

Social Gamers' everyday (in)visibility tactics: playing within programmed constraints

Michele Willson^{a*} and Katharina Kinder-Kurlanda^b

^a School of Media, Creative Arts and Social Inquiry, Curtin University, Perth, Australia; ^b Data Archive for the Social Sciences, GESIS Leibniz Institute for the Social Sciences, Cologne, Germany

^{a*}Professor Michele Willson, School of Media, Creative Arts & Social Inquiry, Curtin University, GPO Box U1987, Perth, Western Australia, Australia 6845. Email: m.willson@curtin.edu.au

.As continual scandals around internet data collection, manipulation and dissemination (the Snowden disclosures, the Facebook emotion contagion research and more recently, the Cambridge Analytica revelations) have made resoundingly apparent, activity online – because it is online – can be mapped, managed and manipulated. How well everyday users understand and manipulate the possibilities, constraints and imperatives of the programmed environments within which they operate may be able to be discerned through a closer examination of actions within the sphere of social game play.

We are interested in how gamer awareness of programmed requests to engage, divulge information, connect to other users alongside broader privacy concerns are navigated and translated into specific tactical behaviours and choices. Drawing together results from literature reviews and a qualitative online questionnaire, we discuss the everyday practices of social gamers in their interaction with games as algorithmic, programmed spaces. What is apparent from our discussion is that social games offer a multi-faceted microcosm for a closer analysis of the nuanced interplay of algorithms, data acquisition management and player visibility tactics understood in a broad sense.

Keywords: privacy; everyday; social games; data; algorithms; players; Facebook

Introduction

Capacities to trace, track, record, aggregate and manipulate online environments and activities are extensive and are becoming increasingly sophisticated. As the scandals surrounding the NSA and Snowden disclosures, the Facebook emotion contagion research publication and more recently the Cambridge Analytica revelations have made resoundingly apparent, activity online – because it is online – can be mapped, managed and manipulated by system actors through the programmed environment within which that activity takes place. However, this is not to assert that there is no flexibility within these coded, programmed spaces or that all outcomes are necessarily preordained. Instead there are a range of possibilities for the user to employ

inside these spaces: capacities for tracking depend on the choices users make within the constraints of programs or platforms, the types of activities they employ and their decisions as to what activities to undertake and how they do so in the first place. These are complex and multifaceted decisions that are informed by a range of reasons, too complex and varied to describe simply and often too convoluted to be able to discern by simple observation or to categorise into a particular schema. Some insight into how well everyday users understand the possibilities, constraints and imperatives of the environments within which they operate may be able to be discerned through a closer examination of actions within the sphere of social game play.

In this paper, we examine the everyday practices of social gamers in their interaction with games as algorithmic, programmed spaces (Galloway, 2006) with a particular focus on what we refer to as visibility tactics. We employ Michel de Certeau's (1984) notion of tactics and strategies as a way of framing the discussion of player actions within social games: Games on computers, mobile phones or tablets intend to engage users and to encourage particular user behaviour, often over long periods of time, using various strategies and enabling the collection and analysis of user data. These analyses are performed by simple or complex algorithms. We are interested in how gamer awareness of programmed requests to engage, divulge information, or connect to other users alongside broader privacy concerns are navigated and translated into specific tactical behaviours and choices.

Through the use of an online questionnaire, and drawing on relevant literature, we investigated the practices of social gamers - with a focus on social casual games - in terms of their management of their (in)visibility. By player visibility tactics, we are referring to the actions taken by game players that render them more or less visible (identifiable, recordable, trackable, notable) to others; whether the 'audience' is/are the data system/s, providers, technology, other individuals, or social networks. We consider these practices as tactics for managing player visibility, in the sense of managing data privacy and impression management.

Social, casual or mobile?

Jesper Juul (2010, p.5) describes casual games as 'games that are easy to learn to play, fit well with a large number of players and work in many different situations.' Most of the so-called social games fall into the category of casual games (causing confusion around terminologies). Wohn, Lampe, Wash, Ellison and Vitak (2011) observe that the definition of these games is determined more by the technical aspects of how they are accessed and distributed, not on the genre; there are in fact many different genres of social casual games 'including board, word, simulation, arcade, role-playing, and action games.' (2011, p. 3). Popular game examples include Hay Day, and the various Candy Crush Saga and FarmVille games. For the sake of brevity, we therefore refer to these games as social games throughout this paper, while recognising that games are frequently straddling various categories simultaneously.

Social games have a range of particular characteristics that differentiate them from more traditional and subscription-based console games. Some of the more notable attributes include game interruptibility, requiring low levels of player technical and game skill competencies,

freemium economic payment models and a focus on encouraging player networks either directly in the game or through linking to SNS platforms. Interruptibility means that gameplay can be interrupted, episodic and played in short bursts in ways that enable playing in moments of the everyday more easily: while waiting for something to finish, between tasks and so forth (Kinder-Kurlanda & Willson, 2016; Juul, 2010). Games can be played on a number of devices both stationary and mobile. The portability of mobile devices (mobile phones, ipads and other tablets) enables players to play in a multitude of locations and throughout the day whereas stationary devices such as PCs require the user to be located in a specific place.

Indeed, this is one of the reasons that social games are so interesting as a focus of analysis: they have been rapidly adopted by a diverse range of people who incorporate their game play in and around their everyday activities. Playing these games has become a commonplace, everyday activity. People play while on the bus, while sitting on the couch or while waiting for a doctor's appointment: in other words, they take opportunities to grab short periods of time to fill with game play in and around (and sometimes during) the other often mundane activities taking place.

(In) visibility tactics in programmed spaces

Social games are enacted as highly programmed spaces with very limited, specific actions available to players alongside the capacity for game developers, program designers and platform providers to observe, and extract player data and in turn to manipulate player behaviour. In terms of the game itself, as the researchers found in their own gameplay, programming includes a range of play mechanisms such as imposing a limit on the number of particular actions that can be undertaken, or a particular number of lives available, in one play session; limited social interaction possibilities; asynchronous play; and programmed timed actions that require player attention in an intermittent but ongoing manner (for example, crops take different times to grow and need to be harvested at certain times or they wither). Game activity is also limited to specific tasks such as harvesting crops, purchasing seeds or game items, giving gifts or selling produce, for example, in the case of Farmville, or to swapping coloured game pieces to make particular combinations in Candy Crush. Social games frequently also involve (or even require) playing with others in a player's social network or they can be linked to an SNS to enable competition and sharing options across an individual's social network. These opportunities and constraints require the player to make conscious decisions throughout their engagement with the game: who they may invite or link to, what platforms they will access the game through, what profile they will use, where they choose to advertise their achievements and when. Such choices can be seen as tactics applied to the player's managed visibility within and across the game and social space.

Social games have attracted considerable media attention for how they have been used as a mechanism to capture large amounts of data on individual players, on their online practices and on their social network activities and contacts. Even before the game is played, the game program needs to be chosen, downloaded, terms of use agreed to either implicitly or by default (through accessing the game through a social network site (SNS), see Willson & Leaver, 2015),

and the release of a range of information to third parties approved. These games have also been notable for employing a range of cross-advertising and spamming strategies within the games but also with activity extending out to a player's broader social network through advertising and offers posted to the player's broader social network (Willson & Leaver, 2015). For example, game achievements can be posted to a player's social profile (outside of the confines of the game). Similarly, leaderboards can be established by linking the specific game app with a SNS account. These possibilities extend the game activity to broader audiences and locations. With the scale of player activity and the number of people playing, social games become an important source of and opportunity for data extraction and analysis.

The social game environment therefore is a complex media ecosystem with a range of stakeholders: they all have different but intersecting interests, claims and involvement in the game play. These stakeholders include the players themselves, their social networks, the developers and game providers, the platforms, the advertisers, the software that manages the play and the algorithms that harvest, combine and manipulate the data generated as a result of downloading and playing the game.

In this paper, we distinguish between the game software and algorithms for heuristic reasons. Following Gillespie (2014, p. 167) we define algorithms as 'encoded procedures for transforming input data into a desired output, based on specified calculations'; in this paper, this primarily refers to the particular outcome of collecting, aggregating, analysing and displaying user data gathered through game activity and engagement so that it becomes possible to profile players, to rank topics, to make players visible to other players and eventually to shift player attention. This differentiation by intent allows us to highlight the strategies – in the sense employed by de Certeau (1984) – implemented by various system actors and the tactics that players employ to make themselves (in)visible. This will be explained in more detail below.

While there has been considerable attention to users' interactions with (game, and other) software and programmed spaces (e.g. Scacchi, 2010; Sotamaa, 2010), more recently, researcher attention has expanded to include a specific focus on algorithms as technical artefacts used to process large amounts of data (e.g. Diakopoulos & Koliska 2016; Kitchin, 2017). For players, it may or may not be apparent which actors or which technology they are dealing with in a specific situation: the differences between notifications of the device, app or SNS, for example, are sometimes hard to discern. When faced with a specific game event it is also difficult to understand what aim the programmers had when they made certain decisions – a feature such as a special game event may have been introduced for various or multiple aims: allowing advancement in the game, motivating players to link to Facebook or to invite friends to play, promoting pay-for features etc.

Beer (2009) mentions three areas for empirical studies of social media: the organizations of social media providers; software infrastructure and their applications on the web; and how these play out in the everyday lives of those using (or not using) participatory web-applications. This third area considers 'how and why individuals divulge information about themselves, how they play with and within the boundaries of the software, how they react to and resist the impulses written into the codes' (Beer, 2009, p. 998); it is this area that we are interested in here.

In our study, we investigated what sort of understandings game players have of their visibility and how they manage visibility/ies across the ecosystem that circulates around games: the actions taken by game players that render them more or less visible (identifiable, recordable, trackable, notable) to others; whether the 'audience' is/are the data system/s, providers, technology, other individuals, or social networks.

In an article exploring the Facebook newsfeed algorithm's privileging of certain characteristics, Taina Bucher (2012, p. 1165) notes that new modalities of visibility are enabled by algorithmic and software processes. According to Bucher,

the media participate in configuring the visible as oscillating between what can and should be seen and what should not and cannot be seen, between who can and cannot see whom. Examining new modalities of visibility becomes a question of how rather than what is made visible, through which specific politics of arrangement, architecture and design.

Algorithms render particular things more or less visible. The fact that social media users are cognisant of algorithmic practices and also of ways in which to manipulate them (even if largely intuitively, given the proprietary nature of many algorithms) in order to minimise or maximise their visibility has been noted elsewhere. Tufekci (2014), for example, showed how social media users adapt their practices on the basis of experiences with algorithmic agency using the example of Twitter trending topics. Tufekci (2014) describes how the announcement of the publication date of a specific hashtag in advance led to the hashtag being re-tweeted by thousands of Twitter users thus generating a spike to which Twitter's trending algorithm reacts.

Such practices are complex because 'cultures of circulation' emerge as the algorithms adapt to user behaviour and users in turn adapt to the results of algorithmic analyses (Beer & Burrows, 2013). Data that feeds into algorithms changes the results of algorithmic calculations, which are then shown to users who may change their behaviour; additionally those who maintain algorithms may adapt and tweak them depending on experiences with users and the platform. This is particularly relevant in social games where developers continually monitor and refine game design according to monitored player behaviour (Willson & Leaver, 2015).

In his discussion of everyday life practices, de Certeau (1984) notes how tactics are commonly employed by people (in their capacity as consumers, readers, audiences, pedestrians, and so forth) in order to shape or influence constrained environments (e.g. technical, economic, political systems) and practices. Tactics are described as practices of resistance and appropriation enacted against the strategies of (seemingly) larger and more powerful systems and actors. In our discussion, these strategies refer to the practices of game developers; companies such as Facebook; other actors who may utilize user data; and the broader capitalist system that generates value from data gleaned from players' everyday activities.

When looking at social games, it can be suggested that game players (the consumers/users) enact tactics as a way of customising, and working within the constraints of the game and SNS' strategies and relatedly, with the algorithms that are enacted as part of these strategies. Some of these tactics may be discerned through an examination of how game players render themselves more or less visible to the game, other players, social networks, third parties and so forth. We set out to examine Australian and German social game play in order to identify player tactics of situated algorithmic management in their everyday.

The study

An online questionnaire (using the SurveyMonkey platform) was compiled in English and in German and distributed by both researchers through their online networks (e.g. Facebook profile, Twitter, listservs, university staff list, etc). A snowball distribution method was decided as the most appropriate way to locate participants given the nature and location of the research, and the challenges of identifying a wide range of online social game players.

Participants were asked to complete a short online questionnaire on social games and the player visibility tactics that they might employ. They were also asked to distribute to others: friends, family, colleagues. Social games were explained as online games played through social network sites such as Facebook or GooglePlus where players interact in the game with family or friends. Games such as Farmville 2, Sims Social, Candy Crush or Words with Friends were listed as examples of social games, but the information sheet also explained that there are many other games that also fit this description. The survey was open for a period of roughly 3 months (15/08/2016- 07/11/2016) and it received a total of 111 responses (74 through the Australian survey; 37 through the German).

The survey consisted of 35 multiple choice or ranking questions, and the possibility to add text comments after some of the questions. Both researchers played a range of games prior to the questionnaire construction and dissemination. Their experiences and understanding of play mechanisms and environment helped to shape the questions asked and the framing of the discussion below. A series of demographic questions were posed as well as questions relating to where people play, what might inform their decision to download a game or to link it to their SNS account, when they might play games and with whom. Respondents were asked questions about concerns around privacy and use of privacy settings in order to garner a sense as to different player awareness of information sharing and the visibility of personal information online. They were also asked to explain some of the steps they might take as a way of managing their visibility and why.

While the survey was distributed through local networks in Germany and Australia, the respondents were from a range of locations including Mauritius, UK, Germany, Austria and Australia. Australian respondents ranged in age from 18-70 with the majority of respondents falling within the 21-30 age range (44.59 %). The remaining cohort spread across 18-20 (2.7%), 31-40 (21.62%), 41-50 (17.57%), 51-60 (10.81%) 61-70 (2.7%).

About 18% of the German respondents chose not to provide any demographic information. Of those who did fill in these details, most (ca. 38%) were between 21 and 29 years old. About 16% were between 30 and 39, ca. 29% between 40-49 and ca.17% were 50 or older. Roughly 40 % of the respondents in the German survey who provided demographic information were male and 60 % female.

Similar patterns can be seen with the Australian respondents with more female respondents and quite high levels of education. Of the Australian respondents, roughly 57% were female, and 42% male with 1 respondent skipping the question (they did not select a response including other or prefer not to specify). With regard to educational qualifications, Australian respondents were quite well educated with more than 81% respondents having a university degree, and almost all of the remainder having completed high school or vocational training.

In the German survey players also were well educated; roughly 60% of those providing demographic information had obtained at least a university degree and a further 6% had a degree from a university of applied science. Almost all others had at least finished higher secondary education.

Of the total respondents in both the German and Australian questionnaire, 62 respondents identified as playing social games (2 other respondents were unsure so have been excluded from the discussion below). The remainder of this discussion is focussed on these self-identified game player responses and behaviours.

The questionnaire was an exploratory exercise to uncover a range of player visibility tactics and to identify research questions: the responses were too small to be statistically representative or significant. The smaller number of German respondents also meant that broader direct comparisons between the two cohorts was not possible. The intent, therefore, in the discussion below is not to generalise questionnaire findings to all social game user practices; instead the data is used to highlight some of the different, more nuanced ways in which players understood the online environment in which they were operating (for example, the use of privacy setting or choice of platform) and the choices they might make within programmed constraints (for example, whether they choose to use an identifiable profile picture) in order to manage their visibility. The different locales of the players and the specific cultural and political milieu within which they are situated mean that their practices may well be influenced differently also. However, these differences do not interfere with the validity of the discussion; rather they broaden out the possibility of identifying a wider range of practices.

Many of the questions did allow for additional or clarificatory comments and these were useful and have been drawn on at times below. Where these comments have been included in the text below, they have been selected as representative of the key concerns that are noted (i.e. we have not included comments that repeat the same points already noted by others, rather we have selected comments that seem to be the most representative of this feedback) The survey software also enabled the extraction of particular (anonymous) respondent profiles – these were generated randomly by the researchers – enabling the presentation of different types of individual game visibility tactics, motivations and some of the rationales for choices made.

Complex and personalised (in)visibility tactics

What becomes quickly apparent from the responses is that player tactics to manage algorithmic visibility – and levels of visibility to different parties – are orchestrated in different locales, in different ways and for different reasons. Profiles drawn from extracting and aggregating anonymous individual responses illustrate the complex ways in which players navigate the algorithmic assemblages and media ecologies they encounter with social games in their everyday. Three profiles are detailed below to illustrate the complex and personalised reasons for managing visibilities in different ways; the profiles also show how visibilities (related to privacy and impression management) intersect with players' everyday lives in variable and nuanced ways.

Person 1 is in his mid-fifties and lives in Germany with his partner. He has a university degree and possesses not only smartphone, laptop and tablet but also a desktop computer and a games console and also utilizes online gaming platforms such as Steam. He plays social games downloaded from the app store and is on Facebook. He plays games about once a day, mostly alone, but also with people he does not know and with friends who live elsewhere. Mostly he plays social games to take a break from working and thus while in his office. He has privacy concerns because of his social games play: to address these concerns he avoids registration, uses separate accounts and utilizes the game options/settings. For example, he usually changes the privacy settings and when asked about further details as to why he does so, he says 'out of principle, in the game and in the underlying system.'

Person 1 does not use in-game purchases because he does not want to pay and because he does not want to provide credit card details. When he plays games as an app on a mobile device he rarely links the game to a social network site and strictly avoids providing any personal information such as pictures or his real name in his game profile. He also never posts game information such as 'successes' on social networks.

While he does access games directly from a social network site his profile there also provides no identifiable photo or username. To summarize, person 1 had well-established privacy-conscious practices aimed at trying to remain anonymous to other players, game providers and social network sites while still participating in various services and platforms.

Person 2 is in her mid-fifties with a degree from a university of applied science and she lives in Germany with her partner. She plays a variety of social games on her smartphone, tablet and desktop computer. At the time she was mostly playing the game 'Criminal Case' (a hidden-object puzzle game), but also other (often: Facebook) games such as Gardenscapes (another puzzle game) and Township (a farm- and city-building game), multiple times a day. She estimates about 4-6 hours overall play in the last week. When she learns about new games it is mostly through in-game advertising. Mostly she plays in

her office because that is where her gaming device is, but, weather permitting, also in her garden where she likes to spend time with her dog. She plays with anonymous other players, but also with friends who live elsewhere. She talks to others about games 'only rarely to compare what games we are playing, but it's really not that interesting', but she does not talk about game play details.

Unlike person 1, she is not worried about privacy in gaming and does not usually change privacy settings. She always uses her personal profile which also clearly identifies her through her real name and photo, but she only sometimes allows the game to post successes and never 'likes' others' successes.

So while this player is not concerned about privacy she still chooses not to share game play information such as in-game 'successes' with others, neither in personal chats nor on Facebook. While she seemed to embrace some of the features that others may avoid due to concerns about privacy, she still had clear opinions and established practices about which information to make visible to others.

Person 3 is a 31-40 year old female who lives in Australia and plays social games about once a day. Her household consists of herself and a child. She has a postgraduate university qualification and has a number of devices: smartphone, tablet/ipad, MP3 player, and console device. She has a profile on Facebook, but downloads games from the app store. She plays only by/with herself rather than with family, friends or anonymous others. She is concerned about privacy, and 'tries to' customise settings. She also tries to avoid registering, however if this is not possible, she uses a generic gmail account 'not closely linked to my identity'. The factors that contribute to her decision to download games include the fact it is not connected to her social network (despite having a Facebook profile), whether it is free to play and whether it is something that can be played quickly.

She does not pay for in game purchases as she does not like to pay for these but also she does not like to disclose her credit card details. She also notes that when she plays the game as a separate app she never uses her real name, uses an identifiable photo, posts progress to her social networks. However, if she plays through an SNS such as Facebook, she 'sometimes' uses her real name, uses an identifiable photo and allows the game to advertise her achievements on the site.

She usually plays when commuting, sitting on the couch, at a lunch location or when waiting for short periods (e.g. on public transport or at appointments). In other words, this player uses games as a way of filling time while waiting to do other things and by fitting her game play in around the rhythms of her daily life for roughly 1-3 hours a day. She does not talk to others about her gameplay as 'it is not something I am motivated to talk about'. When asked about whether there was anything else she would like to add about her social game play and how she manages her information and visibility to others, she notes that 'a few years ago my primary way of playing/accessing games was through

Facebook. I stopped this practice due to privacy concerns and moved to using games as apps without registering my details.'

This player demonstrates some awareness of privacy issues and has modified her behaviour as a result through shifting where she downloads games from and by restricting the provision of her details. She plays mostly by herself thereby restricting her game visibility to those in her social networks.

The complexity and variance of individual decision making around game play and player visibility is very evident in these three profile summaries: other summaries would reveal similar variance or nuance in particular ways. This individualised and particular complexity needs to be kept in mind whilst considering the discussion below about individual privacy and impression management approaches that were revealed in our study.

It is also worth reasserting that while players operate in algorithmically and programmatically constrained spaces, they have a range of choices they can make to customise outcomes. Some of these are programmed options that they choose to use (or not) and others involve 'playing' with their engagement (for example, through obfuscation or other tactics discussed below).

Even before engaging within a game, certain player choices are being made: For example, decisions as to what games to download, on what devices to download, where to download from, what sort of profile to use and also what privacy settings to employ need to be made. These decisions inform who has access to player information and what level of player visibility within and outside the game is achieved. Other decisions include considering whether to, at which point and in which way, to link their games to SNS such as Facebook; balancing the sometimes incommensurable game interests of social interaction and making use of game features for player interaction, often something required to advance in the game; managing membership in player groups such as 'neighbourhoods' or 'clans' to fit in with different levels of intimacy and anonymity depending on the situation; and navigating personal and social information data choices through their game practices.

In the questionnaire, we asked about factors that contribute to the decision to download a game. The responses reveal that the most decisive reasons were informed by calculations as to whether the game looks like something the players might enjoy; whether it is free; and then also whether it can be played on mobile devices. Put simply, cost benefit calculations are made initially as to whether players wish to enter this game space. However, also notable is that the issue of making data available to third parties or others (i.e. information or personal information and site access to information) do not figure highly in this initial calculation.

[Figure 1: Factors that contribute to decisions to download a game]

However, when we asked more specifically about privacy and information sharing practices, the responses became more nuanced, reflecting an underlying concern around control of personal information. When analysing player responses, for the purposes of the discussion, we categorised visibility tactics and rationales (to manage visibility to other players, to their social

network groups, the game developers and other third parties) into two areas: privacy and impression management.

The questionnaire did not define privacy but left this to respondents to infer in order to capture the range of understandings and practices that people might hold or enact with relation to visibility practices (we did not ask for respondent definitions explicitly nor did we provide a precise definition). Privacy, in the discussion below, then is not understood according to a specific definition, rather it is employed as a useful heuristic category to discuss respondent management of the disclosure of their personal information (whether to developers, other third parties or those with criminal intent) whereas impression management is used largely to refer to the ways in which respondents manage their visibility to others (friends, family, colleagues, players) in their social networks. Obviously, there are overlaps between these two areas, this will become apparent in the discussion below; however, the categories are a useful device for structuring the discussion of the results.

Privacy

We asked players specifically about whether they were concerned with privacy issues as a result of their game play and whether they used any of the available privacy settings. We also asked whether they use privacy settings. Overall, the responses indicated that more players were not concerned, than concerned, about social game privacy. However, this answer is not as straightforward as it initially might appear.

[Figure 2: Players concerned about privacy: 27% (14) yes, 61.5% (32) no, 11.5% other - sometimes concerned (52 answered, 10 skipped)] goes here

When asked about why they might use these settings (if they do), as Figure 3 below indicates, the majority responded that they did so to protect/control information. Their text responses included:

- *To prevent information theft*
- *Make sure that third party cannot access my information freely*
- *To avoid other people using my information*
- *To avoid sharing too much information and receiving nonstop advertising. In games or subscription to any website.*
- *Do not want to be found and I also do not want the game provider to be able to read out too much information about me*

[Figure 3: Players who use privacy setting: 71.2% (37) yes, 28.8% (15) no - (52 answered, 10 skipped)] goes here

Interestingly, but perhaps not surprisingly, many of the respondents rely on Facebook privacy settings as a tool to manage their privacy; they use these settings to manage information to third parties, to developers and to social networks (although clearly not to Facebook itself). Responses included,

- *Privacy setting on Facebook so that people don't see too much information*
- *I don't want my identity stolen. Privacy settings on Facebook.*
- *I use high level privacy settings on Facebook because I fear being scammed or having my page taken over or my friends conned.*
- *I use privacy settings on Facebook to make sure only people I know can view my information*

Many of these responses indicate a level of player trust in Facebook and Facebook tools to manage their privacy; or at the very least, they use Facebook tools in the absence of other tools or actions being available to them. This is within the context of a high level of general awareness amongst the public in both Germany and Australia of a raft of privacy concerns surrounding the use of Facebook itself.

Since its inception, Facebook has been dogged by claims about invasive privacy strategies and the data collection the SNS engages in and facilitates. The interplay over time between Facebook and its users is a classic illustration of de Certeau's assertions about recursive interaction between strategies and tactics. Facebook enacts strategies (collect data about its users) that prompt reactions and tactics from its users objecting to these strategies. For example, reaction to changes in newsfeed broadcasting of friend activities in 2006 initially provoked strong responses from users (see Debatin, Lovejoy, Horn, & Hughes, 2009, for discussion of this and other reactions to Facebook initiatives). Facebook, in order to keep its core business operating, responds to these reactions by introducing or modifying its privacy settings and also some of the ways in which it displays information to users. However, in doing so, it not only allays fear and consequently facilitates increased user disclosure of information, it also retains and expands its data collection activities. As Stutzman, Gross, and Acquisti (2012, p. 9) note,

Access to increasingly granular settings (which help individuals determine which profile data other Facebook users get to peruse) may increase members' feeling of control and selectively direct their attention towards the sharing taking place with other members of the network covered under those settings; in turn, perceptions of control over personal data ... and misdirection of users' attention ... have been linked in the literature to increases in disclosures of sensitive information to strangers.

These interchanges have been covered extensively in the mainstream press and also within scholarly literature meaning that it would be unlikely our game players would be completely unaware of Facebook data gathering and privacy violations. Indeed, later individual responses do reveal a level of awareness that player activity has broader ramifications for their visibility. Thus, while many respondents relied on the Facebook privacy settings, they also managed their visibility using obfuscation, to use a Brunton and Nissenbaum term, whereby,

With a variety of possible motivations, actors engage in obfuscation by producing misleading, false, or ambiguous data with the intention of confusing an adversary or

simply adding to the time or cost of separating bad data from good. (Brunton & Nissenbaum, 2011)

Player responses indicated a range of obfuscation tactics employed: For example, they use false profiles, use different game names that are not linkable to their other social media profiles, they choose not to register their details or to register false details.

Player responses to the question: If you are [concerned about privacy], can you describe some steps you might take to manage these concerns?, included:

- *Avoid registering. If I can't avoid registering, then use a generic gmail account that I use that is not closely linked with my identity.*
- *Do not share or post anything and manage settings*
- *No photos in the profile*
- *Not accepting all types of requests without reading terms and conditions*
- *Check parts of agreement and disable sharing options where required*
- *Faking identity*
- *Don't give personal information*
- *I have a faker [sic] name facebook account, also avoid connecting games to facebook if I can (unless the data requires it which I'm not happy about)*
- *Deny sending out my details*
- *Maintain privacy settings*
- *Use a game handle unlike any social media handles*

These obfuscation behaviours can all be described as tactics in the way that de Certeau employs the term. Players are using or appropriating the tools and techniques made available to them by the system (the platform, the game developer, the advertiser, etc.) however, they are choosing to subvert and personalise the ways in which they use them; ways that are contrary to the ways the system would like them used. This defuses or divests the system's strategies and therefore subverts or undermines the intended outcomes for the system. It becomes more challenging for the system to collect accurate data profiles, makes it more difficult for the game developer for example, to effectively or accurately modify algorithms to encourage certain player behaviour and so forth. Through this process, the player asserts a limited amount of autonomy and power, being able to play the game he or she wants to play while ensuring that the system and therefore also the algorithms that are employed by the system do not have complete control over their actions, environment or outcome. However, the ways in which players accomplish these things are varied and complex: they have to balance or negotiate their 'in-game' progression with their broader personal 'out-of-game' visibility. This includes managing their visibility to people within and outside of their social games and their networks using impression management tactics.

Impression management

Goffman (1969 [1959]) refers to impression management as the need to manage, curate and perform a particular presentation of self to a particular audience. With regard to social game

players, impression management is further complicated by the need for players to manage the actions of the game's programmed imperative to map and broadcast player activities to others within and across player's social networks if linked with an SNS (Willson, 2015). As Van Dijck (2013, p. 202) notes,

Goffman's two levels of conscious and unconscious self-performance are thus newly relevant when it comes to online platforms. While users consciously construct their own profile, platform owners and investors collect behavioral data that users are unaware of creating....

It became apparent from the range of responses that players have some awareness as to who has access to their data and that they employ various tactics as a result of this awareness. Their responses, however, also demonstrate a mindfulness of the role that underlying algorithms and game software play in the way that their identities and activities are transmitted to other people and the need to modify or manage their practices accordingly: they enact conscious impression management tactics (also, see discussion in Willson, 2015).

We asked players directly about management of their social game visibility to their friends, colleagues, to other players, and to people who they might not know. Roughly half of the respondents indicated that they talk to others about their social game play: these players indicated they talk mostly to those who either play that particular game, who they play that game with, with those they know play social games, and with family and friends (they could indicate multiple answers for this question). In other words, they discussed their social games with others who they believed shared an interest and therefore would be more interested but also more likely to be accepting of social game play. Of those who indicated they don't talk about their game play; the most common response (multiple answers could be given) was that they did not believe others would be interested.

The cultural framing of games (particularly social games?) as not serious, frivolous, and time-wasting activities could be suggested to influence the impression management strategies that players enact. For example, one respondent noted,

I prefer not to have any identifying features (name, images) to me however I have developed a recognisable game persona which I do have some small anxiety about. I prefer others not to know when or how long I play games as this is my escape time and I find others tend to not understand that this doesnt [sic] mean I have lots of free time - rather that I just allocate some of that free time for 'escape' play.

For example, the majority of respondents do not share or post achievements, they do not use a recognisable profile photo, they do not tweet about the game, and where the game is available as a separate app they 'only sometimes' link this to their SNS. Another comment noted:

I prefer not to let people know when I'm on a break (especially with facebook notifications) or playing games as it tends to be a reason people use to either contact me for a chat or counter any of my claims about being busy. I find people don't

understand that I may only spend a small portion of 'escape' time on games from my very busy daily schedule.

In other words, they manage how they and their activities are portrayed and to whom. Other responses included:

- I very deliberately only share my photos, status updates etc. with selected people/groups*
- Do not share or post anything and manage settings*
- Disable sharing options where required*

Throughout the questionnaire, responses indicated the compromises and negotiations enacted to play the game successfully alongside tactically navigating various algorithmic visibility strategies (and, at times, the ways these may be complementary).

What the collective and also individuated responses reveal is that gaming activities are situated within privacy and impression management tactics that are variegated, subtle and complex. It is clear that understandings and practices of visibility go beyond a simple conception of information control, instead displaying a more nuanced and individuated understanding that intersects and overlays with impression management: Differing types of visibility are identified and levels of importance acceded to different audiences with whom that (in)visibility is displayed. Recognition of these complexities and nuances are important: there are contradictions and differing understandings of privacy, of what is important to reveal or to obscure and to whom, and of the various tactics to employ.

Conclusion

In this paper, we examined some of the everyday practices of social gamers in their interaction with games as algorithmic, programmed spaces with a particular focus on what we refer to as visibility tactics. We employed Michel de Certeau's (1984) notion of tactics and strategies as a way of framing the discussion of player actions and of how their awareness of programmed requests to engage, divulge information, connect to other users alongside broader privacy concerns around data collection and exposure to third parties were navigated and translated into specific tactical behaviours and choices. Through this process, we have revealed how algorithms become – in observation but also in players' awareness and interactions – entangled and often indistinguishable from logics and structures offered by devices, platforms, programs, and people. It was obvious that players' actions were influenced by many simultaneous considerations, for example, a decision to join an in-game group could be motivated by wanting to gain an advantage in the game, avoid payment for specific items (and having to provide credit-card details), by the possibility to join anonymously (or not – social interests or even pressures may have been at play) and eventually by assumptions about how player behaviour may influence the game providers' strategies for improving the game in their assumed interest of gaining more revenue, also possibly through data collection and advertising.

Player actions were highly structured by the mechanics of the game and platform requirements, yet players also found ways to tactically obfuscate, manipulate and appropriate these to address their needs and concerns around algorithmically enabled visibility with regard to privacy concerns and impression management. Individual player tactics were highly situated and contextualised: the choice of what device to use, the decision about linking to a SNS, or to pay for something or not using a credit card were multiplex and often decided by how convenient/pleasurable/ advantageous an action in a concrete situation might be alongside negotiated costs of privacy and impression management and the conditions of algorithmic visibility. What is apparent from our discussion is that social games offer a multi-faceted microcosm for a closer analysis of the interplay of algorithmic play, data acquisition management and visibility tactics understood in a broad sense.

References

- Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, 11, 985-1002.
- Beer, D. & Burrows, R. (2013). Popular Culture, Digital Archives and the New Social Life of Data. *Theory, Culture & Society*, 30, 47-71.
- Brunton, F. & Nissenbaum, H. (2011). Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation. *First Monday*, 16(5). Retrieved from <http://www.ojphi.org/ojs/index.php/fm/article/view/3493/2955>.
- Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, 14(7), 1164–1180.
- de Certeau, M. (1984). *The Practice of Everyday Life*. trans. S. Rendall. Berkeley: University of California Press.
- Debatin, B., Lovejoy, J.P., Horn, A-K., & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15, 83-108. doi:10.1111/j.1083-6101.2009.01494.x
- Diakopoulos, N., & Koliska, M. (2016). Algorithmic transparency in the news media. *Digital Journalism*. Published online: 27 Jul, doi:10.1080/21670811.2016.1208053.
- Galloway, A. R. (2006). *Gaming: Essays on Algorithmic Culture*. (Electronic mediations; Vol. 18). Minneapolis: University of Minnesota Press.
- Gillespie, T. (2014). The Relevance of Algorithms. In T. Gillespie, P.J. Boczkowski, and K. A. Foot (Eds.), *Media Technologies: Essays on Communication, Materiality, and Society* (pp. 167-93). Cambridge, MA: MIT Press.
- Goffman E. (1969 [1959]). *The Presentation of Self in Everyday Life*. London: Allan Lane.
- Juul, J. (2010). *A Casual Revolution: Reinventing Video Games and their Players*. Cambridge, MA: MIT Press.
- Kinder-Kurlanda, K. & Willson, M. (2016). Facebook Social Games. In K. Knautz & K.S. Baran (Eds.), *Facets of Facebook: Use and Users* (Knowledge and Information: Studies in Information Science, pp. 94-114) Berlin: De Gruyter Saur.
- Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14–29.

Scacchi, W. (2010). Computer game mods, modders, modding, and the mod scene. *First Monday*, 15(5). Retrieved from <http://firstmonday.org/article/view/2965/2526>

Sotamaa, O. (2010). When the game is not enough: motivations and practices among computer game modding culture. *Games and Culture*, 5(3), 239-255.

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*, 4(2), 7-41. Retrieved from <http://repository.cmu.edu/jpc/vol4/iss2/2>

Tufekci, Z. (2014). Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls. In *ICWSM'14: Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*.

Van Dijck, J. (2013). 'You have one identity': Performing the self on Facebook and LinkedIn. *Media, Culture & Society*, 35(2), 199-215.

Willson, M. (2015). Social Games as Partial Platforms for Identity Co-Creation. *Media International Australia*, 154(1), 15-24.

Willson, M. & Leaver, T. (2015). Zynga's FarmVille, social games, and the ethics of big data mining. *Communication Research and Practice*, 1(2), 147-158.

Wohn, D. Y., Lampe, C., Wash, R., Ellison, N., & Vitak J. (2011). The 'S' in Social Network Games: Initiating, Maintaining, and Enhancing Relationships. *Proceedings of the 44th Hawaii International Conference in System Sciences*. (HICSS '11) Kauai, HI Jan, IEEE.

(word count: 7998)