and Stefanie Pötzsch. 2012. Collective Exposure: Peer Effects in Voluntary Disclosure of Personal Data. In *Financial Cryptography and Data Security*, George Danezis (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–15.

[14] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237 – 254. https://content.sciendo.com/view/journals/popets/2016/4/article-p237.xml

[15] Nellie Bowles. 2018. Early Facebook and Google Employees Form Coalition to Fight What They Built. *The New York Times* (Feb 2018). https://nyti.ms/2GJoKHg

[16] Harry Brignull. [n.d.]. Dark Patterns Types of Dark Pattern. https://darkpatterns.org/types-of-dark-pattern. Accessed: 2019-17-01.

[17] Elija Cassidy. 2016. Social networking sites and participatory reluctance: A case study of Gaydar, user resistance and interface rejection. *New Media & Society* 18, 11 (2016), 2613–2628. https://doi.org/10.1177/1461444815590341

[18] Ann Cavoukian. 2011. Privacy by Design: The 7 Foundational Principles.

[19] Erika Chin, Adrienne Porter Felt, Kate Greenwood, and David Wagner. 2011. Analyzing Inter-application Communication in Android. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services (MobiSys '11)*. ACM, New York, NY, USA, 239–252. https://doi.org/10.1145/1999995.2000018

[20] Tsz Hang Chu and Tien Ee Dominic Yeo. 2018. Rethinking Social Media and Political Engagement: An Examination of the Disconnective Practices of Politically Active Youths in Hong Kong. In *Proceedings of the 9th International Conference on Social Media and Society*. ACM, 41–50.

[21] Russell B Clayton, Glenn Leshner, and Anthony Almond. 2015. The extended iSelf: The impact of iPhone separation on cognition, emotion, and physiology. *Journal of Computer-Mediated Communication* 20, 2 (2015), 119–135.

[22] Michael Colesky, Julio C. Caiza, José M. Del Álamo, Jaap-Henk Hoepman, and Yod-Samuel Martín. 2018. A System of Privacy Patterns for User Control. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing (SAC '18)*. ACM, New York, NY, USA, 1150–1156. https://doi.org/10.1145/3167132.3167257

[23] Michael Colesky, Jaap-Henk Hoepman, Christoph Bösch, Frank Kargl, Henning Kopp, Patrick Mosby, Daniel Le Metayer, Inria Olha Drozd, Jose M. del Alamo, Yod Samuel Martin, Julio C. Caiza, Mohit Gupta, and Nick Doty. [n.d.]. Privacy Patterns. https://privacypatterns.org/. Accessed: 2018-17-12.

[24] Tim Cook. 2019. You Deserve Privacy Online. Here's How You Could Actually Get It. *Time* (Jan 2019). http://time.com/collection/davos-2019/5502591/tim-cook-data-privacy/

[25] Norwegian Consumer Council. 2018. Deceived By Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. (2018). https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

[26] Edward Deci and Richard M Ryan. 1985. *Intrinsic motivation and self-determination in human behavior*. Springer Science & Business Media.

[27] Nick Doty and Mohit Gupta. 2013. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. (2013).

[28] Ramona-Riin Dremljuga. 2018. The process and affordances of platform-specific social media disconnection. *Studies of Transition States and Societies* 10, 2 (2018).

[29] Stefanie Duguay. 2017. *Identity modulation in networked publics: Queer women's participation and representation on Tinder, Instagram, and Vine*. Ph.D. Dissertation. Queensland University of Technology.

[30] Nicole B Ellison, Charles Steinfield, and Cliff Lampe. 2007. The benefits of Facebook "friends" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication* 12, 4 (2007), 1143–1168.

[31] Facebook. [n.d.]. What names are allowed on Facebook? https://www.facebook.com/help/112146705538576. Accessed: 2019-26-01.

[32] Liz Farmer. 2014. Canada's Global Player in the Privacy Debate. *GOVERNING* (May 2014). https://www.governing.com/topics/public-justice-safety/gov-global-player-in-privacy-debate.html

[33] BJ Fogg. 2002. Persuasive Technology: Using Computers to Change What We Think and Do (Interactive Technologies). *Ubiquity* 5 (2002).

[34] Ben Gilbert. 2018. The #DeleteFacebook movement has reached a fever pitch, as former Facebook insiders turn on the company. *Business Insider* (March 2018).

https://www.businessinsider.com/deletefacebook-facebook-movement-2018-3
[35] Saikat Guha, Kevin Tang, and Paul Francis. 2008. NOYB: Privacy in Online Social Networks. In *Proceedings of the First Workshop on Online Social Networks (WOSN '08)*. ACM, New York, NY, USA, 49–54. https://doi.org/10.1145/1397735.1397747
[36] Tristan Harris. [n.d.]. Center for Humane Technology. http://humanetech.com/. Accessed: 2019-19-01.
[37] Todd Haselton. 2018. How Google is fighting smartphone addiction with its next Android update. *CNBC* (May 2018). https://www.cnbc.com/2018/05/09/google-fighting-smartphone-addiction-with-android-p-digital-wellness.html
[38] Tom N. Jagatic, Nathaniel A. Johnson, Markus Jakobsson, Markus Jakobsson, and Filippo Menczer. 2007. Social Phishing. *Commun. ACM* 50, 10 (Oct. 2007), 94–100. https://doi.org/10.1145/1290958.1290968
[39] Kylie Jarrett. 2015. "Let's Express Our Friendship by Sending Each Other Funny Links instead of Actually Talking": Gifts, Commodities, and Social Reproduction in Facebook. *Networked affect* (2015), 203–219.
[40] Daniel Kahneman. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux.
[41] Rachel Kraus. 2018. 'Time Well Spent' features are the Marlboro Lights of the tech industry. *Mashable* (August 2018). https://in.mashable.com/tech/319/time-well-spent-features-are-the-marlboro-lights-of-the-tech-industry Accessed: 2019-04-07.
[42] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.
[43] M. Laverdiere, A. Mourad, A. Hanna, and M. Debbabi. 2006. Security Design Patterns: Survey and Evaluation. In *2006 Canadian Conference on Electrical and Computer Engineering*. 1605–1608. https://doi.org/10.1109/CCECE.2006.277727
[44] Dahui Li, Glenn J. Browne, and Patrick Y. K. Chau. 2006. An Empirical Investigation of Web Site Use Using a Commitment-Based Model. *Decision Sciences* 37, 3 (2006), 427–444. https://doi.org/10.1111/j.1540-5414.2006.00133.x
[45] Arunesh Mathur, Gunes Acar, Michael Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11KShopping Websites. (2019). https://webtransparency.cs.princeton.edu/dark-patterns/assets/dark-patterns-v2.pdf
[46] Natasha Mathur. 2019. U.S. senators introduce a bipartisan bill that bans social media platforms from using 'dark patterns' to trick its users. https://hub.packtpub.com/u-s-senators-introduce-a-bipartisan-bill-that-bans-social-media-from-using-dark-patterns-to-trick-its-users/.
[47] Samantha Murphy. 2013. Report: 56% of Social Media Users Suffer From FOMO. *Mashable* (Jul 2013). https://mashable.com/2013/07/09/fear-of-missing-out/#83r7t4gHriq4
[48] Cal Newport. 2019. *Digital Minimalism: Choosing a Focused Life in a Noisy World*. Penguin.
[49] Casey Newton. 2018. Google's new focus on well-being started five years ago with this presentation. *The Verge* (May 2018). https://www.theverge.com/2018/5/10/17333574/google-android-p-update-tristan-harris-design-ethics
[50] Patricia A Norberg, Daniel R Horne, and David A Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126.
[51] Khaldoon 'Khal' Nusair, Anil Bilgihan, Fevzi Okumus, and Cihan Cobanoglu. 2013. Generation Y travelers' commitment to online social network websites. *Tourism Management* 35 (2013), 13 – 22. https://doi.org/10.1016/j.tourman.2012.05.005
[52] Open Security Architecture (OSA). 2019. https://www.opensecurityarchitecture.org/cms/.
[53] OpenDNS. 2019. PhishTank: out of the net, into the tank. https://www.phishtank.com/.
[54] Oxford Dictionary. [n.d.]. FOMO. https://en.oxforddictionaries.com/definition/fomo. Accessed: 2018-11-12.
[55] Susanna Paasonen. 2018. Affect, data, manipulation and price in social media. *Distinktion: Journal of Social Theory* 19, 2 (2018), 214–229. https://doi.org/10.1080/1600910X.2018.1475289
[56] Zizi Papacharissi and Paige L. Gibson. 2011. *Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites*. Springer Berlin Heidelberg, Berlin, Heidelberg, 75–89. https://doi.org/10.1007/978-3-642-21521-6_7
[57] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's Creepy, But It Doesn't Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 5240–5251. https://doi.org/10.1145/2858036.2858381
[58] Andrew K. Przybylski, Kou Murayama, Cody R. DeHaan, and Valerie Gladwell. 2013. Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior* 29, 4 (2013), 1841 – 1848. https://doi.org/10.1016/j.chb.2013.02.014
[59] Katelyn Ritchie. 2018. *To Post, or Not to Post? Exploring Adjunct Faculty and Staff Social Media Use Among a Converged Mixed Audience*. Ph.D. Dissertation. University of Cincinnati.
[60] Sasha Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. 2006. Privacy Patterns for Online Interactions. In *Proceedings of the 2006 Conference on Pattern Languages of Programs (PLoP '06)*. ACM, New York, NY, USA, Article 12, 9 pages. https://doi.org/10.1145/1415472.1415486
[61] Yoel Roth. 2016. Gay data. (2016).
[62] Hagit Sasson and Gustavo Mesch. 2014. Parental mediation, peer norms and risky online behavior among adolescents. *Computers in Human Behavior* 33 (2014), 32 – 38. https://doi.org/10.1016/j.chb.2013.12.025
[63] John Schwartz. 2000. 'Opting-in': A Privacy Paradox. *Washington Post* (2000).
[64] Oscar Schwartz. 2019. Why beating your phone addiction may come at a cost. *The Guardian* (March 2019). https://www.theguardian.com/technology/2019/mar/13/digital-wellness-phone-addiction-tech
[65] Johanneke Siljee. 2015. Privacy Transparency Patterns. In *Proceedings of the 20th European Conference on Pattern Languages of Programs (EuroPLoP '15)*. ACM, New York, NY, USA, Article 52, 11 pages. https://doi.org/10.1145/2855321.2855374
[66] Sarah Spiekermann. 2012. The Challenges of Privacy by Design. *Commun. ACM* 55, 7 (July 2012), 38–40. https://doi.org/10.1145/2209249.2209263
[67] Polly Sprenger. 1999. Sun on Privacy: 'Get Over It'. *Wired* (Jan 1999). https://www.wired.com/1999/01/sun-on-privacy-get-over-it/
[68] Katherine Strater and Heather Richter Lipford. 2008. Strategies and Struggles with Privacy in an Online Social Networking Community. In *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1 (BCS-HCI '08)*. British Computer Society, Swinton, UK, UK, 111–119. http://dl.acm.org/citation.cfm?id=1531514.1531530
[69] Daniel Susser. 2019. Invisible Influence: Artificial Intelligence and the Ethics of Adaptive Choice Architectures. (2019).
[70] Daniel Susser, Beate Roessler, and Helen Nissenbaum. 2018. Online Manipulation: Hidden Influences in a Digital World. (December 2018). https://ssrn.com/abstract=3306006orhttp://dx.doi.org/10.2139/ssrn.3306006
[71] Monika Taddicken. 2014. The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication* 19, 2 (2014), 248–273.
[72] Karen P. Tang, Jialiu Lin, Jason I. Hong, Daniel P. Siewiorek, and Norman Sadeh. 2010. Rethinking Location Sharing: Exploring the Implications of Social-driven vs. Purpose-driven Location Sharing. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing (UbiComp '10)*. ACM, New York, NY, USA, 85–94. https://doi.org/10.1145/1864349.1864363
[73] The United States Department of Justice. [n.d.]. Entrapment—Elements. https://www.justice.gov/jm/criminal-resource-manual-645-entrapment-elements.
[74] Zeynep Tufekci. 2008. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society* 28, 1 (2008), 20–36. https://doi.org/10.1177/0270467607311484 arXiv:https://doi.org/10.1177/0270467607311484
[75] Sonja Utz and Nicole C Krämer. 2009. The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3, 2 (2009).
[76] Sebastián Valenzuela, Namsu Park, and Kerk F Kee. 2009. Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation. *Journal of computer-mediated communication* 14, 4 (2009), 875–901.
[77] Emily van der Nagel. 2018. 'Networks that work too well': intervening in algorithmic connections. *Media International Australia* 168, 1 (2018), 81–92.
[78] Jeroen van Rest, Daniel Boonstra, Maarten Everts, Martin van Rijn, and Ron van Paassen. 2014. Designing Privacy-by-Design. In *Privacy Technologies and Policy*, Bart Preneel and Demosthenes Ikonomou (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 55–72.
[79] Xiao Wang and Steven R. McClung. 2011. Toward a detailed understanding of illegal digital downloading intentions: An extended theory of planned behavior approach. *New Media & Society* 13, 4 (2011), 663–677. https://doi.org/10.1177/1461444810378225 arXiv:https://doi.org/10.1177/1461444810378225
[80] Mark R. Warner and Deb Fischer. 2019. Deceptive Experiences To Online Users Reduction (DETOUR) Act. https://www.scribd.com/document/405606873/Detour-Act-Final.
[81] Lance Whitney. 2018. How to Use Screentime in Apple iOS 12. https://www.pcmag.com/feature/363837/how-to-use-screen-time-in-apple-s-ios-12/6. Accessed: 2019-26-01.
[82] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. 2018. Contextualizing Privacy Decisions for Better Prediction (and Protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 268, 13 pages. https://doi.org/10.1145/3173574.3173842
[83] Claire A Wolniewicz, Mojisola F Tiamiyu, Justin W Weeks, and Jon D Elhai. 2018. Problematic smartphone use and relations with negative affect, fear of missing out, and fear of negative and positive evaluation. *Psychiatry research* 262 (2018), 618–623.
[84] Nobukazu Yoshioka, Hironori Washizaki, and Katsuhisa Maruyama. 2008. A survey on security patterns. *Progress in informatics* 5, 5 (2008), 35–47.
[85] Alyson Leigh Young and Anabel Quan-Haase. 2013. Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society* 16, 4 (2013), 479–500.