Sci Eng Ethics
DOI 10.1007/s11948-014-9621-1

ORIGINAL PAPER

The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy

Fiachra O'Brolcháin · Tim Jacquemard · David Monaghan · Noel O'Connor · Peter Novitzky · Bert Gordijn

Received: 8 August 2014 / Accepted: 9 December 2014

Abstract The rapid evolution of information, communication and entertainment technologies will transform the lives of citizens and ultimately transform society. This paper focuses on ethical issues associated with the likely convergence of virtual realities (VR) and social networks (SNs), hereafter VRSNs. We examine a scenario in which a significant segment of the world's population has a presence in a VRSN. Given the pace of technological development and the popularity of these new forms of social interaction, this scenario is plausible. However, it brings with it ethical problems. Two central ethical issues are addressed: those of privacy and those of autonomy. VRSNs pose threats to both privacy and autonomy. The threats to privacy can be broadly categorized as threats to informational privacy, threats to physical privacy, and threats to associational privacy. Each of these threats is further subdivided. The threats to autonomy can be broadly categorized as threats to freedom, to knowledge and to authenticity. Again, these three threats are divided into subcategories. Having categorized the main threats posed by VRSNs, a number

F. O'Brolcháin (✉) · T. Jacquemard · P. Novitzky · B. Gordijn
Institute of Ethics, Dublin City University, Dublin, Ireland
e-mail: Fiachra.obrolchain@dcu.ie

T. Jacquemard
e-mail: tim.jacquemard@dcu.ie

P. Novitzky
e-mail: pnovitzky@gmail.com

B. Gordijn
e-mail: bert.gordijn@dcu.ie

D. Monaghan · N. O'Connor
Insight Centre for Data Analytics, Dublin, Ireland
e-mail: david.monaghan@insight-centre.org

N. O'Connor
e-mail: noel.oconnor@insight-centre.org

Published online: 01 January 2015

of recommendations are provided so that policy-makers, developers, and users can make the best possible use of VRSNs.

Keywords Social networks · Virtual reality · Ethics · Privacy · Autonomy · Freedom

Introduction

The on-going societal transformation that is being brought about by the digital revolution might in time prove itself to be as radical and turbulent as that brought about by the invention of the printing press. Indeed, in a speech delivered to the CeBIT 2014 trade fair in Hannover, Germany, the current British Prime Minister, David Cameron, recently referred to a "new industrial revolution" (Cameron 2014). The Internet's evolution from a network of networks containing chunks of static content into something that incorporates interactive features—the so-called "Web 2.0"—has seen much of contemporary life represented online. This rapid evolution shows no sign of abating—"apps" and mobile devices are now profitable, useful, and an almost integral part of daily life. The economic value of apps was demonstrated by WhatsApp being bought by Facebook for $19 billion in February 2014 (O'Dwyer 2014). The increased focus on personalisation might even herald "Web 3.0".

The Internet has changed and continues to change the ways in which people interact and socialise, access information, and find entertainment. It is a major source of news and entertainment, as well as a hub for commerce. This empowers companies such as the search engine Google and places them in a hugely influential position, as the gatekeepers to key elements of individual and social life e.g. fulfilment of informational needs, social environments, and entertainment. Online social networks (SNs) such as Facebook, MySpace, LinkedIn, Bebo, Pinterest, and Twitter are a contemporary social phenomenon, with Facebook claiming to have 1.32 billion active daily users (Facebook Newsroom 2014). Massively multiplayer online role-playing games (MMORPGs) have become enormously popular, with World of Warcraft (WoW) perhaps the best known, having an estimated 77 million subscribers (Karmali 2013). MMORPGs have a number of interesting characteristics: they are social and they are set in immersive virtual worlds. Virtual worlds are the best-known manifestation of virtual reality (VR)—computer-simulated environments—and have been driven primarily by the computer gaming industry, however VR can have a multitude of other uses outside computer games. Depending on how the digital environment is displayed, it is more or less immersive. For example, if a virtual world is displayed on a high-end 3D cave, it will be more immersive than if it were displayed on a standard screen.

The focus of this article is on the increasing convergence between SNs and VR.[1] There are indicators that these two technological areas might increasingly merge

[1] There is also academic interest in the merger of VR and SNs: the European Union has funded a 4 year research project that brings together key players in both domains—REVERIE—that aims to provide "the means for building a mixed reality space in which real and virtual worlds engage and seamlessly interact in real-time, generating compelling and highly realistic immersive environments" (Objectives-REVERIE 2014). This will, it is thought, "introduce a paradigm shift for how communication happens in social

together in the future. Facebook's acquisition of the VR technology company, Oculus VR Inc., for 2 billion dollars (Cellan-Jones 2014) has increased interest in the technology, with Facebook planning for a future in which its members "[share] not just moments with [their] friends online, but entire experiences and adventures" (Zuckerberg 2014). Meanwhile, gaming has taken on aspects of SNs, with the immersive worlds of massive multiplayer online role-playing games (MMORPGs) functioning (to some degree) as sites for socialising and interacting with friends. It is not only that games are becoming more social, but SNs are taking on aspects of games. The idea of "Gamification", i.e. making day-to-day activities resemble games by awarding points or similar and recording these on apps and SNs, further illustrates the impact of Internet technologies on everyday life: the providers of the "games" profit by gathering data on the players.

In a converged virtual reality social network (hereafter VRSN), people would be represented by avatars and be able to interact in real-time in virtual environments. VRSNs would build on the success and popularity of social networks, in which users can post information about their lives, their interests, their friends and family, for others to peruse as well as contact each other and talk to message each other. Significantly social networks are based on the assumption that people in them are who they say they are, unlike MMORPGS where people play a character. VRSNs would extend the social aspect of social networks and combine it with developments in virtual reality by facilitating people using avatars that are realistic representations to interact with each other in immersive virtual environments. An avatar can be thought of as any graphical representation of a person or user. There are a wide variety of forms avatars can take: from simple icons, personalized cartoon characters, pictorial mock ups to full 3D humanoid representations. In computer gaming, avatars are primarily fictional or fantasy based characters (such as in WoW) and often the user will personalize the avatar based on how that user wishes to be represented. However, recently there has been a shift towards realistic personal avatars that accurately capture the likenesses of the user. This shift has been brought about, in part, by readily available and cheap data-capture platforms such as the Microsoft Kinect depth sensor and low-cost HD web cameras. Avatars that represent the person in real-time are now being developed—these avatars will do in the virtual what the person does in the real world. In our conception of VRSNs realistic real-time avatars are likely to dominate, thus differentiating them from MMORPGS and online worlds such as Second Life. The popularity of current social networks illustrates that there is exists a desire amongst people to interact with others as themselves—to put their lives online. It is the premise of this paper that future social networks will retain their popularity whilst making use of the technological capacity to create realistic avatars and more immersive environments in which people will be able to virtually interact. Indeed, depending on the level of immersion and the technologies available, people might be able to receive

Footnote 1 continued
networks" (ibid) by revolutionizing "immersive media distribution from a passive centralized context to a personalized highly distributed framework" (ibid). Furthermore, this "will provide for the individuals new ways of 3D/immersive media sharing and distribution under a socially aware, personalized, collaborative and distributed framework" (Expected Results-REVERIE 2014).

sensations from interacting with others. The avatars would be able to communicate with other avatars controlled by "real" people, with artificially intelligent (computer controlled) avatars, and with the virtual world. This would not only be used in gaming, but could also be used for historical reconstructions, political debates, business meetings, health services, and for education. These worlds would likely be "walled-off" and under the control of the designers, developers, or governments responsible for their creation.

The distinguishing feature of VRSNs as opposed to game environments with a social aspect will be that people will by and large enter VRSNs *as realistically-represented versions of themselves*. Data-capture technologies already make this feasible. Many avatars will be representing how the person is in real-time. A VRSN would not only allow a user to look at a person's profile, but to meet them in an immersive virtual environment. Thus, people with similar interests in various parts of the world will be able to meet in immersive environments. Haptic technology that provides sensations to users would make encounters even more realistic. These worlds—VRSNs—are the focus of this article.

So, in discussing a VRSN, we hypothesise a scenario in which a significant portion of the world's population is a member of a social network, which either are immersive or at least offer immersive experiences. A significant difference between current VRs and even prototypical VRSNs such as WoW is that in this new scenario, users would enter the VRSN *as themselves*, rather than playing a character as in a game. Users would appear in these immersive worlds as either realistic representations of themselves or as avatars, which may or may not resemble the user. New technologies permit avatars to represent the movements, expressions, and emotions of the user in real-time. It is likely that this sort of representation will be extremely popular outside of the gaming spheres. For instance, it is possible that many important services, currently primarily available off-line, will be available in VRSNs, e.g. teaching or extra-tuition, medical check-ups, and business and financial advice. As artificial avatars become more sophisticated and people's interactions with them more closely resembles interacting with a real person, more and more of them would be used in VRSNs in order to facilitate people receiving these services without having to travel or wait for appointments. A further point to consider is that VRSN providers would have financial incentives to encourage users to appear as real-time representations of themselves. Facebook is, for example, very keen that people use their real names and identities when joining as this allows them to harvest information about real people that can then be sold to advertisers. Real-time representations of users of VRSNs would provide more detailed, and consequently more valuable, information.

It is possible that social networks will evolve to incorporate these features, with the result that all social network users will participate in immersive worlds. Whether or not this sort of convergence comes to dominate the way people interact with the Internet overall, or just becomes another feature of the online world cannot be known at present. For instance, it is plausible that current users of social networks are quite content to post photos of their holidays and to comment on their friends' posts, without wanting to meet their friends in an immersive environment. Nonetheless, there is evidence for an ongoing process of convergence and it is

equally plausible that those users who do not always want to participate in the immersive aspects of a VRSN will nonetheless create profiles that would enable them to do so if they chose. On top of this, there will be a significant number of users that will regularly participate in VRSNs. In doing so we are presupposing a scenario in which a large proportion of the world's population are members of VRSNs, meaning that they participate in online immersive virtual environments in which they are represented as avatars, and possibly by avatars that realistically represent them in real-time.

The ethical problems VRSNs present will not be entirely new. VRSNs themselves will emerge only gradually, in stages. Thus, many ethical problems will already be present in current social networks or virtual worlds. Our contention is not that VRSNs will present completely new problems but that the convergence of current technologies into VRSNs will transform current ethical concerns, making them more acute and urgent. Moreover, the scale of VRSN usage will be far greater than is the case for virtual worlds now, with VRSNs replacing the necessity of real-world interaction in many cases. More information about peoples' traits and behaviours will be available.

The threats to privacy arising from new Internet technologies taken individually are already the subject of much debate (Vallor 2010; Sartor 2012). The threats to autonomy are less prominently discussed in explicit terms in the current ethical debate. However, issues with autonomy underlie many of the problems raised in the academic literature. Hence, we deem them equally important. Numerous potential social and political ills have been identified relating to, amongst others, addiction, manipulation, and political and/or corporate control (Cranford 1996; Gotterbarn 2010; Gooskens 2010; Papagiannidis et al. 2008), all of which might reduce an individual's capacity to act according to their own desires and wishes. Moreover, we argue that the threats to privacy may themselves pose a danger to autonomy. Outlining two of the chief ethical issues that might emerge from VRSNs ought to aid policymakers, providers, and users in avoiding the worst pitfalls.

We focus on autonomy and privacy, as they are foundational principles in the Western liberal democracies i.e. the cultures primarily responsible for the development of VRSNs. The autonomous human subject is a central one in contemporary liberal thought. Liberalism is explicitly concerned with protecting people's opportunities and abilities to choose for themselves what to do with their lives. One ideal of liberalism is to protect the rights of autonomous individuals, who can choose their own goals and create their own values. It is therefore particularly important from a liberal perspective to preserve the conditions that facilitate individuals being autonomous. Insofar as a lack of privacy undermines the conditions required for autonomy VRSNs pose an indirect threat to autonomy as they undermine privacy. VRSNs also pose more direct threats to autonomy. However, there are some scenarios in which VRSNs will possibly enhance people's autonomy. Thus VRSNs might create new societal norms in which privacy is all but absent and autonomy is much more precarious.

The paper is organised as follows. We begin with an analysis of the concept of privacy, distinguishing informational, physical, and associational privacy. We then look at the ways in which each kind of privacy is threatened by the convergence of

VR and SNs. We subsequently analyse the concept of autonomy as having three necessary components: knowledge, freedom, and authenticity. This then allows us to explore how each of these components is affected by the convergence. We suggest that both privacy and autonomy are of great ethical importance and that there are therefore obligations for policymakers, providers of VRSNs, and users of these services to protect these values. We provide some recommendations and strategies for tackling the problems of privacy and autonomy in the final section, which we believe will help policymakers, providers, and users understand the issues of privacy and autonomy at stake and avoid the potential losses of privacy and autonomy.

Privacy

Privacy plays an important role in protecting valuable conditions of moral personhood or normative agency. Most people would not be comfortable exploring certain ideas, expressing some opinions, or behaving in specific ways without a certain degree of privacy. Persons, if they are to develop themselves and explore their ideas, require a degree of privacy in which to do this. Life in a world of diminished privacy will affect the development of individuals' moral characters. Individuals will no longer have as much of a private space in which to make mistakes, experiment, explore different aspects of themselves (Vallor 2010). It is a founding principle of liberal states that there should exist a personal realm exempt from government interference (Locke 1689; Mill 1859). Without privacy, the ability of governments (and companies) to influence individual and group behaviour will be extensive.

Unfortunately, the possibility of maintaining privacy is seriously reduced with the advent of digital technology, and with the further convergence of SNs and VR, the threats to privacy will in some cases be exacerbated. The fact that people are carrying out more and more daily tasks and activities online means that they are leaving an increasingly larger and larger digital footprint. This footprint can be used to find out a lot about individuals and thus threaten their privacy. Furthermore, others might capture a person's image or record them, thereby making it more difficult for an individual to control how information about them is released. Indeed, if the "Internet of Things" (which would see the creation of a world of ambient technology) emerges as predicted ("Internet of Things" 2014), genuine privacy is likely to become even less feasible. Moreover, VRSNs are likely to provide users with the possibility of being realistically represented in real-time. In some cases, VRSNs will insist on users being represented in this manner. This will require that users' likenesses, expressions and emotional reactions are captured as they interact with the virtual world and the other people within it.

Helen Nissenbaum advances the idea of privacy as "contextual integrity" (Nissenbaum 1998: 559). According to this theory privacy norms will be dependent on context. For Nissenbaum, violations of privacy can be determined by non-compliance with norms that relate to appropriateness and distribution. Some norms concern the appropriateness of asking for and revealing information; whilst others

concern the distribution of information. The aim of this section is not to provide a full exploration of the concept of privacy as such, but to explore the ways in which VRSNs will create new contexts and consequently new norms of privacy. In order to do so, we distinguish three different kinds of privacy (adjusted from Allen 2011). *Informational* privacy relates to protection against third party access to all kinds of information about an individual including an individual's thoughts, utterances, correspondence, and financial, medical and educational records. *Physical* privacy relates to some sort of shelter against third party sensory access to an individual's body and actions. Thus it concerns modesty, separateness, bodily integrity and the like. *Associational* privacy concerns an individual's control over excluding and including third parties in certain specific experiences. It thus guarantees the intimacy of certain social situations that an individual wishes to be intimate (Allen 2011). Based on this distinction we identify three kinds of threats to privacy.

Threats to Informational Privacy

There are several threats to informational privacy. In order for VRSNs to function we would need personal information to expand functionality and create a better user-experience. For example, medical information would be required for virtual meetings with doctors (either fully artificial doctors or the avatars of real-life doctors). There are two threats related to information privacy when VRSNs become a reality.

Increased Vulnerability of Data

The first such threat is that by digitizing data, it becomes accessible to a larger group of people. Some threats to informational privacy come from hackers, government agencies, malware and criminal organisations that are able to use electronic media to access information about an individual. Widespread use of VRSNs will mean that more information about an individual will be potentially available to these groups than ever before. The fact that information is being stored electronically makes it accessible to people irrespective of geographical location. For instance, bank details, medical records, personal correspondence are all stored online. This is obviously a very useful feature, but it means that personal information is at risk of being used in ways that are inappropriate or unjust, e.g. being stolen by hackers, criminal organisations, or used by government agencies. In the VRSN scenario, these sorts of data will need to be protected.[2] The recent discovery of the Heartbleed bug—which enabled people to steal data, eavesdrop, and impersonate users and servers by accessing sites thought to be secured by OpenSSL (used to encrypt communication between a user's computer and the server) without the possibility of detection, illustrates the risks of online information (Wakefield 2014). This affected a huge number of sites, including Internet behemoths such as Google as well as smartphones running Android 4.1.1 (cca. 35 % of all smartphones, 50 million users), Amazon Web Services and Pinterest. Prior to the digital era it was possible to

[2] Clearly data will need to be protected in other scenarios also.

steal this information too, but now it can be potentially stolen from anywhere in the world, very quickly, and the theft might go unnoticed. These threats exist currently, prior to the widespread adoption of VRSNs. However, as mentioned above, the extra information that a VRSN will gather (eye-movements, emotions, real-time reactions), will mean that even more data about the individual is digitized and (potentially) available to those who would misuse it. Furthermore, in our scenario, VRSNs would be used for more than gaming—people might meet virtual doctors, virtual accountants, virtual teachers and so on. As such, more people are likely to make use of VRSNs than currently partake in either VRs or SNs and they are likely to reveal more intimate and personal information in online scenarios, placing it at risk.

Furthermore, individuals are often unaware of the amount of personal data that they are making available online. Therefore, although a person might be extremely careful regarding certain information (e.g. medical records) and might be content to reveal a certain degree of information, they may find that they are revealing more than they intended. Companies arguably purposefully use overly complicated and convoluted terms and conditions so that individuals might not be aware of the amount of information about themselves that they are "agreeing" to make available. Websites gather huge amounts of data about the individual (Ford 2001), e.g. via "cookies" or other user-tracking activities. There is little reason to assume that VRSNs, were they to become popular, would not also gather data about their users. The business model of Internet firms such as Google and Facebook is predicated on gathering information about their users and selling these data on to others—take for example Facebook's aforementioned acquisition of WhatsApp, which provided it with the phone numbers, locations, user names and contact lists of the 465 million users. Increasingly websites and Internet features request users to create profiles or to sign up to membership, which involves providing real (the host's hope) personal information and submitting to legally binding contracts, in order to use the service.[3]

Misuse of Data

The use of these data can have undesirable consequences. The erosion of informational privacy will have significant effects. With VRSNs more data about more people will likely be available. Many individuals will have an interest in certain information remaining private, i.e. information about health, financial status and sexual preferences (Gill 2008). If this sort of information were no longer private individuals might face discrimination as a result of what is known about them. It is already possible to determine to a significant degree a person's political stance or sexual preferences through analysis of their "likes" on Facebook (Kosinski et al. 2013). For example, someone who has previously had mental health issues might find their job opportunities reduced or their social life affected (Lory 2010; Kaupins and Park 2011; Birky and Collins 2011). Consider the story of the Target store in the

[3] Everyone with a Gmail account has automatically been given a Google+ account; whilst Microsoft's latest Windows system—Windows 8—requires users to create a Microsoft account if they are to avail of many of the applications that come with the software.

US enraging the father of a teenage girl by sending coupons for baby clothes and other maternal items to the daughter (Duhigg 2012). It later emerged that she was pregnant and the store had worked this out by analysing her purchases. A similar scenario might cause huge problems for a teenage girl who wished to control when, and if, she told her parents about being pregnant. Another example is information about a gay person's sexual preferences; in certain countries they would face time in prison, were these to be made public. As more socialising moves online, this sort of information will be accessible to more people. A VRSN may give the illusion of greater privacy in these matters than is actually the case, e.g. a person may act with fewer inhibitions in a VRSN than in the real world, forgetting that their actions might become known to many more people than expected—both within and outside of the VRSN. This is more likely the more immersive the VRSN. Users are going to be immersed in the moment and may be tempted to abandon caution about their actions more so than they would be in the offline world.

Threats to Physical Privacy

These threats are likely to arise from the proliferation of devices that can record people in their physical surroundings and the ease with which recordings can be shared and made public. Indeed, it is reported that there exists one CCTV camera for every 11 people in the UK (Barrett 2013). For example, it is likely that new smartphones will be able to continuously record sounds around them without the consent of the user (Talbot 2013). Recordings of people's faces and emotional states, and possibly bodily movements might be required to create virtual avatars and can be considered a threat to physical privacy. We will access VRSNs via devices, be they on mobile phones, tablets, laptops, computers TVs, or even in everyday objects. These devices will be able to record us and send that data to the VRSN. There are three main threats from VRSNs to physical privacy.

Prevalence of Recording Devices

The first threat is that we might lose control over being observed in our physical environment. Recording devices will be essential in order to access VRSNs, particularly if persons are to be realistically represented as themselves in real-time. That recording devices might be both ubiquitous and practically invisible, or embedded in furniture or clothing, will make physical privacy even more difficult to protect. Ideally if a person is alone in a room, they can be confident that they have a degree of physical privacy. They can check if someone is hidden somewhere, they can ensure that no one can look in through a window or an open door. However, the convergence of VR and SNs makes this type of privacy less certain. Physical privacy can even be compromised for those that are aware of the existence of these recording devices. The fact that these devices are often accessible and possibly activated through the Internet makes it in theory possible that a third party would activate the device outside the control of its legal owner. For instance, under certain circumstances, the FBI can turn on a person's camera on their phone or computer without their knowledge (Timberg and Nakashima 2013). This technology is also

used by criminal gangs, who, in a phenomenon known as "camfecting", gain control of a person's webcam. If VRSNs were to become hugely popular—as in our scenario—these threats would be exacerbated.

Unintended Revelation of Physical Information

A second threat is that we might lose control over what information is revealed when using these devices required to enter a VRSN i.e. these devices will record not only what we intend to reveal but also many things we did not intend to reveal. Whilst this is the case to a degree in current social networks, the addition of data-capture technologies will exacerbate this problem in VRSNs. When a person is watching something online they will react in numerous, unconscious ways—their eyes will flicker, their position will shift, their face will react and so on. The incorporation of eye-tracking devices or emotion-capture technologies into immersive worlds, games, SNs and the web in general, will make it possible to track these physical reactions to online stimuli. As such, data can be gathered about a person that they might not be aware of, such as the length of time they looked at a particular product and their physical reaction to what they're seeing. Indeed, it will be possible to record and track reactions that the user is unconscious of and is unable to mask. New facial recognition technology, in particular a newly developed algorithm known as "GaussianFace" exceeds the ability of humans to identify matching faces (Tomkins 2014). Previously, it was possible to obtain physical information of people's facial reactions and eye-movements, but it generally required obtrusive and obvious close observation or the employment of experts. Eye-tracking and emotion capture software—likely to play a major role in VRSNs—make obtaining this type of information far easier, more accessible to a wider number of people, and more precise.

Loss of Anonymity

A third threat is that we might become increasingly unable to choose anonymity or to hide ourselves. The development of avatars designed to realistically represent the user (for reasons of transparency) would mean that there is a digital representation of their physical self on the web. This feature would make the loss of anonymity a particularly acute problem in the VRSN scenario. Entering one of these VRSNs as someone else would be extremely difficult. Facebook, the most popular SN at the time of writing tries to get its members to use their real names; it is plausible that if there were a convergence of VR and SNs led by Facebook, they would want avatars to represent the real users. This would have the benefit of ensuring that people would know the age of the person they are interacting with in a virtual environment. It would also be beneficial if VRs were used for business meetings or educational purposes. There is something of an overlap with informational privacy at this point, as the digital representation could also be defined as digital information. Depending on the accuracy of the representation, observers of the digital representation might be able to extrapolate much information regarding the real person, e.g. age, health, distinguishing features, emotional responses to certain cues.

Threats to Associational Privacy

These will come from the greater ability of people to record and make widely available interactions amongst people as these will take place or be publicised in a VRSN, as well as from the greater difficulty in controlling who finds out about upcoming events. There are two threats identified.

Online Socialising

The first threat is that one may lose control over associational freedom outside the VRSN. An increasingly common media story is of parties thrown by teenagers (usually) who use Facebook to send out invites, and then find that thousands of people turn up, usually because they neglected to control the privacy settings (BBC News 2012). This is an example of the loss of "associational privacy", which refers to the ability to include or exclude people from certain events. The phenomenon of "revenge porn", where disgruntled exes post intimate and explicit photos or videos of former lovers illustrates the problem further. Such material can lead not just to anger and humiliation, but to people losing their jobs (Cadwalladr 2014). This last example obviously overlaps with informational privacy. In the event of the convergence of VRSN, it is likely that more social life will take place in online environments, thus exacerbating these threats as online events are going to be accessible irrespective of geographical location. In VRSNs it will be harder to control who attends a virtual event—it will be more difficult to control who knows about it, and harder to control who attends it.

The Global Village

The second threat is that important public and private places in which we communicate suffer from a lack of privacy. The threat to associational privacy has implications beyond birthday parties ending in riots, of course. Being able to socialise, share experiences with others, and debate and argue with others is instrumentally important for the individual's growth as a moral agent and for society. Individuals may wish for their activities with others, even if it is something as simple as eating a meal, to remain private. If VRSNs become significant platforms for discourse and social interaction, huge amounts of data will be created about people. This will be different from current social networks due to the scale and to the fact that information about the real person (including physical information) is being used to create the avatar of the user. This data will therefore be available to all. The fact that much of our social activities could take place on VRSNs might mean that many of our conversations about trivial *and* important matters are potentially available to third parties. Individuals lose much of their ability to control who shares experiences with them once it becomes possible for any one of those directly involved in the experience to release a video of that experience online. Furthermore, depending on the prevalence and security of the devices used to access VRSNs, a person might not even have to be in the VRSN for this to be a problem. As mentioned, if the device can be hacked, a person might not

be aware that their activities are being recorded. This could be called the "global village" problem. In villages, everyone knew everyone else's business. This could lead to small-mindedness, conformity, and a stifling social atmosphere. With the development of SNs and recording devices, this aspect of village life—the ability to pry and see what others are doing—is becoming a feature of the global village. It is now harder to control who can hear your conversations, see your actions, and find out about your life in general.

Autonomy

For our purposes, autonomy can be understood as "self-government" (Buss 2008). Autonomy plays a central role in Kantian ethics, in liberal political theory, and in the political theory of Hegel. All these theories emphasise, albeit in different ways, that to be autonomous is to obey only ourselves—to be able to deliberate and make decisions without being influenced or manipulated by external sources. The value we place on our status as human beings centres on our being agents, i.e. we choose and deliberate, make plans and form goals. That we are autonomous then, is of the utmost significance (Griffin 2008). For some libertarian thinkers, such as Robert Nozick, autonomy is of such great importance that it overrides all other considerations (i.e. equality) (Nozick 1974). Unlike the impact on privacy however, it must be noted that, the convergence of SNs and VR might also bring some benefits to autonomy. For instance, people might be able to reveal their authentic selves online whilst being prevented from doing so socially (i.e. gay people in homophobic cultures), or people accessing more information in order to make better-informed decisions. These benefits are not discussed here because the aim of this paper is to analyse only the threats and provide recommendations on how these might be avoided. The benefits are loudly trumpeted by technology companies and thus need little further promotion.

In our analysis we understand autonomy as requiring three components: (1) knowledge, (2) freedom, and (3) authenticity or being one's own person. In order to be autonomous then, people will need access to relevant *information* in order to make choices; they will need a certain *lack of constraints* so that their autonomy is not hollow; and they will need to be able to choose for themselves according to *their own ideas and values*.

Threats to Knowledge

The threats to the knowledge condition of autonomy can come from filter bubbles, cyberbalkanization, and from gatekeepers such as search engine providers or SNs or governments controlling the availability of information. Being adequately informed about relevant facts is essential for autonomy. However, the power of SNs, virtual worlds, and, especially, of search engines, to act as gatekeepers of information pose a threat to the informational condition of autonomy. Those with control over information can control how people perceive and interpret the world. It follows that insofar as companies or governments monopolise how and what information is

presented to users online, they will have a great deal of influence over how people perceive and interpret the world. For instance, it was recently revealed that Facebook was able to affect over 689,000 peoples' moods by altering their newsfeeds over the course of one week (BBC News 2014a; Kramer et al. 2014). If SNs and VR converge and become one of the chief ways people access information, users will only receive the information that the designers of the world wish them to receive. This is similar to the problems arising from search engines as such, but within a walled off VR, there might be less scope to examine alternate information sources. There are various threats to this control over knowledge, some of which are already present and some of which will be exacerbated by the convergence of VRSN.

The Filter Bubble

A first threat is the personalisation of the web, as this presents information based on an algorithm-based interpretation of a user's interests. These concerns are explicitly addressed in discussions of the "Filter Bubble" (Pariser 2011). The term "Filter Bubble" refers to personalised searches in which algorithms decide on the search results shown to a user based on information about the user. Information is being filtered based on the perceived preferences of the user, ultimately leading to a personalised online experience. Both Google (via personalised search results) and Facebook (personalised news streams) contribute to the creation of filter bubbles. For instance Google uses algorithms to determine search results and the design of the algorithms deciding which data sources are selected is opaque. If people primarily access news and information about the world via sources recommended to them by friends on SNs or by the preferences a company (via automated assessment software) considers they have, they are at risk of having a reduced range of information. Adding a virtual element to personalised news streams already extant in social networks will not reduce this threat as VRSNs come into being. Just as Facebook was able to influence users' emotional states, people in charge of a VRSN could also select the news available to a user, or the presentation of that news, e.g. through the use of sound effects or colour schemes that make certain topics more or less attractive. The filter bubble effect might also be exacerbated by the enhanced social aspect offered by a VRSN—not only would people get to post and respond to each other in text, but they would be able to meet (virtually) face-to-face—with the result that they would have even less incentive to move beyond the confines of their filter bubble.

Cyberbalkanization

A second threat is cyberbalkanization. Cyberbalkanization is the phenomenon of users confining themselves to specific but mutually incompatible perspective-forming positions (Parsell 2008; Brey and Søraker 2009). This can be partly the outcome of individual choice—individuals will prefer some sources over others—and partly as a result of personalised searches, i.e. filter bubbles. Another way in which cyberbalkanization might occur would be the nation state exerting control

over access to the Internet (BBC News 2014b) or attempts to build its own Internet (arXiv 2012). Furthermore, if companies such as Google and Facebook are thought to be too close to the US security system (for instance), nations distrustful of the US are likely to wall off their Internet in order to control information for reasons of security. Both filter bubbles and cyberbalkanization could have serious implications for public discourse, as they will make it harder for people to see each other's point of view. Cyberbalkanization is already an issue with social networks, as people can interact with others who reinforce their views. Adding a virtual element to these interactions, particularly if the virtual world responds to the users, is likely to make such a world more appealing to those users with the result that they are less likely to look beyond its horizons. The development of artificial avatars that further reinforce users' beliefs and perspectives would further exacerbate this threat.

The Gatekeeping Problem

A third threat is that companies can also manipulate or select the information being presented, as in the above-mentioned Facebook example (Kramer et al. 2014). This can be called the "Gatekeeping problem". Companies such as Google, as well as being a primary gatekeeper to information on the web, control vast quantities of data about individuals, but their main agenda is profits rather than the public good. Accordingly, there is a risk of conflicts arising between the goals of these companies and the public good. Information gatekeepers will have the ability to present information so as to create crises or stifle debate, depending on their interest or to influence the emotions of their users. This ability could allow them not only to influence public policy. If a company decided to invest in developing artificial intelligence (AI) or robotics, as Google is doing, they would, by presenting information in a certain way, be able to influence public policy. Criticisms of AI might not appear near the top of search results, whilst favourable articles about AI might be given great prominence. This is not to say that this is currently happening, but it is certainly possible that it or a similar scenario might occur in the future. Whilst there are other ways to access Internet information than to access Google (people can use a different search engine such as Bing, DuckDuckGo, or just typing the URL), if the site is running Google Analytics in the background, Google will be informed about the site being accessed. Real alternative ways to block Google from gaining this information would be to use some sort of Private OS (booted from a live distribution), blocking all Google Ads and Analytics attempts to track you, or using Tor or VPNs. It is not yet known whether such alternatives will be available in VRSNs. If VRSNs become the main gateway to online activity, the companies designing and controlling them will become the new gatekeepers.

Distortion of Knowledge

A fourth threat is that the design of VRSNs can distort knowledge. Threats to the information condition of autonomy might also arise in the design of virtual environments, especially if immersive virtual worlds (particularly those that operate as SNs) become dominant gateways to the online world. Online worlds can be

designed with colour schemes, or aesthetic patterns that are designed to make certain ideas appealing at the expense of others. One of the EU's REVERIE project's use-cases is a tour of a virtual European Parliament Building ("Objectives-REVERIE" 2014). The Parliament Building could be presented in myriad ways, each of which might have a subtle effect on how the visitor emotionally responds to it. A virtual world could portray the city of New York as a den of vice and iniquity or as a vibrant and fun place. Similarly, direct portrayals of ideas or peoples can be manipulated. The underrepresentation of ethnic minorities and of women in virtual worlds (to date) mirrors and possibly adds to discrimination in the real world. Another such issue is related to the virtual representation of the user. Artificial avatars that interact with users could be designed to influence those they interact with so as to manipulate or nudge the user towards accepting certain propositions or worldviews. An avatar might respond with a smile if asked about one political or religious idea, and frown when discussing another. Whilst the example is not subtle, these and similar designs will influence the way in which users in virtual worlds think about the information being presented to them. Artificial avatars would be all the more effective if they can access data about the user's emotional responses via eye-tracking or emotion capture.

Threats to Freedom

The most likely threats to freedom arising from the convergence of SNs and VR come from addiction, and from governments using information gathered from these technologies to limit freedom. A person cannot be said to be autonomous if they do not have a sufficient degree of freedom. The psychological harms that the development of the Internet, electronic games, online shopping and online worlds, etc., might create was a significant theme in discussions of the topic (Brey 1999; Gill 2008; Johansson 2009). Addictions and surveillance pose direct threats to autonomy

Addiction

A first threat is posed by addiction. Both SNs and VR have shown themselves to be potentially addictive. The convergence of both into VRSNs is likely to maintain the most appealing aspects of both VR and SNs (being able to see friends and keep in touch, whilst also being able to explore fantastically-designed immersive environments) making the VRSN potentially addictive. People with addictions cannot be considered to possess full autonomy. Users risk becoming addicted, losing touch with external reality (Cranford 1996; Gooskens 2010; Andreassen et al. 2012), developing bad social or behavioural habits (i.e. habits that might be rewarded in a virtual scenario but condemned outside of this virtual environment) that carry from their online behaviour to behaviour in the real world (Papagiannidis et al. 2008). The virtual world also facilitates some other addictions—for example, gambling and pornography are, with the Internet, available all the time. Thus, it is much more difficult for those with these problems to avoid temptation. There is also some discussion that frequent Internet use or SNs themselves might be addictive (Carr 2010). Developments such as eye-tracking and emotion capture greatly increase the

ability of engineers to create addictive online situations—the data gathered from eye-movements and facial changes will allow sites to respond and adapt to their users' wishes and emotional state, ensuring that their users spend more time on the site or in the virtual world.

Manipulation

A second threat is that VRSNs could be used to manipulate behaviour. Games that accustom players to certain norms have been developed. The US Army developed a game intended to promote enlisting, whilst jihadist groups (amongst others) are known to use SNs and YouTube for recruiting. It is conceivable that such games—using VR technologies, eye-tracking, emotion capture, and even brain-computer interfaces (BCIs)—would be able to influence players beyond the games by training them to respond in specific ways. Users of VR—particularly if VR headsets integrate BCIs—might be open to forms of brainwashing. Users might become more aggressive as a result of playing violent video games (Muñoz and El-Hani 2012). The degree to which this can be said to undermine a person's liberty will need to be determined by further empirical study. The recent controversial study conducted by Kramer et al. on Facebook users' emotional states illustrates that social networks can easily influence a person's mood. It illustrated that "emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness" (Kramer et al. 2014: 1) and that this contagion could take place on a massive scale via social networks. In short, it was found that if people saw more positive posts in their news feed (i.e. the stories, pictures, and videos they are shown, they would be more likely to post positive content themselves, and if they received negative posts in their newsfeed, they would be more likely to post negative stories. Furthermore, the terms and conditions of the social network were viewed as providing consent—the users affected had no knowledge that they were subject to this social science experiment.

Moreover, depending on how sophisticated emotional manipulation—via tracking of emotions, for instance—becomes in virtual worlds, certain programs could possibly manipulate a user's mood so that they behave in a certain way when offline, which, again, could reduce autonomy.

The Big Brother Scenario

A third threat is that information obtained from VRSNs could be used by governments to exert their power on users. Individuals might lose freedom as a result of the convergence between SNs and VR in other ways too. Governments can use the data they gather to influence individuals in selected ways, to promote certain courses of action and dissuade people from others. In some ways this is an extension of the issues associated with advertising and propaganda. If a person is constantly tracked, their activities monitored, their purchases registered and their physical and mental states frequently recorded, it is much easier to either manipulate them or to reduce their liberty. Rebelling or acting contrary to group norms in such a scenario would be practically far more difficult than it is currently.

This does not require governments to be malevolent. Governments may, unless they are careful, act on fluke results—fluke results that appear statistically significant. This is a problem that can be exacerbated by large datasets. If governments are using the data gathered from information and computer technologies (ICTs) to nudge their citizens in particular directions (c.f. the British Government's Behavioural Insights Team) that aims to encourage people to make better decisions for themselves and to inform public policy using insights from behavioural economics and psychology) but act on mistaken interpretations of the data or falsely perceived patterns, they could limit liberty without strong justification (Behavioural Insights Team 2014). Nudging in this fashion is not necessarily malevolent, but democratic oversight will still be required.

The issue of privacy discussed is also a concern here. The more privacy is eroded, the easier it will be for governments to curtail a person's liberty—governments will, if they choose, be better able to find out where a person is, what they are interested in, and who they communicate with. The deluge of data about individuals—whether it is the content integrally or data about the content (metadata)—is potentially a Trojan horse for an Orwellian dystopia. This knowledge will aid governments in curtailing liberty should they choose to do so. People involved in causes disliked by governments will be easier to identify and arrest: for instance, it was reported that the Ukrainian government of Victor Yanukovych texted protesters in Kiev's Independence Square in 2014 (Walker 2014). There is also an extreme scenario in which governments use the massive amounts of data that will be available to them to pre-emptively arrest those that assessments of the data (undertaken by individuals or by algorithms) deem likely to commit criminal acts. The LAPD is already using "big data" techniques to predict future crimes (Morozov 2013). The resemblance to Orwell's thought police is unsettling (Orwell 2013).

Self-Censorship

A fourth threat to liberty is the issue of self-censorship arising from the loss of privacy (Light and McGrath 2010; Coll et al. 2011). If people constantly feel that they are being watched, and begin to self-censor, they cannot be said to have full liberty. The perception of constantly being under-surveillance alters the conditions of liberty significantly—individuals would not risk saying certain things or acting in specific ways. Jeremy Bentham's prison—the Panopticon (Bentham 1995) in which an unseen observer was able to see every prisoner—will find a digital component when search, social, and entertainment converge. Within a VRSN, all actions will be recorded, just as all our activity on social networks is recorded. Thus, within VRSNs, users will be become accustomed to being under surveillance.

Threats to Authenticity

The threats to authenticity could come from increased peer pressure and expectation of conformity to group norms, from immersive VR tempting people away from real life, and from people's habits being governed by computerised guides. Authenticity—

the third key element of autonomy—might also be threatened by the convergence between SNs and VRs. Authenticity can be thought of as the degree to which a person acts according to their own will, and not simply because it is how "one" acts.

Social Conformity

The first threat is that of social pressure to conform to norms. Those who spend significant amounts of time on SNs will influence each other's norms and expectations of behaviour. This is almost certainly an issue where sexual behaviour is concerned with peer pressure regarding sexual behaviour being exacerbated via SNs. It must also be noted that VRs and SNs might allow people with unusual tastes to find others similar to them and that this might lead to greater tolerance for diverse tastes and behaviours (Soderlund 2008; Eichenwald 2013). However, the culture of certain online fora may also make it difficult for people to feel as if they are acting as their authentic selves as due to peer pressure, people feel as if they must conform (Vallor 2010). Even the settings in a VR or SN may solidify social norms—consider the range of options available when setting up user profiles. By necessity, a person must choose to represent their authentic being via a relatively narrow range of categories. The companies hosting VRSNs will, assuming that large numbers of people spend significant amounts of time in VRSNS, be capable of setting social norms that conform with their interests. Furthermore, the awareness that every action undertaken by an agent in an online world might be stored and recorded—might also become a threat to autonomy as people will be more likely to internalise group norms if they do not have a private space in which to develop their own selves. The ubiquity of SNs has made surveillance and self-surveillance part of everyday life. If VRSNs become extremely popular, it is likely that users will come to accept surveillance as a new norm.

The Quantified-Life

A second threat is that the data gathered by VRSNs could be used to instruct users how to behave in real-life. Consider loss of liberty might come from SNs alone—as technologies record more information about people and SNs encourage people to share that information—those that step outside the social norms risk ostracism and social opprobrium. As more and more data is gathered about individuals, they will be able to determine how much exercise they take each day, what they ate, how long they spent doing certain things, and so on. This data will be available for people to use in making decisions, guided by apps. There are obvious health benefits to this, but there is a risk that people will begin to live according to the diktats of technological guides (Sartor 2012). Central aspects of human life, from reading, to cooking, to exercise can be quantified and recorded; and technologies designed to instruct people in how to undertake these pursuits are being developed. Whilst such technologies will have many benefits, e.g. informing people of how much exercise they've taken, how many calories they've consumed, etc.; they might also be considered to diminish authentic living if people begin to live lives governed by technological diktats. There might exist greater pressure to conform to quantifiable

norms and less openness to the arbitrary aspects of daily life. As more of these experiences become subject to technological guides—apps, "smart" technologies, and autonomous artificial avatars—individuals may have less exposure to "real" life, thus diminishing the authenticity of their experiences. The "gamification" of normal activities could also be used to steer people in certain directions. Gamification is the phenomenon of using game techniques—i.e. awarding points and setting tasks—to encourage participants to achieve certain goals. In VRSNs it is likely that artificial avatars (i.e. types of AI) will be prominent. These artificial avatars could be extremely influential, acting as guardians policing all aspects of a person's life.

The Experience Machine

There is a third threat, namely that the convergence of VR and SNs further complicates our metaphysical assessment about what is real and what is not. Arguably, those living predominantly in a VRSN, would not be living in the real world, hence not living authentic lives. On top of this, the "Experience Machine" of Robert Nozick (1974: 42–45), is becoming more and more feasible: indeed an immersive VRSN would be quite similar to Nozick's experience machine (with the caveat that the user might be aware that they are in a VRSN). In this scenario, people have the choice to enter into the titular machine and live out their dreams in a virtual environment, never aware while they are inside that the experiences are not real. Nozick doubted that people would choose such an "inauthentic" life (Nozick 1974: 43). It is not impossible, however, that some people might find such a life appealing. The question of whether experiences in an online world should be considered real and authentic experiences is, however, an open one (Weckert 2002). From a phenomenological perspective, the conscious events one has inside the machine are as real as conscious events one has in the "real" world. If this is the case, the life in the machine is just as real as life outside the machine.

Shallowness

There is a fourth threat, namely that people might become "shallower" as a result of spending more time in VRSNs. Facebook is seen as enabling forms of communication that might result in "a bracketing of contextualizing and synthesizing activities that are at the core of critical engagement with the world" (Dubrofsky 2011: 112). People might read less substantive works, engage in political debate in a more vitriolic and less thoughtful way (or not at all), and otherwise lose their capacity and interest in taking part in the life of the society around them. It is possible that people might become so reliant on computers deciding things for them, that their own capacity for thought and decision-making might be diminished. VRSNs, being immersive, are likely to be extremely easy to spend time in; are likely to present information in a very immediate way that does not require a person to concentrate or spend time digesting. Indeed, it is plausible that people might find their real lives drab and banal in comparison with the idealised world available to them in a VRSN. This sort of society would resemble the world as described by

Huxley in *Brave New World* (Huxley 2013). With little exposure to "higher" culture, to great works of art and literature; and without the skills (and maybe attention spans) to enjoy them; people could be less able to engage with the world at a deep level. People without exposure to great works and ideas might find that they inner lives are shaped to a large degree by market-led cultural products rather than works of depth and profundity. This issue is controversial however; as it assumes that people with reduced access to, or interest in, great works of literature and art, in some way lack authenticity. Whilst this may not, ultimately, be a threat to authenticity, it might nonetheless be an unfortunate occurrence.

Tackling Strategies and Recommendations

Which are the best strategies available that will allow us to deal with the threats to privacy and autonomy raised by the convergence between SNs and VR? At first sight there seem to be three possible approaches: (1) a neo-Luddite approach, (2) a technophilic approach, and (3) an "Aristotelian" approach.

1. The neo-Luddite approach would mean abandoning the new and innovative VRNS technologies so as to preserve privacy and maintain autonomy to the largest possible degree. If we try and live off the grid, this would avoid many of the problems sketched above. This would necessitate people refusing to participate in VRSNs at minimum. A properly neo-Luddite approach would necessitate people leaving SNs and using ICT technologies less.
   However, on closer analysis this strategy seems neither desirable nor practical. It is clear that the digital revolution has brought with it many benefits, in terms of entertainment, socialising, and the capacity to research. One problem with this approach is, of course, that new ICTs, including both VR and SNs, are of immense usefulness and value. People enjoy being able to access information and entertainment quickly and easily: everyone from governments to researchers to children are able to access more information than ever before for whatever ends they deem worthwhile to pursue. There is no reason to suppose that VRSNs would not achieve similar levels of popularity. There are also huge economic benefits arising from these new technologies—the video game market is now larger than Hollywood (Correa 2013). If our ability to communicate would be diminished, we would lose access to huge amounts of knowledge, and we would have less entertainment. Another problem with this approach is that it would require top-down prohibition on the development of technologies already firmly embedded within society. Thus the neo-Luddite approach, although attractive because it most conclusively avoids issues with autonomy and privacy, is probably too impractical to be a serious option and maybe even ethically undesirable.
2. The technophilic approach would do the opposite, meaning that it would endorse adopting VRSNs irrespective of the costs to privacy or autonomy. It would probably mean giving up on privacy to a large extent as well as accepting the negative effects on autonomy, whilst profiting from all the advantages of the new Internet technologies.

This approach currently appears more prevalent—new technologies have often been adopted prior to consideration of either autonomy or privacy. There already exist prototypical VRSNs, such as World of Warcraft and Second Life, although this has been losing members (Newitz 2014)—there is little reason to think that new VRSNs will not emerge before societies have prepared legislation for them. The privacy debate has begun in earnest, though the threats to autonomy are less frequently discussed. These threats are subtler and less immediate—they will emerge incrementally. Furthermore, the concept of autonomy, although its value is quite concrete, is itself abstract; and it can be in conflict with more concrete concepts such as pleasure, entertainment, and efficiency. Living in a world without privacy and autonomy is not only undesirable but causing this state is immoral. Autonomy and privacy are extremely valuable as essential aspects of human life, so technologies that undermine them need to be approached with great care.

3. The "Aristotelian" approach would be to find a middle ground—a golden mean. This is referred to as the Aristotelian approach due to Aristotle's antipathy towards extremes and preference for a middle grounds. This would address both concerns of the neo-Luddite as well as the technophilic approach to avoid both the weaknesses and profit from the strongpoints of both strategies. This is the option we prefer. Since, neither extreme option appears desirable, we will adopt something of an Aristotelian strategy, and attempt to locate an appropriate mean, i.e. outline an approach to these difficulties that is proportional. Accordingly, the following recommendations are provided for policy-makers, providers of services, and users.

Recommendations for Policy-Makers

Policy makers have a duty to protect their citizens. Privacy is practically important to people and thus deserving of protection—it is, in addition, important for autonomy. Moreover, liberalism as a political philosophy aims to protect the rights of the autonomous individual. No liberal society can sanction the undermining of the autonomous individual and remain a liberal society. Insofar as individual autonomy and freedom are values that a society wishes to protect and uphold, it is incumbent on governments to protect these values. VRSNs pose challenges most obviously to privacy, but also, over a longer term, to autonomy. Thus it is imperative that policy-makers prepare for their emergence. In order for this to happen, serious thought will have to be given to emerging norms of relating to both the appropriateness of requesting and storing the data and the rights to distribute the data that will emerge from VRSNs—particularly data relating to people's physical bodies.

Legislation

As such, strong legal limits need to be placed on the sorts of information companies and government agencies can gather on individuals and on what they can do with

that information. Laws and regulations are required in order to ensure that (a) the powers of government agencies and private companies are strictly limited in relation to accessing information,[4] (b) users of the technologies know when their privacy might be threatened, i.e. it should be obvious when a camera or recording device is activated, and (c) that companies provide opt-out policies for their users. Legislation to ensure that VRSNs provided users with the ability to alter settings so as to maintain associational privacy might be considered. Legislation might also be required to prevent the direct manipulation of users of VRSNs and to regulate and prevent the emergence of new addictions. Providing incentives to encourage the creation of secure networks, online environments, and other digital technologies that will protect people's autonomy and privacy, or provide individuals with the means to protect themselves is necessary. This could be achieved by making certain breaches of privacy and threats to autonomy illegal or by providing funding for companies, tech developers and research groups to develop technological means of protecting privacy and autonomy. Previously, the development of to peer-to-peer networks for content sharing (e.g. Napster) stimulated increased research into digital watermarking (or Digital Rights Management) and audio/video fingerprinting. The development of analogous technologies for avatars and immersive worlds might go some way towards ensuring that only the genuine owner of an avatar can use it.

The EU is considering a new legal framework for the protection of personal data. This would include a proposal for a regulation of the European Parliament regarding the processing of personal data and the free movement of that data.

Contracts

Policymakers will need to examine the sorts of contracts being offered to users of VRSNs technologies and analyse the fairness of these contracts, particularly in relation to the protection of autonomy and privacy. This will be one of the keys in setting the new and appropriate privacy norms. A choice offered to an addict or to someone unaware of the deeper implications of this choice is not a fair choice. Users, in their eagerness to use the service, will accept the terms and conditions, particularly if they have already built use of the service into their daily lives. This means they are unlikely to consider the terms of the contract, a condition exacerbated by contracts often being written in technical language, meaning they may not understand it. This is very illustrated by Facebook's terms and conditions were considered to be consent for the emotional-contagion research experiment (mentioned above). Finally, users are not required to consider the wider societal implications of the rights they give up when agreeing to these contracts. Therefore,

[4] The EU has been active in these areas, e.g. a proposed directive of the European Parliament on the protection of individuals regarding the processing of their data by authorities security or criminal purposes (Commission 2012). See also the "right to be forgotten" ruling that makes internet search engine operators responsible for the processing that they carry out of personal data which appear on web pages published by third parties (Skouris et al. 2014).

the rights of companies providing these technologies to create contracts that lay claim to such intimate information must be questioned.

Transparency

Similarly, users should be alerted to what sort of digital footprint they are leaving in a VRSN and who will be able to see it. Ensuring that individuals can see that data about them, and remove it, would also be desirable. This should also apply to data about a person's physical self. This will be of the utmost importance if realistic real-time representations become the norm in VRSNs. Real-time representations of people will gather a great deal of information about people—users should be permitted to access this information. Many of these bodily actions might not be intentional meaning that the storing of data about bodily activity therefore would be storing information about a person, which they are neither conscious of nor responsible for. Promoting open-source software, so that users can see whether there exist backdoors for security agencies, could be considered, though this is unlikely to benefit many (possibly most) users, who are unlikely to have the expertise to assess the safety of the software they are using. Nonetheless, this would be of benefit to those with coding literacy.

Research Funding

Research funding bodies need to be made aware of the threats to privacy and autonomy and the ways in which VRSNs will exacerbate these threats. Funding could be conditional upon addressing these threats in some ways. Governments and funding bodies that value privacy and autonomy might aim to fund technological developments that would protect people's privacy and ensure that autonomy is not threatened. Governments might also consider funding of alternatives to Google, Facebook, and Yahoo—the providers of nominally free services that gather data on individuals. Governments that value autonomy and privacy could, in theory, provide alternatives that performed the same services, e.g. free email, but that did not gather data on users and thus protected autonomy and privacy. If users trusted the governments (which would ideally be subject to democratic oversight), they would have an alternative to the products of large companies only beholden to shareholders.

Education

Governments will need to ensure that their citizens are educated regarding the threats posed by VRSNs. With education users will be able to make informed choices regarding how they interact online and what sort of information they are willing to reveal. Given that many people are likely to begin to make use of VRSNs at a young age, lessons relating to the threats posed by VRSNs may need to be incorporated into school systems. People should also be educated regarding their legal rights

Recommendations for Providers

Data Protection

Providers of VRSNs will need to ensure that people's data is protected, e.g. adequately encrypted at all times during storing and use. Providers will need to demonstrate that they will protect their users from government prying. In order to maintain the trust of their users, transparency ought to be the norm. Permitting users to access the data held about them, and to delete this data should the user choose to do so, would help users trust the providers. The provision of clear privacy policies, store information securely, avoid releasing information about others, and minimise the amount of personal information in the possession of corporation offering VR and SNs. Beyond this, there may be economic opportunities for providers to create means of protecting people's privacy and securing their information (at least if people begin to take their online privacy more seriously).

Transparency

Transparency in relation to the results provided by search features, and the design choices made by VRSNs would help avoid the "gatekeeping problem". VRSNs should include settings that allow users to determine who they wish to include and exclude from certain social circles. Providers (including designers) of online environments will also need to be aware of the potential to include unconscious biases in their designs.

Avoiding Filter Bubbles and Cyberbalkanization

Providers of VRSNs should also aim to avoid filter bubbles and cyberbalkanization. To this end, a move away from personalisation and back towards "objective" gatekeepers would be desirable. The algorithms providing the "objective" guidance, be it search results or an autonomous avatar, should be transparent and available for democratic oversight. Unfortunately, while this would help avoid filter bubbles and cyberbalkanization (to some degree) and thus protect autonomy, it runs up against the economic interests of these companies. In specific instances of VRSNs, such "objectivity" may not be possible.

Encryption Services

There may be economic opportunities for providers to create means of protecting people's privacy and securing their information, e.g. selling technological means to allow people to encrypt data. End-to-end encryption that protects people's correspondence, cloud services that encrypt all data with individual keys, might become very desirable for companies and citizens wishing to protect their privacy, though will do nothing to avoid the use and selling of mass data arising from other accessible sources. Moreover, there is a risk that with end-to-end encryption if a

user loses their key, they will lose the ability to access all their data. However, this would not resolve the threats to autonomy arising from mass-data.

Recommendations for Users

Avoid the Technology

The convergence of SNs and VR will threaten privacy in society, with serious implications for autonomy. The simplest and most efficient way to avoid these problems is to avoid or minimise interaction with the technology. Users interested in privacy could also use software that blocks cookies, trackers, and so on. Citizens who value autonomy and privacy—both personally and for its social importance—might avoid using services that will undermine these values. If autonomy is utterly undermined, people will not be free to pursue any other goals they might normally have valued. However, unless a majority of users avoid allowing their data to be accessed, even those who do value their privacy will be at risk due to the losses of associational privacy, and the gathering of big data. However, in our scenario, in which VRSNs occupy a social space akin to Facebook or LinkedIn, avoidance will not be an option for many.

Awareness

If avoidance is not a viable or desirable option, citizens need to be aware of the potential to be manipulated and misinformed. Given that many of the changes to privacy are unlikely to be halted, with consequent impacts on autonomy, people need to be informed about what others can know about their future actions. People should carefully analyse the contracts they are signing when joining VRSNs, examine changes to terms and conditions, and take care in what personal information they reveal. Citizens still have the power to sets new norms of appropriateness and distribution of private information in VRSNs.

Consumer Action

If governments and corporations neglect their responsibilities for protecting privacy and autonomy, this responsibility for protecting privacy then might fall on users, those that wish to avoid invasions of physical privacy can resort to technological solutions, both low and high tech. Low-tech solutions might mean physically blocking cameras on phones or computers to ensure privacy; whilst high-tech solutions would involve using hardware or software to block potential invasions of physical privacy. Users might also consider paying for services currently provided by large tech-companies, i.e. buying encrypted VRSNs similar to how they can choose encrypted email services. For instance, mailbox.org, houses its servers in Berlin and thus is subject to the strict German laws on data protection. In short, citizens can reward companies and services that value the protection of privacy and autonomy and punish those that do not.

Conclusion

We have outlined the threats to privacy and autonomy arising from the convergence of SNs and VR—focusing on informational privacy, physical privacy and associational privacy and on the information, the freedom, and authenticity. These were further subdivided into specific threats/problems arising from VRSNs. The threats to privacy were as follows: the vulnerability of data problem and the misuse of data problem (threats to informational privacy), the prevalence of recording devices problem, the unintended revelation of informational problem, and the loss of anonymity problem (threats to physical privacy), the socialising problem and the global village problem (threats to associational privacy). The threats to autonomy were as follows: the filter bubble problem, the cyberbalkanization problem, the gatekeeping problem, and the distortion problem (threats to the knowledge condition of autonomy), the addiction problem, the manipulation threat, the government threat, and the self-censorship threat (threats to the freedom condition of autonomy), and the social conformity threat, the quantified life problem, the experience machine problem, and the shallow threat (threats to authenticity condition of autonomy). The threats to privacy are well known and serious; whilst those to autonomy are less-well known but equally as profound. Moreover, it is suggested that the threats to privacy themselves may in fact constitute a threat to autonomy, as people might become used to a life under surveillance.

This is not to say that the development of the technology needs necessarily to be curtailed. Whilst these problems are serious, they might not be insurmountable. More research is no doubt needed to determine the full extent of the ethical problems associated with VRSNs and to develop appropriate responses to their emergence. We have provided a preliminary sketch of the broad options available to society at large and provided specific recommendations for policy-makers, providers, and users of these converging technologies. It is in the long-term interests of all three groups of people to protect people's privacy and guarantee their autonomy. All three groups are likely to need to work in harness to ensure that people retain control over the development of technologies that ought to serve us rather than determine how we interact.

Acknowledgments The research leading to these results has received funding from the European Community's Seventh Framework Programmes (FP7/2007-2013) under Grant Agreement No. ICT-2011-7-287723 (REVERIE project).

References

Allen, A. (2011). Privacy and medicine. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2011). Retrieved from http://plato.stanford.edu/archives/spr2011/entries/privacy-medicine/

Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. (2012). Development of a Facebook addiction scale. *Psychological Reports, 110*(2), 501–517. doi:10.2466/02.09.18.PR0.110.2.501-517.

arXiv, E. T. F. (2012). *Evidence emerges that Iran is building its own hidden internet*. Retrieved March 31, 2014 from http://www.technologyreview.com/view/429447/evidence-emerges-that-iran-is-building-its-own-hidden-internet/

Barrett, D. (2013). *One surveillance camera for every 11 people in Britain, says CCTV survey*. Retrieved from http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

BBC News. (2012). *Facebook party invite sparks riot in Haren, Netherlands*. Retrieved March 31, 2014 from http://www.bbc.co.uk/news/world-europe-19684708
BBC News. (2014a). *Facebook attacked for emotion study*. Retrieved June 30, 2014 from http://www.bbc.com/news/technology-28051930
BBC News. (2014b). *Turkey "blocks YouTube access."* Retrieved March 27, 2014 from http://www.bbc.com/news/world-europe-26773702
Behavioural Insights Team. (2014). Retrieved February 26, 2014 from https://www.gov.uk/government/organisations/behavioural-insights-team
Bentham, J. (1995). *The panopticon writings*. London: Verso.
Birky, I., & Collins, W. (2011). Facebook: Maintaining ethical practice in the cyberspace age. *Journal of College Student Psychotherapy, 25*(3), 193–203.
Brey, P. (1999). The ethics of representation and action in virtual reality. *Ethics and Information Technology, 1*(1), 5–14. doi:10.1023/A:1010069907461
Brey, P., & Søraker, J. H. (2009). Philosophy of computing and information technology. In M. Anthonie (Ed.), *Philosophy of technology and engineering sciences* (pp. 1341–1407). Amsterdam: North-Holland. Retrieved from http://www.sciencedirect.com/science/article/pii/B9780444516671500513
Buss, S. (2008). Personal Autonomy. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2008). Retrieved from http://plato.stanford.edu/archives/fall2008/entries/personal-autonomy/
Cadwalladr, C. (2014). Charlotte Laws' fight with Hunter Moore, the internet's revenge porn king. *The Guardian*. Retrieved from http://www.theguardian.com/culture/2014/mar/30/charlotte-laws-fight-with-internet-revenge-porn-king
Cameron, D. (2014). *CeBIT 2014: David Cameron's speech—Speeches—GOV.UK*. Retrieved April 10, 2014 from https://www.gov.uk/government/speeches/cebit-2014-david-camerons-speech
Carr, N. (2010). *The shallows: How the internet is changing the way we think, read and remember*. London: Atlantic Books.
Cellan-Jones, R. (2014). *Facebook buys the future*. Retrieved March 27, 2014 from http://www.bbc.com/news/technology-26746694
Coll, S., Glassey, O., & Balleys, C. (2011). Building social networks ethics beyond "privacy": A sociological perspective. *International Review of Information Ethics, 16*, 47–53.
Commission, E. (2012). *Proposal for a regulation of the European Parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)*. European Commission. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF
Correa, C. (2013). *Why video games are more addictive and bigger than movies will ever be*. Retrieved Feb 23, 2014 from http://www.forbes.com/sites/christophercorrea/2013/04/11/why-video-games-are-addictive-and-bigger-than-movies-will-ever-be/
Cranford, M. (1996). The social trajectory of virtual reality: Substantive ethics in a world without constraints. *Technology in Society, 18*(1), 79–92. doi:10.1016/0160-791X(95)00023-K
Dubrofsky, R. E. (2011). Surveillance on reality television and Facebook: From authenticity to flowing data. *Communication Theory, 21*(2), 111–129.
Duhigg, C. (2012). How companies learn your secrets. *The New York Times*. New York. Retrieved from http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0
Eichenwald, K. (2013). Facebook leans. In *Vanity fair* (May). Retrieved from http://www.vanityfair.com/business/2013/05/facebook-future-mark-zuckerberg-sheryl-sandberg
Expected Results-REVERIE. (2014). Retrieved from http://www.reveriefp7.eu/project/expected-results/
Facebook Newsroom. (2014). *Company Info\Facebook newsroom*. Retrieved from http://newsroom.fb.com/company-info/
Ford, P. (2001). A further analysis of the ethics of representation in virtual reality: Multi-user environments. *Ethics and Information Technology, 3*(2), 113–121.
Gill, S. (2008). Socio-ethics of interaction with intelligent interactive technologies. *Ai & Society, 22*(3), 283–300. doi:10.1007/s00146-007-0145-y
Gooskens, G. (2010). The ethical status of virtual actions. *Ethical Perspectives: Journal of the European Ethics Network, 17*(1), 59–78.
Gotterbarn, D. (2010). The ethics of video games: Mayhem, death, and the training of the next generation. *Information Systems Frontiers, 12*(4), 369–377. doi:10.1007/s10796-009-9204-x
Griffin, J. (2008). *On human rights*. Oxford: Oxford University Press.
Huxley, A. (2013). *Brave new world*. London: Everymans.

Internet of Things: The Future of Business Technology|Microsoft. (2014). Retrieved July 23, 2014 from http://www.microsoft.com/windowsembedded/en-us/internet-of-things.aspx

Johansson, M. (2009). Why unreal punishments in response to unreal crimes might actually be a really good thing. *Ethics and Information Technology, 11*(1), 71–79.

Karmali, L. (2013). *World of Warcraft down to 7.7 million subscribers*. Retrieved April 22, 2014 from http://ie.ign.com/articles/2013/07/26/world-of-warcraft-down-to-77-million-subscribers

Kaupins, G., & Park, S. (2011). Legal and ethical implications of corporate social networks. *Employee Responsibilities and Rights Journal, 23*, 83–99.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), 5802–5805. doi:10.1073/pnas.1218772110

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massivescale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 201412469. doi:10.1073/pnas.1320040111

Light, B., & McGrath, K. (2010). Ethics and social networking sites: A disclosive analysis of Facebook. *Information Technology & People, 23*(4), 290–311. doi:10.1108/09593841011087770

Locke, J. (1689). *The second treatise of government* (3rd ed.). Oxford: Blackwell.

Lory, B. (2010). *Using Facebook to assess candidates during the recruiting process: Ethical implications.* NACE Knowledge Centre.

Mill, J. S. (1859). *On liberty*. London: Penguin.

Morozov, E. (2013). How Facebook could get you arrested. *The Guardian*. Retrieved from http://www.guardian.co.uk/technology/2013/mar/09/facebook-arrested-evgeny-morozov-extract

Muñoz, Y. J., & El-Hani, C. N. (2012). The student with a thousand faces: From the ethics in video games to becoming a citizen. *Cultural Studies of Science Education, 7*(4), 909–943. doi:10.1007/s11422-012-9444-9

Newitz, A. (2014). *Is second life about to become a ghost world?* Retrieved June 26, 2014 from http://io9.com/is-second-life-about-to-become-a-ghost-world-1594324051

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy, 17*(5–6), 559–596.

Nozick, Robert. (1974). *Anarchy, state and utopia*. Oxford: Blackwell.

O'Dwyer, D. (2014). *Why Facebook founder had to buy WhatsApp*. Retrieved July 23, 2014 from http://www.irishtimes.com/news/technology/gadgets/why-facebook-founder-had-to-buy-whatsapp-1.1700459

Objectives-REVERIE. (2014). Retrieved from http://www.reveriefp7.eu/project/objectives/

Orwell, G. (2013). *1984*. London: Penguin.

Papagiannidis, S., Bourlakis, M., & Li, F. (2008). Making real money in virtual worlds: MMORPGs and emerging business opportunities, challenges and ethical implications in metaverses. *Technological Forecasting and Social Change, 75*(5), 610–622. doi:10.1016/j.techfore.2007.04.007

Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. London: Penguin.

Parsell, M. (2008). Pernicious virtual communities: Identity, polarisation and the Web 2.0. *Ethics and Information Technology, 10*(1), 41–56. doi:10.1007/s10676-008-9153-y

Sartor, G. (2012). Human rights in the information society: Utopias, dystopias and human values. In C. Corradetti (Ed.), *Philosophical dimensions of human rights* (pp. 293–307). Netherlands: Springer. Retrieved from http://www.springerlink.com/content/q731672287x354m2/abstract/

Skouris, V., Lenaerts, K., Ilešič, M., Bay Larsen, L., von Danwitz, T., & Safjan, M. (2014). *Case C-131/12. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Grand Chamber May 13, 2014).

Soderlund, G. (2008). Journalist or panderer? Framing underage webcam sites. *Sexuality Research and Social Policy, 5*(4), 62–72. doi:10.1525/srsp.2008.5.4.62

Talbot, D. (2013). *Moto X and other smartphones are set to listen to their environments all the time*. Retrieved May 3, 2014 from http://www.technologyreview.com/news/517801/the-era-of-ubiquitous-listening-dawns/

Timberg, C., & Nakashima, E. (2013). FBI's search for "Mo," suspect in bomb threats, highlights use of malware for surveillance. *The Washington Post*. Retrieved from http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story_2.html

Tomkins, M. (2014). *New face recognition algorithm knows you better than you know yourself*. Retrieved from http://www.imaging-resource.com/news/2014/04/23/new-face-recognition-algorithm-knows-you-better-than-you-know-yourself

Vallor, S. (2010). Social networking technology and the virtues. *Ethics and Information Technology, 12*(2), 157–170. doi:10.1007/s10676-009-9202-1

Wakefield, J. (2014). *Heartbleed: Do you need to worry?* Retrieved April 11, 2014 from http://www.bbc.com/news/technology-26969629

Walker, S. (2014). Text messages warn Ukraine protesters they are "participants in mass riot." *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

Weckert, J. (2002). Lilliputian computer ethics. *Metaphilosophy, 33*(3), 366–375.

Zuckerberg, M. (2014). *I'm excited to announce that we've agreed to acquire Oculus VR, the leader in VR technology*. Facebook.com. Retrieved March 27, 2014 from https://www.facebook.com/zuck/posts/10101319050523971