Uses Unaddressed:

How Social Technologies Tacitly Allow Gender-Based Violence

Honors Thesis

Brooke Marston

Advisor: Nora Draper

University of New Hampshire

Department of Communication

May 2021

Abstract

Growing technological capabilities have enhanced and intensified the potential for surveillance in many areas of life. Particularly, the placement of advanced technology in the hands of everyday people has produced ample opportunities for interpersonal monitoring. This growing capacity to surveil others we know without sophisticated techniques has concerning implications for acts of gender-based violence and intimate partner violence, which often hinge on surveillance, isolation, and control. Often, technology is used to the advantage of abusers in achieving such ends, and the wealth of personal information that is often available online leaves users vulnerable to acts of gender-based violence such as cyberstalking. In the following analysis, I systematically and forensically interrogate the seemingly mundane apps Find My and Venmo to investigate how these and other apps could be used to aid in such behaviors, paying special attention to privacy settings and account security features. I find that these apps generally overlook special risks that are often present in gender-based violence and intimate partner violence, especially hindering users' efforts towards independence when their account may be compromised by an abuser. Additionally, limited privacy settings on social apps like Venmo leave an abundance of personal information publicly accessible with few options to improve security while continuing to use the service. In light of these findings, I make recommendations to help alleviate gender-based privacy and safety concerns, including more equal gender representation in technological development, and more advanced security features such as fingerprint identification or facial recognition.

Keywords: gender-based violence, intimate partner violence, privacy, surveillance, gender and technology

TABLE OF CONTENTS

I. Introduction

Querying "*how to spy on my girlfriend*" generates about 75 million web search results on Google. Among these entries, countless articles promise solutions to track the activity of an intimate partner, from call and text history all the way to social media sites like Facebook. The most common suggestion is the installation of malware apps on the suspected partner's devices, which can either be planted as a phishing link in an innocent-looking email, or discreetly installed on the device while its owner isn't around. Once installed, these apps run in the background while the device can continue to be used as normal— all while reporting a host of private information remotely to the attacker, including call and text history, keystrokes, web browsing history, social media activity, geolocation, and even audio and/or video recording.

The use of technology in order to facilitate surveillance, isolation, and control of a romantic partner is a modern extension of traditionally recognized abusive behaviors known as intimate partner violence (CDC, 2020). Intimate partner violence is additionally closely related to the concept of gender-based violence, which constitutes violent acts carried out on the basis of a person's perceived sex or gender identity (Ott, 2017). While gender-based violence affects people of all genders, women are statistically most likely to encounter such threats in everyday life and in intimate relationships. The World Health Organization (2021) have found that 1 in 3 women have experienced physical or sexual abuse in their lifetimes, which does not factor in other types of gender-based violence and intimate partner violence such as financial and emotional abuse. Additionally, due to differing legal definitions of various acts of gender-based violence between different nations, as well as the social stigma (and often physical danger) surrounding reporting, the actual number of women who have experienced some form of

gender-based violence is much more difficult to ascertain and likely higher than current figures suggest.

While the malware apps described above are generally only accessible off-market due to their dubious purposes, mainstream app stores are otherwise populated by free or low-cost software with a variety of uses, from entertainment to finance management to health monitoring. Alongside this rapid technological growth has emerged a modern crisis in privacy. While we've come to rely on apps, websites, and social media for our day-to-day lives, these platforms have surreptitiously collected and compiled a wealth of our personal information, primarily for the purposes of selling to advertisers and marketing agencies. While the data collection capabilities of giant corporations have come into greater focus in light of events such as the Facebook-Cambridge Analytica data scandal in 2018, the interpersonal risks posed by such highly capable technologies have only recently been the focus of scholarly and public attention. Even the most mundane apps collect personal information, and the potential for exploitation of access to that information in order to surveil, isolate, and control others is a formidable threat further complicating the struggle to quash gender-based violence and intimate partner violence.

II. Literature Review

IIa. Intimate Surveillance, Tracking, and Apps

Karen Levy (2015) uses the term *intimate surveillance* to encapsulate acts of data-gathering in the realm of intimate relationships and behaviors, including interpersonal relationship tracking, health-related tracking of one's own ovulation and fertility for family planning, and individual or interpersonal sexual wellness tracking. Intimate surveillance has emerged in recent years as an interpersonal phenomenon that has exponentially increased in part

due to the proliferation of personal technologies like the smartphone and social media. Levy argues that today it is more common and socially expected for people to perform acts of intimate surveillance upon themselves and those they know, rather than be subjected to institutional surveillance-- that which is conducted by outside bodies such as researchers or governments. Much of this surveillance is conducted interpersonally through the use of software applications (apps), which are specialized to "solve particular, often singular, user needs" (Light et al., 2016). While apps are commonly associated with the smartphone, they are not exclusive to mobile technologies, and are often accessible through other means such as on a personal computer. However, smartphones are closely linked to the concept of the app because of the way these devices uniquely rely on and emphasize apps in order to structure and segment user activity.

The ever-increasing volume of both apps and users has revealed a trove of previously unknown data and personal information that can be collected, stored, and shared. Some of the world's most used apps, such as social media giant Facebook, rely heavily on the sharing of personal information to create the user's experience— allowing the user to connect with other people from both on- and offline based on information they choose to share, such as "likes", hobbies, and more personal information such as where they work or the city they reside in— while this information in turn drives Facebook's profit model. Mobile technologies in particular have brought about many new forms of surveillance that are somewhat unique to the medium. One such example is the introduction of user-friendly location services that are integrated into apps to help a user get directions, find businesses or other establishments close to them, or even locate other people in close geographic proximity (Spiekermann, 2004).

Health-related tracking has also risen in prominence, in part due to location services as well as the development of enhanced wearable technologies such as the Fitbit and Apple Watch.

The capability to track health characteristics has greatly increased through the invention of such devices, and this is the foundation of the *quantified self* movement that has become increasingly relevant in the mid to late 2010s (Lupton, 2016). At the heart of this movement is the notion that the ability to collect and analyze as much data about the self as possible-- between our bodies, minds, and movements-- is integral to self-improvement efforts (Wolf, 2009). Increasingly, data related to intimate relationships and behaviors has been incorporated into this suite of data that users and developers seek to track, quantify, and analyze. Lupton (2015) makes note of numerous "sex tracker" apps into which data about sexual activity can be either manually inputted or recorded using smartphone features such as the microphone. The purported benefit of such apps to the user is to generate metrics of sexual performance, and ultimately, to encourage self-improvement and enhance sexual relationships.

The millions of apps now available through official channels such as the Apple App Store and Google Play Store, spanning a wide variety of categories such as health, finance, education and entertainment, competition for users' loyalty and attention has led to the integration of social conditioning practices into many apps' user interfaces to increase desired forms of participation. One widely observable technique to encourage information-sharing is the practice of gamification, which incorporates aspects of gameplay into the app's requests in order to incentivize user participation (Blohm & Leimeister, 2013). For example, an app may award badges, points, or other symbols of achievement to users who take advantage of its features in an intended way. These achievements may unlock further access or benefits within the app, and may also be sharable among a user's social network. Through the addition of incentives, specific uses of an app are encouraged, even though the app may have uses beyond the specific ones that are encouraged (Davis & Chouinard, 2017). Gamification is only one strategy that apps employ to

create *seduction* to smartphones-- and ultimately, to surveillance. Troullinou (2017) identifies gamification along with notions of security, immediacy, and novelty as constructing a seductive view of surveillance which users are incentivized and attracted towards participating in.

IIb. Normalizing Surveillance

Both heightened achievements in technological systems themselves, along with new and innovative techniques to incentivize user engagement, have contributed to what Levy refers to as a normalization of surveillance, and particularly of intimate surveillance (2015). Information that may have once been kept private is now able to be easily shared, both with our own apps as well as the people we connect with within them. Thus, while there is not necessarily a requirement to share intimate information, it may come to be expected from ourselves or others around us in certain social contexts. For example, many consider it a norm to look for an acquaintance or date on Facebook or Google before meeting-- not only to ensure safety, but also often out of genuine curiosity. A certain amount of personal sharing is also advantageous in the career world due to the prominence of networking sites such as LinkedIn. However, Levy & Schneier (2020) contend that this trend of normalization in gathering such information leaves technological surveillance practices vulnerable to exploitation, writing that "well-intentioned intimate monitoring can create a slippery slope of acceptability, inuring users to accepting surveillance as a mode of social control in other contexts" (p. 2). For example, the customary and often personal information-sharing that takes place on social media sites like Facebook (and even moreso on the intimate tracking apps previously described) can lead to the expectation of extensive private sharing in intimate relationships, and any desire to retain individual privacy by withholding certain information may be seen as dishonest or suspicious. While we may partake in

information-sharing innocuously to learn more about ourselves and improve relationships with others, it is all the while possible that bad actors may take advantage of the sheer ubiquitousness of such practices in order to monitor and control others.

The proliferation of interpersonal surveillance activities poses other challenges to our conception of privacy, with some of the largest issues revolving around the idea of consent. As Levy (2015) and others have pointed out, some acts of intimate surveilling such as sex tracking can be conducted by an individual without others' (such as a partner's) knowledge or consent. This fact is clearly problematic, with the removal of informed consent in this particular sitution being comparable to more broadly recognized acts of sexual violence, without the expected legal ramifications. With social interaction increasingly aided by the internet and social media, personal data is often stored online by the choice of the user. While social sharing platforms act as repositories for our memories and experiences, they also can present our information to others without our express consent or even our knowledge, due to limited privacy settings that favor public sharing. This highly accessible wealth of data can create danger in situations of gender-based violence and intimate partner violence, by allowing an abuser or stalker to identify and track an individual's real-world connections such as friends, family, and employers, as well as specific geolocation data showing where they currently are or have been recently. By the time a bad actor has accessed this data, it is too late to revoke that access because they may take screenshots, reach out to friends or acquaintances of the victim to get closer to them, or have information about them such as location that allows them to carry out a violent act (Freed et al., 2018).

IIc. Data Violence and the Building of Gender Bias

Women have historically been underrepresented in the technology sector, making up less than 30 percent of the tech workforce in the year 2020, leading to a higher proportion of men than women designing and approving the apps and systems the general public interacts with on a daily basis (CNBC, 2020). As Faulkner (2001) puts it, women are more likely to be "on the receiving end" of novel technologies, rather than in the position of creating them (p. 80). In regards to intimate surveillance, Levy (2018) purports that women are more often constructed as monitored subjects than men, who are more likely to be placed in control of data collection either as users or developers. For example, many of the sex tracking apps analyzed by both Levy (2018) and Lupton (2015) are clearly organized around masculine and heteronormative ideals, using metrics such as duration of sex and number of partners to generate analyses of performance. As more mainstream examples of how these ideals pervade even mundane apps, some may recall how Facebook began as a website for Harvard students to rate female students based on attractiveness, or how YouTube's founders were inspired to create a video-sharing platform after they were unable to find videos of Janet Jackson's wardrobe malfunction, which exposed her bare breast, at a Super Bowl Halftime Show performance in 2004. Historically, women on the internet have been constructed more as objects to view than as fellow users. Their relationship to technology has long been questioned and doubted, and they often are excluded from digital culture movements such as fan cultures (Scott, 2019).

The lack of equal gender representation in app development can have influential social and political consequences. Hoffmann (2018) uses the term *data violence* to describe the idea that the features that are or are not included in a service or technology can "implicitly and explicitly lead to harmful or even fatal outcomes" (para. 15). The "biased" technology that may

come about as a result of underrepresentation is not always based on an explicit desire to discriminate, but rather, an implicit ignorance as a result of social privilege leading to the exclusion or underrepresentation of diverse perspectives. As already noted, the growing realm of sex tracking apps seem to be almost exclusively crafted around masculine and heteronormative perspectives, norms, and ideals regarding sex, and this approach has lead to apps that are unwelcoming of and possibly even incompatible with users who are women or members of the LGBTQ+ community. In the case of apps with broader uses, such as social media platforms or web search engines, gender bias may appear not only as explicit displays of sexism which reinforce cultural bias and discrimination, but more subtly in a lack of safeguards against sexist behavior.

IId. The Growing Role of Technology in Abusive Situations

Technology often intersects with and magnifies other abusive behaviors that are present in intimate partner violence situations, by potentially aiding an abuser in surveilling their victim in an effort to control activity. As already described, social media platforms host a wealth of information about people that is generally easily accessible, especially by people who know each other offline or have mutual friends. This can prove dangerous in situations of intimate partner violence, as abusers can take advantage of this knowledge in order to surveil and isolate survivors. The shift of many spheres of daily life, such as communication, career, and entertainment, to online platforms presents greater opportunities for abusers to exert control in places where this once would have been more difficult. Particularly in situations where abusers and their partners cohabitate, abusers may be able to gain even more access into personal accounts by guessing passwords or coercing their partners to reveal them (Freed et al., 2018).

As the data collection and information sharing capabilities of our personal devices were just beginning to enter public focus, Mason and Magnet (2012) argued that although surveillance, privacy and security are of high concern to users, the implications of such technologies for women in abusive situations were largely unnoticed by the public. As they note, strategies of consumer surveillance such as screen capturing and tracking location using GPS mirror strategies that abusers have used to track their intimate partners. Surveillance is purposeful as a form of exerting control at both institutional and interpersonal levels, and new technologies have aided and simplified the act of surveillance for the typical user. While "high-tech" strategies such as installing malware or hiding GPS trackers have been utilized by abusers, these often can be complicated, expensive, and risky. Now, as Mason and Magnet (2012) purport, simple tracking systems integrated into common apps like Facebook and Twitter are highly accessible and convenient in monitoring those known to a user. As one example, Facebook profiles often host a suite of information that may be dangerous in the hands of an abuser, such as physical locations visited, names and pictures of friends, and contact information such as phone numbers, email, and workplace information. If we consider the potential roles of Facebook and other social media platforms as tools for stalking and harassment, it becomes clear that much of the technology used to engage in these violent acts is widespread and easily accessible, and already in use by much of the population.

Safeguards against abusive behavior on social media platforms fall even shorter when an abuser has physical access to their partner. While password protection and other security efforts purport to ensure only the owner of a private profile has access to it, such efforts are ineffective when a victim lives with their abuser, who can coerce them to reveal passwords and may even have legal ownership of their devices. Freed et al. (2018) argue that conventional security threat

models in technology "do not anticipate attackers who possess such intimate knowledge" of their targets, instead building account protection mechanisms more likely to fend off unknown hackers and strangers (p. 1). However, the reality is that often privacy attacks are carried out by interacting with standard user interfaces, rather than through more technologically sophisticated techniques. Freed et al. (2018) refer to these attackers as *UI-bound adversaries*, meaning that they conduct intimate partner violence or other forms of gender-based violence within the constraints of the apps' intended uses. For example, in the above scenario, an abuser may gain access to their partner's various social, financial, and professional accounts by coercing them into revealing account information. With this information, the abuser can easily log into these accounts as if they were the owner, gaining access to private information ranging from messages and emails to bank or credit card information. After compromising the account, the abuser is able to wield a high level of control and can change passwords and other information, revoke the original owner's access, or delete the accounts entirely. For the original owner, regaining control may be difficult and even unsafe, as the attacker may be alerted to password or security setting changes, and this can lead to retaliation and even violence (Freed et al., 2018). Notions of account security are further clouded by the existence of financial and legal arrangements such as family phone service plans, where multiple devices are bundled under one account and generally managed by one *owner* (Draper, 2014). Any group willing to enter into a financial agreement can generally sign up for such plans, regardless of their relationship. However, the family plan imposes a more traditional power imbalance in favor of the designated "owner" of the plan, conferring additional service features such as geolocation tracking of other devices on the plan, ability to monitor and limit usage of features such as calling or texting, and ability to restrict and filter the types of content viewed on the device (Draper, 2014). These features are generally

viewed as more appropriate within the context of parents or guardians and their children, but when it is two adults who share such a plan, the features can be problematically exploited by the owner to facilitate surveillance and control.

IIe. Financial Information as Social and Personal

In addition to integrating all kinds of identifying and personal data into social interfaces, some apps have even shifted towards personalizing and socializing our most mundane data. The social payment app Venmo, owned by the online payment company PayPal, uniquely attempts to do this by adding a social component to interpersonal payments. Venmo looks much like a minimalist version of a traditional social media app, with all of the basic components-- a profile complete with name and picture, a friends list, and an activity feed where users can leave likes and comments on their friends' posts. However, the only type of activities recorded in this feed are financial transactions between users, annotated with a personalized caption and with the actual amount of the transaction hidden from public view. With its resemblance to other social media platforms, Swartz (2020) purports that Venmo is a kind of natural extension of our entrustment of social media platforms to retain and mediate our memories. Just as Facebook holds onto our social memories in the forms of photos, wall posts, and private messages, Venmo serves as a repository for our transactional memories. At the same time, Venmo retains a social component to these financial transactions, through the additional affordances of a friends list, liking and commenting features, and captions for each transaction.

In situations of intimate partner violence, financial power is often exerted as a means of maintaining an abuser's isolation and control. As mentioned previously by Freed et al. (2018), abusers often have financial power over survivors that makes it very difficult for them to hold on

to their independence or to regain it when attempting to leave an abusive situation. Technology is an extension of such wealth, as cell phones and computers remain luxury goods despite their increasing necessity in all spheres of life. Particularly in situations where an abuser and their partner live together, the abuser may pay the phone bill or even technically "own" the device through arrangements such as family plans. This fact is highly problematic when considering how an abuser might be able to make legal claim over their partner's phone or other device, even if their intentions are to use that device to steal their information or leverage it against them as an additional layer of control (Freed et al., 2018).

IIf. "Dual-Use" as Abuse

Davis and Chouinard (2017) outline a mechanisms framework illustrating how an artifact's affordances vary by degree. Specifically, they purport that artifacts "request, demand, allow, encourage, discourage, and refuse" (p. 241). This framework can be applied to apps in the sense that certain courses of action within an app can be emphasized, while other courses of action may be hidden or made impossible, due to the app's features such as design and layout. When an action is not refused, but at the same time not specifically encouraged or even discouraged, it is *allowed* (Davis and Chouinard, 2017). These distinctions are important because they highlight how an app may *allow* itself to be used for particular purposes, even if those purposes are outside its intended mode of use.

Within this vein of reasoning, Chatterjee et al. (2018) use the term *dual-use apps* to describe "a class of tools that have some advertised use unrelated to intimate partner tracking . . . but that are easily and effectively repurposed for intimate partner surveillance, often with the tacit support of app vendors" (p. 441). This means that while an app may have an advertised

purpose that is innocuous, such as helping to locate a lost phone or monitoring a child's internet activity for safety, that app may at the same time *allow* itself to be used as a means of surveilling an intimate partner by lacking any safeguards against such use (Draper, 2019; Hasinoff, 2017).

While partner spying and surveillance apps are not difficult to come by, dual-use apps are arguably more insidious. They are easier to justify having, given their more innocuous intended uses such as preserving safety or preventing theft. Additionally, given these advertised uses, they are more likely to not be flagged by app stores' vetting procedures for content and safety, despite their potential uses for harm. Levy (2018) argues that developers bear ethical responsibility for their apps' privacy consequences despite intentions, saying that "the very design of the technology makes determinations about the scope of intimate privacy" (p. 23). Now that these capabilities are so widespread and accessible, the lack of safeguards against privacy threats from those close to us are becoming more and more difficult to justify.

III. Methodology

The research for this paper draws primarily upon affordance theory, a concept originally advanced by Donald A. Norman (1999). Norman uses the term *affordance* to refer to a technological artifact's properties, both perceived and actual. Norman additionally purports that an artifact's affordances "provide strong clues to the operations" of that artifact— a user understands in what ways the artifact can be used simply by looking at it, without any further instruction being necessary (p. 9). This same logic can be extended to digital technologies, and by examining the affordances of a digital technology, some insight can be gained about its intended uses.

Davis and Chouinard (2017) expand upon affordance theory by proposing a system of interrelated mechanisms through which artifacts afford or don't afford to various degrees. In the context of digital technologies This framework relies on the idea that the affordances of a technology vary by degree, offering insights into what sorts of uses are explicitly intended, tacitly permitted, or outright prevented. Specifically, they propose that artifacts "request, demand, allow, encourage, discourage, and refuse" (2017, p. 2). This analysis will incorporate the mechanisms framework by interrogating the range of potential uses within each app, and specifically focusing on such actions that may not be intended but are nonetheless tacitly allowed.

In the following analysis, I consider both the device tracking app Find My and the payment app Venmo. These apps are both widely used; Find My is pre-installed by default on every Apple product, making it highly accessible to the owners of some 1.65 billion active Apple devices worldwide, while Venmo reported having over 60 million active users in 2019 (Welch, 2021; de Best, 2021). They also both have seemingly innocuous and utilitarian purposes— Find My can be used to locate Apple devices that are synced with a user's account using geolocation technology, or to locate others known to the user who have consented to sharing location data using their own Apple devices, while Venmo is primarily used for sending instant payments which can then be publicly viewed in either a global feed or by friends of the user.

Both apps are to be investigated using the walkthrough method as outlined by Light, Burgess, and Duguay (2016). The walkthrough method is an approach to app analysis in which the researcher, having discerned the app's expected environment of use, "deploys a walkthrough technique to systematically and forensically step through the various stages of app registration and entry, everyday use and discontinuation of use" (p. 881). This method involves direct

interaction with the app's user interface to determine intended uses, to investigate how options and uses are portrayed, and to understand cultural meanings that may be embedded in choices regarding the app's design and development.

As somewhat mundane apps without the primary purpose of dating, hooking up, or other general social networking, both Find My and Venmo risk being overlooked when considering how a perpetrator of harassment, intimate partner violence, or other forms of gender based violence may use app features to achieve outcomes not necessarily intended by the app's creators. I apply the walkthrough method in analyzing these apps in order to build a foundation of the apps' intended uses, recalling Davis and Chouinard's (2017) mechanisms framework of affordance theory to describe these uses in further detail and to distinguish possible uses that seem to fall outside of the apps' intended purposes, yet are allowed by their interfaces.

Lastly, I draw upon available research in the role of technology in surveillance and gender-based violence to make sense of the data gathered, making use of critical technocultural discourse analysis (CTDA), an approach which applies critical theory to analyses of technological development and use (Brock, 2016). Although intimate partner violence and other forms of abusive behavior may affect any individual regardless of their gender, women as a group are disproportionately impacted by such behaviors. Thus, a critical lens is necessary for any link between technological development and gendered violence to be considered. Using CTDA and the information gathered using the walkthrough method, I will put forth potential implications of my apps of focus as well as other mundane technologies on current and future patterns of both surveillance and gender-based violence, and discuss future considerations that could be made in technological development generally to help prevent unintended misuse of technologies and safeguard users from experiencing gender-based violence.

IV. Analysis & Discussion

IVa. Venmo

Venmo upends the supposed banality of splitting bills and settling up by thrusting these transactions into the social world, through the inclusion of social media elements such as likes and comments, a friends list, and an activity feed. Although available to any user with a bank account over the age of 13, the app appears to implicitly target young adults, who are prominently featured in images on Venmo's homepage. The most basic version of Venmo is free to use for sending person-to-person payments not for goods or services, but users may take advantage of a "freemium" model where they can pay to have money received moved to their bank account instantly, and a business feature for merchants in which Venmo charges a fee per transaction has been recently introduced.

Since Venmo relies on financial transactions, it is required by law to collect a host of personal information in order to identify users and mitigate risk. To create a basic account, users must provide their first and last name, email, and phone number. However, to send payments or transfer money out of Venmo, a bank account or card must be connected, and this in turn may trigger requests for further information for identity verification purposes such as home address or social security number. For safety purposes, Venmo requests users input their real name, and add a photo of themselves so that others can verify with whom they are exchanging money.

Venmo's privacy settings are deliberately limited in nature. Activity on Venmo, including transactions as well as likes or comments on those transactions, is made public according to the app's default settings (See Fig. 1). The app's main activity feed, which it boasts as a novel social component to its mundane purpose, contains three sections: A personal feed where users can view their own activity, a friends feed where any activity from the user's approved friends is

listed, and a global feed, where transactions from any of the millions of Venmo users who have their activity set to public can appear. From the activity feeds, the user can tap on any name to be taken to that person's profile, where their name, username, profile photo, friends list, and activity (depending on privacy settings) will appear (see Fig. 2).

Additionally, a Venmo profile cannot be made fully private, meaning there are no settings to prevent a profile from showing up in public search results or on other people's friends lists, outside of the option to block specific users. Other information on a user's profile, including their full name, profile photo, username, and friends list, cannot be restricted in any way—leaving a wealth of information publicly accessible that a user may want to remain private. In this way, it can be argued that Venmo lends itself to potential dual-use for gender-based violence, particularly in behaviors such as stalking. Even if a user's activity on Venmo is private, the app requests other information that is then made public, and this information could be used to identify a user on other places on the internet such as other social media sites, which are likely to host even more information. For example, if a user uploaded the same photo to both Venmo and another social media site such as Facebook or Twitter, the same photo could be accessed and downloaded through Venmo, then reverse-image searched on any mainstream search engine to bring up other social media profiles and websites that have that same photo. This indicates that the inability to hide a photo on Venmo may have serious privacy consequences for someone who does not want other social media profiles to be discovered.

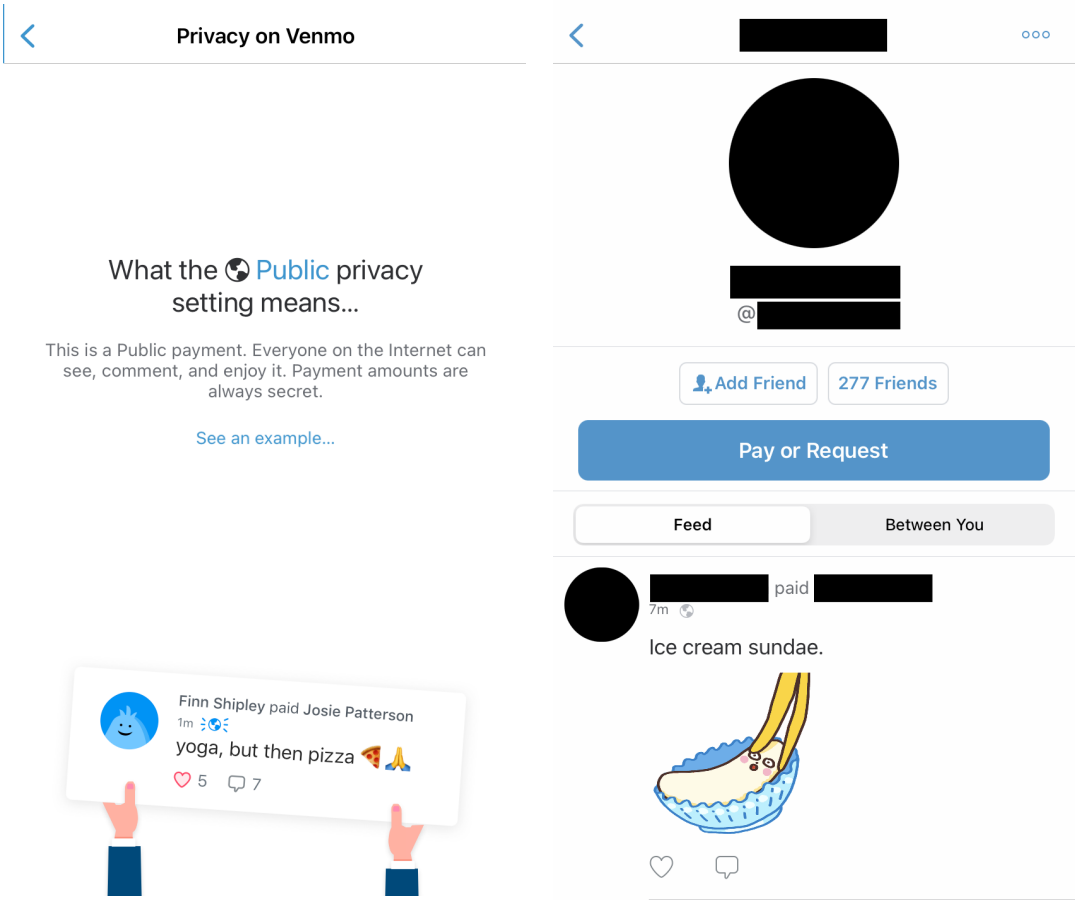


Fig. 1 (left): An explanation of Venmo's public privacy setting, found within the app. Fig. 2 (right): A screenshot of a random Venmo profile found in the public feed.

Activity on Venmo additionally incurs an extensive "paper trail" that is intended to prevent unauthorized activity, but can be problematic if a user is being targeted by a UI-bound adversary such as an abusive intimate partner. Venmo has a highly customizable set of notifications to send alerts to the device, email, or phone number associated with the account when various activities are performed, such as sending a payment or changing account information (see Fig. 3). Thus, if someone other than the Venmo user had access to that email or phone number, they could be remotely alerted to any activity on the account as well as attempts by the original owner to regain control, such as changing the password. As Freed et al. (2018)

discuss, this situation can potentially be a dangerous one for someone experiencing intimate partner violence, as an abuser may retaliate after being alerted to their attempts to regain control of their own account.

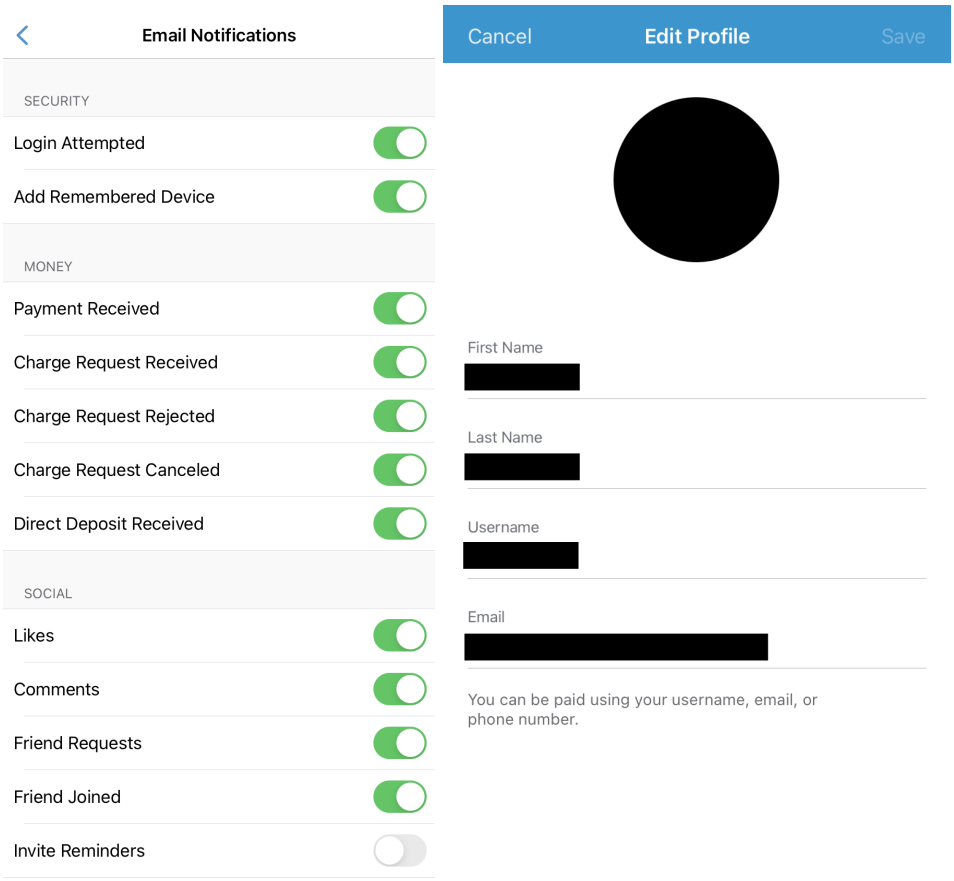


Fig. 3 (left): Just a portion of the notifications that can be sent from Venmo when various activities are performed. Fig. 4 (right): Venmo's profile settings editor, where on a browser the user would have the option to close the account— an option that does not exist within the app.

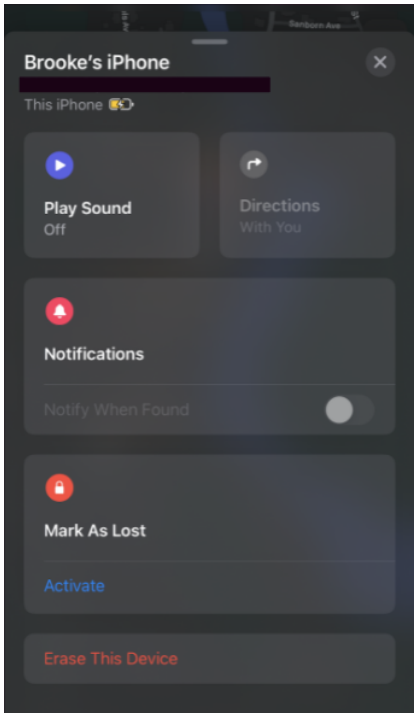
Although many Venmo notifications can be turned off within the app's settings, one type of notification that I found could not be is an email alert triggered after sending a payment. Thus, even if most traces of Venmo activity can be removed if the user prefers, some activities will still trigger alerts with no way to prevent them. This may hinder safety for a user who does not want

their activity shared, and could facilitate financial abuse by making it easy to monitor the frequency of payments, who they are sent to and received from, and their amounts.

Closing a Venmo account, which a user experiencing intimate partner violence may need to do for safety, is also complicated by the app's developers. A Venmo account cannot be closed through the app's interface, and instead this action must be performed by using a web browser to navigate to Venmo's website, logging in with the appropriate account information, and opting to close the account. This alternate course of action is not explained within the app at all, and the option to close an account is simply absent from the settings section (see Fig. 4). Forcing users to take an unfamiliar route to close their Venmo account lengthens and complicates the process for a few reasons. For one, since it is not explained in the Venmo app, users might not know of this option at all— since Venmo activity is conducted primarily through the app, many users may not even know that a separate website exists, let alone that it has exclusive features. Additionally, more Americans each year continue to report that they access the internet predominantly using their smartphones (37% in 2019 [Anderson, 2019]), further indicating that they would likely not be aware of these features, and would be at a disadvantage in this situation if they did not have ready access to a computer. Lastly, requiring users to log in with their Venmo account information when the app automatically keeps users signed in poses additional obstacles, as they may not easily recall this information and would have to go through the process of resetting their account's email or password when time is potentially of the essence.

IVb. Find My

Combining the features of previous iterations of Find My iPhone and Find My Friends, Find My serves as a control center that allows the user not only to view the location of their Apple devices, but to share their location with specified contacts. Users of Apple products already have an iCloud account associated with their device(s), so there is minimal setup required to begin using this app. Signing in with an iCloud account brings up an interface showing a map with pins to indicate the location of Apple devices signed into that account (see Fig. 5). Selecting a device will bring up additional information, such as the device's battery level and the last time its location was recorded. Another option triggers the Maps app (another default app on Apple devices) to display specific directions from the user's current location to their device. There are also numerous commands that can be sent to the device in the event it has been lost or stolen. It can be made to play sounds to help locate it, or it can be marked as "lost", which locks the display on a custom message, and disables standard use of the device and any features such as Apple Pay (see Fig. 6). The final option listed erases the device completely.



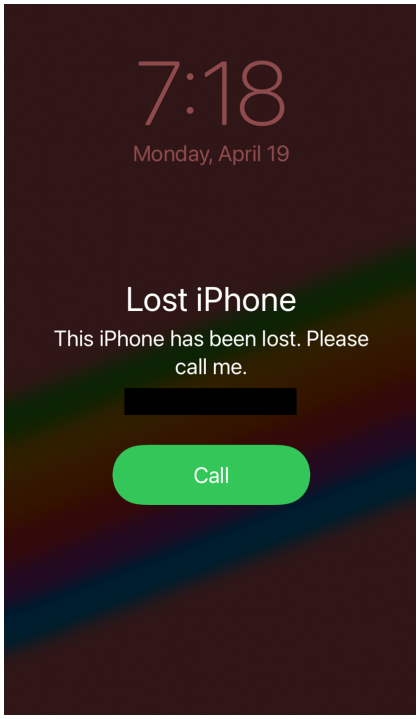


Fig. 5 (left): Information and options displayed about an Apple device when it is selected from the main menu.
Fig. 6 (right): What my iPhone displayed when I marked it as "lost".

Find My's capabilities of remotely altering or disabling a device-- much like Venmo's policies of extensive data collection and public display-- have clear purposes in security, a common rationale for the development and use of surveilling and controlling technologies. If someone loses their phone, being able to precisely track its location may be immensely helpful in finding it, and marking it as lost can help a stranger who finds the device to return it to its original owner. However, in the context of intimate partner violence, it is not difficult to imagine how these features could be repurposed to surveil and even harass someone. Devices such as smartphones are an asset to daily life for both convenience and safety, so it is common to have one within reach almost always. Therefore, someone with access to the associated iCloud account (such as an abusive partner) could easily track the user's location without them knowing, even if they take steps to remain undetected such as turning off data or powering off the device. Someone else with account access could also use Find My to harass the device's owner by disabling the device, making it play sounds that can't be turned off, or erasing its data completely. Although these actions are secured with an iCloud account, this does not take into account the reality that many of the people who experience intimate partner violence cohabitate with an abusive partner, and may even be financially dependent on them. Thus, an abuser could coerce their partner into revealing account information that is normally private, or the device may even be set up in their name (which is often the case with many shared phone service plans that cohabitating partners may sign up for). Without the additional layer of security provided by account authentication, Find My acts in a very similar manner to an off-market malware app, with some of the same capabilities.

Another feature of Find My that has been just recently introduced is an Items section (see Fig. 7). This feature allows compatible Bluetooth devices not manufactured by Apple to be recognized by the app, where they can be tracked in a similar manner to Apple devices. The Items tab also indicates the capability to identify an unknown Bluetooth item, meaning the owner can imprint a message and contact information onto the item that can be scanned by Find My if the item is lost and found by someone else. Although not many of these products are on the market yet, one of the products listed on Apple's website is the Chipolo ONE Spot, a small item finder that can be attached to a larger item for tracking purposes (see Fig. 8). One potential concern with these kinds of devices is that they may be secretly placed on someone's property in order to track location without their knowledge.

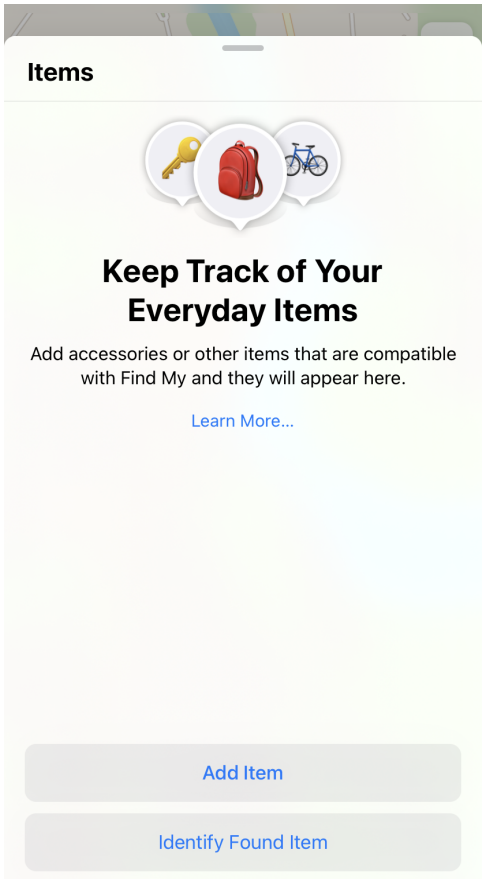


Fig. 7 (left): The interface displayed when selecting the Items tab in Find My.
Fig. 8 (above): Product image of the Chipolo ONE Spot.

The recent unveiling of Apple's AirTags, tracking chips similar to the Chipolo ONE Spot, is even more concerning. As Fox Cahn and Galperin (2021) point out, the fact that AirTags operate on the global tracking network shared by every iPhone means that its location tracking capabilities have the potential to be more precise than any of its current competitors. Additionally, the mainstreaming of this kind of technology through Apple's branding, without much acknowledgement of the potential harm it may cause, is worrying. Leaks of a future iOS update indicate the future introduction of "Item Safety Features" that can inform a user if there is an unknown Bluetooth device such as an AirTag moving with them (Fathi, 2021). However, there is no clear indication of how robust these safety features may be, and the introduction of such discreet trackers may have problematic implications for people experiencing gender-based violence or intimate partner violence, especially if they do not have devices that can warn them of the presence of item trackers, or if they do not know about such devices in the first place.

IVc. Limitations

As established by Light, Burgess, and Duguay (2016), a researcher employing the walkthrough method may create new accounts for the purposes of research, or use their own. Due to the extensive integration of my own personal information with my iCloud and Venmo accounts, I was hindered from creating new accounts for research, as doing so would have wiped my iPhone and likely triggered a fraud alert from my bank. I also find it meaningful to note how tightly woven I found my personal, financial, and even physical information to be with my account data, again proving how such areas contain great exploitative potential in the case of an account security breach.

V. Consequences & Recommendations

In stepping through both of these seemingly simple and mundane technologies, one of my general observations was that traditional mechanisms meant to protect account security are poised to fail when users are experiencing intimate partner violence. The reasons for this align with the unique circumstances of many people in intimate partner violence situations, such as cohabitating with an abusive partner, or being financially dependent on them. Freed et al. (2018) state that traditional account safeguards, such as having a password or requiring email or phone number identification, anticipate security threats from strangers rather than someone who is known to the user— and therefore, are likely to fail when it comes to protecting account security of users affected by intimate partner violence. In fact, these users can even be put in more unsafe situations due to the extensive notifications that are sent out when changing account information such as passwords, which could alert an abuser to the action and cause them to retaliate. These measures are meant to prevent unauthorized account activity, but may pose a critical obstacle to users trying to regain their digital independence.

Another observation I made was that these technologies, particularly Find My, work to normalize substantial data collection and control. Find My collects and reports considerably far-reaching data about our devices, from their precise location down to their battery level. And although these capabilities are certainly useful in locating a lost or stolen device, or sharing location with family members or friends to ensure safety, it is concerning to think about the amount of highly intimate information that could potentially end up in the wrong hands. Lastly, in considering Venmo's unique social component, I found that limited privacy settings— including having completely public activity as the default profile setting, and not allowing users

to make their information fully private if they choose— leave a wealth of personal information out in the open, rendering users vulnerable to threats such as stalking.

Davis and Chouinard's (2017) suggestion of technologies' affordances through mechanisms is appropriate to understanding how the use of mundane apps like Find My and Venmo for gender-based violence and intimate partner violence is not intended by their creators, yet can be easily accomplished while operating within their standard user interfaces. While app features such as identity verification, public activity sharing, and location tracking are intended to be used to ensure security-- such sharing location with a loved one or ensuring a payment is sent to the correct user-- more dubious uses of these features as tools to spy on or stalk a stranger, acquaintance, or intimate partner are not advertised, but still tacitly allowed within the boundaries of each app. Although apps' individual terms of service agreements may state that they are not to be used for illegal activities, many acts of gender-based violence are difficult to fully encapsulate within a legal definition (governments historically have struggled to legally define crimes such as sexual violence in a way that acknowledges their complexity, often leading to a lack of justice for women survivors). As such, these apps' ability to be repurposed for stalking and intimate partner tracking is able to largely go unnoticed in mainstream discourse, leading developers to becoming complacent in the idea that their technologies are innocuous and safe.

As of the year 2020, women make up less than 30% of the technology workforce (CNBC, 2020). The historic underrepresentation of women in this field is rooted in antiquated assumptions about gender roles, and how those roles translate to interactions with technology. Technology has long been viewed as a "hard" science innately suited to men, while women fall

on the receiving end of technological innovation as passive consumers or even objects of surveillance.

When considering the concerns regarding technology's role in facilitating gender-based violence and intimate partner violence, it is appropriate and even necessary to point to the lack of equal gender representation in technology development as a cause of these considerations being overlooked. In fact, the wide potential for disparate outcomes for women using social technologies that tacitly allow acts of gender-based violence, including intimate partner violence and stalking, exemplifies Hoffmann's concept of *data violence*. With men in the majority of tech-based roles, often playing pivotal roles in the development and maintenance of widely used apps, concerns that are less likely to impact men (such as of gender-based violence and intimate partner violence) can go unaddressed-- leaving these apps to enter the public with glaring security risks. On the other hand, including more women in app development increases the likelihood that these gender-based concerns will be properly addressed. One example of this is the social networking and dating app Bumble, founded by Whitney Wolfe Herd. Wolde Herd has described Bumble as "100 percent feminist", referring to the app's highly discussed feature of only allowing women users to send the first message in heterosexual matches (Yashari, 2015, para. 9). Not only does this design choice deliberately challenge traditional heteronormative dynamics of dating, it also enhances safety for women users by preventing unsolicited messaging and harassment from men. Improving technology's impact on women's safety will involve not only hiring more women in tech, but continually working to change the culture and the conversation surrounding technology and the socially-constructed values we have come to associate with it, leading to innovation that enhances safety and inclusivity.

As technological capabilities only continue to expand, it also may be worth considering introducing new forms of authentication to combat advanced cybersecurity threats, including those that may come from others we know. More intimate safeguards, such as facial recognition and fingerprint identification, have been introduced in recent years and are currently in use as part of many mainstream devices' security features. It is possible that mechanisms such as these may ultimately grow to surpass the username and passwords we are currently familiar with. However, the integration of bodily data into technology is a highly contentious issue, raising more concerns about its implications for privacy and independence. Thus, for these kinds of mechanisms to be implemented as ethically as possible, changes must first be enacted— both legally, to impose regulations on big tech in regards to collecting, storing, and sharing data; and socially, to ensure that these impactful technologies are designed with as little bias as possible— to keep the internet and the technological world as accessible and safe as possible.

VI. References

Anderson, M. (2019). Mobile Technology and Home Broadband 2019. *Pew Research Center Internet & Technology*.

Blohm, I., & Leimeister, J. (2013). Gamification: Design of IT-Based Enhancing Services for Motivational Support and Behavioral Change. *Business & Information Systems Engineering*.

Brock, A. (2016). Critical technocultural discourse analysis. *new media & society*, *20*(3), P.1012-1030.

Centers for Disease Control and Prevention (2020). *Violence Prevention: Intimate Partner Violence.*

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., Levy, K., Dell, N., McCoy, D., & Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. *IEEE Symposium on Security and Privacy, San Francisco, CA, USA*.

Davis, J., & Chouinard, J. (2017). Theorizing Affordances: From Request to Refuse. *Bulletin of Science, Technology, & Society*, *1*(8).

de Best, R. (2021). Venmo payment volume 2017-2020, per quarter. *Statista*.

Draper, N. A. (2014). Defining Family: Representation and Rhetoric in the Marketing of Shared Mobile Phone Plans. *Critical Studies in Media Communication*, *31*(1), p. 57-71.

Draper, N. A. (2019). Reputation Anxiety: Consumer Background Checks and the Cultivation of Risk. *Communication Culture & Critique*, *12*, p. 36-52.

Faulkner, W. (2001). The technology question in feminism: A view from feminist technology studies. *Women's Studies International Forum*, *24*(1).

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, USA.

Fox Cahn, A., and Galperin, E. (2021). Apple's AirTags Are a Gift to Stalkers. *Wired*.

Hasinoff, A. A. (2017). Where Are You? Location Tracking and the Promise of Child Safety. *Television & New Media*, *18*(6), 496-512.

Hoffman, A. (2018). Data Violence and How Bad Engineering Choices Can Damage Society. *Medium*.

Levy, K. (2015). Intimate Surveillance. *Idaho Law Review*, 51(3).

Levy, K. (2018). The Phallus-y Fallacy: On Unsexy Intimate Tracking. *The American Journal of Bioethics*, 18(2).

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1).

Light, B., Burgess, J., & Duguay, S. (2016). The walkthrough method: An approach to the study of apps. *new media & society*, 20(3).

Lupton, D. (2015). Quantified sex: A critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4).

Lupton, D. (2016). *The Quantified Self*. Germany: Wiley.

Mason, C., & Magnet, S. (2012). Surveillance Studies and Violence Against Women. *Surveillance & Society*, *10*(2).

Norman, D. A. (1988). *The Design of Everyday Things*. New York: Doubleday.

Ott, M. (2017). Series: What Does That Mean? Gender-based Violence. *Women for Women International*.

Scott, S. (2019). Interrogating the Fake Geek Girl: The Spreadable Misogyny of Contemporary Fan Culture. In *Fake Geek Girls: Fandom, Gender, and the Convergence Culture Industry* (pp. 76-108). New York: NYU Press.

Spiekermann, S. (2004). General Aspects of Location-Based Services. In Voisard, A., *Location-Based Services*. Ukraine: Elsevier Science.

Swartz, L. (2020). Transactional Memories: Social Payments and Data Economies. In *New Money: How Payment Became Social Media* (pp. 108-138). New Haven; London: Yale University Press.

Troullinou, P. (2017). Exploring the Subjective Experience of Everyday Surveillance: The Case of Smartphone Devices as Means for Facilitating "Seductive" Surveillance. *The Open University*.

Welch, D. (2021). Apple surpasses $100 billion in quarterly revenue for first time in its history. *The Verge*.

Wolf, G. (2009). Know Thyself: Tracking Every Facet of Life, From Sleep to Mood to Pain, 24/7/365. *Wired*.

World Health Organization (2021). Devastatingly pervasive: 1 in 3 women globally experience violence. New York.

Yashari, L. (2015). Swipe Night: Meet the Tinder Co-Founder Trying to Change Online Dating Forever. *Vanity Fair*.