The Rise of Speculative Devices: Hooking Up with the Bots of Ashley Madison

Ben Light, Digital Media Research Centre,
University of Salford, UK
Email. ben.light@qut.edu.au
Web. www.benlight.me

Brief Author Biography

My research concerns people's everyday experiences of digital media with a focus on (non)consumption, gender and sexuality and digital methods. I have previously published work in Cultural Sociology, Information, Communication and Society and New Media and Society. My book, Disconnecting with Social Networking Sites was published by Palgrave Macmillan in 2014.

Light, B. (2016). The rise of speculative devices: Hooking up with the bots of Ashley Madison. First Monday, 21(6). http://firstmonday.org/ojs/index.php/fm/article/view/6426/5525

The Rise of Speculative Devices: Hooking Up with the Bots of Ashley Madison

Abstract
I attend to two areas of increasing significance in relation to Web 2.0 since its announcement in 2005. The first is a focus on the non-human in digital media research, and the second is the normalisation of dating apps in society. Building upon ideas from speculative design and speculative method, I introduce the idea of speculative devices, those things that are set in place based on a conjecture of an outcome. Drawing upon a case study of Ashley Madison, generated using a walkthrough method, I demonstrate how the speculative devices of bots and profiles can operate, and why. I argue we need to give careful thought to how our research and practice is understood, and conducted where speculative devices are concerned.

Introduction
During July and August of 2015 the media, particularly the online tech press, were populated with stories about Ashley Madison. Ashley Madison, provides a dating and hook up space for people to engage in discreet encounters, they had been hacked and in the region of 37 million account records along with company documentation was made public. Much of the attention was given to the lack of morality shown by Ashley Madison and its users. Less attention was given to the hackers themselves, although an excellent analysis including this group can be found on the Dailynous. Journalists scrambled to find lurid stories about anyone, particularly those in the public eye. The site was linked with e-mail accounts of supposed USA Homeland Security staff, and other pubic workers, members of several churches and conservative religious bloggers. In the wake of the hack, lawsuits have been filed, partnerships and marriages have been said to collapse and it has even been suggested that it has led to suicides.

Humans were made the centre of this controversy, and the Ashley Madison organization was usually positioned as the first digital site where extra partnership affairs might be generated. This ignores much of what we know about so called early cyber adultery and uses of Tinder, Match.com and OKCupid for clandestine hook-ups. However, it is not the humans I am interested in here, not directly at least. The hack brought to the fore non-human actors, such as bots (software applications that run automated tasks) and hook-up site user profiles. In Ashley Madison, bots appear to be used to chat with human users to keep them engaged, and they use fake profiles, created by Ashley Madison employees, as a 'face' for the interaction. The same bot can inhabit many profiles. These bots and the profiles they inhabit are the focus of this paper.

In the next part of the paper I expand on what I mean by speculative devices. For now, one can think of speculative devices as those things that are set in place based on a conjecture of an outcome – bots and profiles are seemingly active in Ashley Madison in the hope they will engage users and generate business for example. I also discuss how non-humans have always been implicated in dating and hooking up and that although dating apps have risen to prominence since the announcement of Web 2.0, the role of the Internet in this aspect of life has a much longer history. I then explain two ways of thinking that can be combined to help us understand the bots of Ashley Madison. These are disclosive ethics and actor-network theory. Together these ways of thinking ask us to consider the links between ethics and digital media,

and how we might think of the non-human as having the ability to act with us. I then introduce Ashley Madison and describe what the public hack data and other public information about the site can tell us about the role of the bots. After this, I discuss the bots of Ashley Madison, taking into account my desire to show their agency with us and the ethics they are associated with. I conclude the paper by considering the broader implications of this work in terms of learning about, and not causing harm with, speculative devices.

Speculating with Non-Humans

Human agency is a feature of Web 2.0. As Zimmer (2008a) notes in the introduction to the preceding issue in this area in 2008, Web 2.0 has been positioned as promising creative empowerment, the democratisation of media production, collaboration and a more general celebration of the individual. Zimmer goes on to elucidate that questions of human agency were, even at that point (and prior to this), much more complicated than the evangelists of Web 2.0 would have us believe. In that special issue, for instance, Jarrett questions the forms of agency embedded in participation where commercial interests are concerned (Jarrett 2008) and Zimmer (2008b) points to the privacy concerns associated with combining Web 2.0 and search engines as they attempt to build profiles and predict our intentions.

Since the emergence of Web 2.0, we have witnessed a non-human turn in studies of the Internet where the materiality of algorithms, code, interfaces, devices and platforms have been seen to come into play. That is not to say before 2005 these were not considered, such as in work on menu driven identity (Kolko 2000; Nakamura 2002) and early work on the technical turn in philosophy (Feenberg 1992; Feenberg 1995). That said, increasing numbers of scholars have begun to take seriously the non-human in their study of the Internet and account for it, for instance, in their analyses of algorithmic culture (Cheney-Lippold 2011; Gillespie 2014; Crawford 2016; Karppi and Crawford 2016), the politics and ethics of platforms (Gillespie 2003; Gillespie 2010; Light and McGrath 2010) and the role of mediators more generally (Brunton and Coleman 2014; Light 2014). It is in the context of the growth of attention to the non-human that this work is situated. Through a case study of the dating app, Ashley Madison, and a focus upon the positioning and activity of its bots, I interrogate the operation of speculative devices as a consideration in a digitally networked context.

Speculative Design, Method and Devices

Speculation has been engaged in several ways in research and practice, particularly in a methodological context. Whilst there is much research on the effects of speculation in markets of various kinds, I am interested in to how speculation is engaged in terms of design and method.

Speculative design is concerned with deploying artefacts, probes and prototypes that have oblique and ambiguous functions in order to allow designers and users to open up what is at stake in particular events (Auger 2013; Dunne and Raby 2013). This approach has been positioned as a way to engage with design to generate alternative visions of being, inspire, and encourage people's imaginations to flow freely (Dunne and Raby 2013). It is assumed that humans are free agents and that speculative approaches can increase the probability of a more desirable future whilst limiting those that are undesirable (Dunne and Raby 2013).

Speculative method refers to forms of research approach that have the capacity to act themselves as well as be enacted by a researcher. Race for example introduces speculative pragmatism, defining it as "concerned not only with what happens, but also what might happen, the possible – that is, what might come into being" (Race 2015b: 500). In another example, the work of Wilkie et al. (2015), discusses bots inscribed with particular characters (idiot, parasite and diplomat) and how they are deployed with Twitter as a method for generating of discussion with and amongst humans about climate change.

Building upon this work, I extend the possibilities for speculative design and method through an illumination of a particular version of speculative devices. From design I borrow the principle of things such as artefacts, probes and prototypes that have ambiguous functions as holding the potential to shape and interact with human agency to produce sets of associations. However, in contrast to speculative design, I do not necessarily associate their deployment with positive or well-meaning outcomes. From speculative methods, I take the idea of devices as part of methods resulting in unexpected and unknowable outcomes. By device, I mean a thing for affecting a purpose, recognizing that objects contribute to the processes of making events that constitute society (Michael 2012). To be clear, when I refer to speculative devices I see them as holding the potential to be both part of our methodological apparatus and an object of our study. In this paper I focus upon a case involving speculative devices as an object of study (bots and profiles for example), but in the closing stages of the paper, I reflect on this to consider broader implications for speculative devices where we might also use them in our methods.

Speculative devices extend beyond the bots identified in the work of (Wilkie et al. 2015), and technologies of elicitation, such as the discussion group or council meeting intended to generate lay views on a public issue (Lezaun and Soneryd 2007). Speculative devices are those things that are set in place based on a conjecture of an outcome. They possess a degree of ambiguity even though there may be some information on hand that has led to the decision to attempt to act in a situation. The extent and quality of data and information upon which the conjecture inscribed into speculative devices is variable. In the case of digital networks, these may include, but are not restricted to, algorithms, bots, interfaces, or global positioning systems for example.

Locating the Non-Human in Dating and Hook Up Apps

The process of dating and hooking up has always involved non-humans. Personal advertisements in newspapers and magazines, television, video, the use of filing systems by dating agencies, and recreational drugs are but a few examples (Woll 1986; Phua et al. 2002; Race 2015a; Race 2015b). In terms of the digital, as desktop and database applications became more readily accessible during the 1980s, these were used by dating agencies as replacements for filing cabinets. In the 1980s and 1990s, chat rooms and bulletin boards also played a role in dating and hooking up (Correll 1995; Shaw 1997; Campbell 2004). Towards the end of the 1990s, sites such as Gaydar and Match.com emerged enrolling a networked database logic whereby those engaging with such services crafted searchable profiles (Gibbs et al. 2006; Light 2007). During this time, companies such as eHarmony also used algorithms combined with the profiling questionnaires emblematic of traditional dating agencies. Simple

geo-locative functions also appeared as mediators during this time. For example, Gaydar requested user postcodes/zip codes for their Gaydar Positioning System so that users could be presented with profiles nearest to their stated location (Light et al. 2008). In the mid 2000s websites optimized for mobile devices emerged and services such as Gaydar Mobile with its 'pay as you cruise' business model appeared as actors accompanying users on the move (Light et al. 2008). This occurred alongside the vernacular appropriation of technologies for hooking up, such as Bluetooth (Mowlabocus 2010). Quite clearly, as with other aspects of the Internet, the distinctions often made between so called Web 1.0 and Web 2.0 in respect of user participation in content generation and forms of sociality are less than clear cut.

Since the release of the iPhone in 2008, dating and hooking up has become appified and the acceptance of using the digital to find a partner or hook up has rapidly become normalised in many societies especially as apps engaged with discourses of Web 2.0 features and those associated with social media. This process of appification has brought with it further non-humans in the form of diverse apps such as Tinder, HER, Mixxxer and Hornet targeting a range of dating and hook up markets based on segmentations associated with sexual orientations, sexual preferences and socioeconomic status for example. Along with these have emerged app stores as mediators of practice in terms of operating systems available on particular devices and the terms and conditions associated with particular stores as compared to the open web (Roth 2015).

In 2015, the Ashley Madison hack raised the profile of a further potential actor in dating and hooking up – the bot. In this paper I interrogate the role of speculative devices, in the search for, and participation in, discreet encounters where bots are present. Before I do this I outline a theoretical and methodological framework for this study of speculative devices, one based on combining the work of disclosive ethics and actor-network theory.

Disclosive Ethics and Actor-Network Theory

This work is rooted in the descriptive ethics tradition. Here the aim is to unearth narratives regarding morality. This differs from normative approaches which seek to determine appropriate practices of conduct (Johnson 2001). More specifically, a disclosive ethics approach is drawn upon that allows for the attendance to the norms and values embedded in digital media and digital media practices (Brey 2000). Disclosive ethics, for example, has previously been deployed in relation to facial recognition systems, plagiarism detection systems and Facebook (Introna 2005; Introna 2007; Light and McGrath 2010).

It is often argued that things cannot have intentionality and therefore it is not possible for them to have morals. Leaving aside animals as non-humans, and focusing on non-biological non-humans, the point is to see things as coming into being as they interact with other things and humans. It is when a set of associations (Latour 2005) amongst actors is created that moral conditions can be generated. This has also been referred to as heterogeneity – the constitutive mixing of the social and material, the human and the non-human, the subject and the object such that each is partly comprised of the other (Michael 2012a). For example, a gun being fired by one person upon another generates different conditions to those where people fire a gun upon themselves. It is at this point that I need to disclose a particular philosophical position in relation to the

world that I am taking in this analysis. I am arguing that non-humans matter and they do things with us, and I have elaborated on this in much more detail elsewhere (Light 2014)]. In the words of actor-network theory, the non-human can be mediators that transform situations, and ones that we can delegate authority, and morality to (Callon 1986; Latour 1992; Latour 2005). Combining disclosive ethics and actor-network theory has generated the case study of Ashley Madison I present here. The data for the case study has been obtained by drawing upon the principles of the walkthrough method[i] and media reports regarding the hack.

The walkthrough method offers a way to perform a critical reading of apps. It is an empirical method that is informed by science and technology studies and cultural studies which, attends to a reading of how a given app presents itself to others and how others might engage with it. The method offers a framework which guides the researcher in the targeted analysis of an app by examining, for instance, elements of:

- the environment of expected use – including the developer's vision, the app's operating model and its governance structures;
- documenting the app – by exploring registration, everyday use and leaving mechanisms through attention to interfaces, functions, content, tone and aesthetics;
- and, unexpected practices associated with the app – such through the analysis of associated advice blogs, hacking, resistance, and third party additions or manipulations of the app.

The method is used in conjunction with an appropriate set of ideas in the same way case study work might be. The method may focus solely on a reading by the researcher or may involve interviews with users to gain additional insights into individual and group practices. In essence, the method can be used to construct imagined/expected modes of use and those based on user feedback. In this case I used elements of the walkthrough to generate empirical data that discloses the ethics of the presence of bots within Ashley Madison by drawing upon disclosive ethics and ANT.

To collect data, I examined the site's public facing pages (including FAQ and terms and conditions), recorded the process of creating an account (as a straight single man looking for women – based on media reports of the ratio of bots associated with this kind of connection making), and explored the site once registered. I concealed my profile from public view but populated it with content indicating that I was a gay man, using the profile to learn about that site and that I was not interested in any form of connection making with men or women. I did this so that I had no interaction with humans in the site. Interestingly, this did not stop my profile being bombarded with connection requests from female identified bots; the furthest away was in Texas, USA. Since opening my account just over 3 months ago I have received 75 system generated messages encouraging me to connect with women's profiles, geographically located in many different countries, and even though my profile has been hidden from user view.

I collected data by reviweing media coverage of the hack that occurred in June 2015, especially that which referred the data released in the hack. I have not accessed the data hack myself because it was obtained illegally, and have therefore relied on

various sources, including the walkthrough data I collected, to generate a plausible account of how the bots of Ashley Madison operate.

Introducing the Bots of Ashley Madison

Ashley Madison, owned by Avid Life Media, is self-described as the "leading married dating service for discreet encounters" (Figure 1). The service is positioned as a hook up app for people in relationships looking for further relationships. These further relationships may be formed with the app where the consent and knowledge of all of those in a relationship are present or not. As of January 2016, the site's welcome page states that it has over 43.5 million users.

Figure 1. Ashley Madison welcome page (Ashley Madison 2016b).

The site operates like many dating apps – users create a profile, can search for connections and communicate with them in a variety of ways. Free user accounts can be created, allowing users to receive winks, send and receive photos, add members to a favorites list, reply to full members and perform searches. Payment to the site is required to send a custom mail-message, initiate a chat session, send a priority message and to send virtual gifts.

In mid July 2015, Avid Life Media were warned by the hacker group *The Impact Team*, that unless the site was taken down, a large amount of data about the operation of the site and its customers would be released onto the web. This data was said to include employee documents and emails, and the real names, credit card information, addresses, and the sexual fantasies of users. The rationale for the hack was reportedly to stop the exploitation of future users by the site. In the words of the hackers "We did it to stop the next 60 million [users being exploited]. Avid Life Media is like a drug dealer abusing addicts" (Cox 2015). Avid Life Media did not comply and on the 4 August 2016 a 9.7-gigabyte data dump was posted to the dark web (Zetter 2015). A second dump of partly corrupted data, 20 gigabytes compressed, was released to the dark web on the 18 August 2016 (Newitz 2015b), resulting in over a dozen civil law suits to be filed in US federal courts against Avid Life Media (Gershman 2015).

Very soon, the data was available across the open web and was the subject of media coverage. Annalee Newitz, now tech culture editor of Ars Technica, undertook some particularly insightful research (Newitz 2015c; Newitz 2015a; Newitz 2015b; Newitz 2015d) drawing on the data dumps. In brief, Newitz and her collaborators, reported on the presence of fake profiles and the deployment of bots throughout the site. Both the fake profiles and bots where almost all identified as women and were configured to entice straight male users. These profiles and bots I see as speculative devices.

Newitz's analyses of the data dump revealed 70,572 bots, 70,529 configured as female and 43 configured as male. It was also reported that male users received 20,269,675 million messages from female bots, and that female users received 1,492 messages from male bots. Further, female bots engaged in chat with men 11,030,920 times and, male bots engaged in chat with women 2,409 times. Examining the source code of the site, it was possible to see that bot based encounters could be generated every few minutes creating an overall sense of women looking for men throughout the site (Newitz 2015b). These bots were linked with profiles because they are the mode of making connections throughout the site.

The presence of fake profiles operating in Ashley Madison had been raised in the public domain previously. In 2013, the statement of claim of a former employee is said to — state that she was hired to help launch a Portuguese-language version of the site, promised a starting salary of $34,000 plus benefits and was soon asked to create 1,000 fake female profiles whose purpose was to entice paying heterosexual male members to join and spend money on the website (City News 2013).

The data dump also revealed emails that included details regarding Avid Life Media employing people to create fake women's profiles and to chat with men on the site (Newitz 2015b). These emails also revealed that the bots were termed Engagers by Ashley Madison staff and these inhabited the fake profiles, known as Angels. Newitz reports via her interrogation of the source code's comments that bots were given descriptions of how to act by programmers that has them sporadically focusing on engaging straight men:

> host bot mother creates engagers
> birth has been given! let the engager find itself a man!
> randomizing start time so engagers don't all pop up at the same time
> for every single state that has guest [non paying] males, we want to have a chat engager
> (Newitz 2015b)

The vocabulary available to a bot initiating a conversation with a user is also revealed by Newitz, as shown in Table 1. Moreover, an analysis of bot activity by software engineer Jacob Perkowski has pointed to their geographical pervasiveness as shown in Figure 2. Newitz (2015b) has also reportedly identified emails within the data dump which catalogue the difficulty the company had in making bots that were able to speak 31 different languages in approximately 50 countries. It was also noted that developers wrote in exceptions to exclude the bots from being deleted spam sweeps. (Newitz 2015b).

Table 1. Bot talk – Adapted from Newitz (2015b)

I'm sexy, discreet, and always up for kinky chat. Would also meet up in person if we get to know each other and think there might be a good connection. Does this sound intriguing?

Figure 2. Ratio of engager accounts to female accounts by country

A pseudonymous Gizmodo commenter Mr Falcon, was also reported by Newitz to have uncovered a special bot service dedicated to those who had paid for the premium service Guaranteed Affair (Newitz 2015b). This premium bot would engage male users and was configured to encourage them to pay credits, to interact and eventually pass them over to an affiliate. It is not clear who or what that affiliate is.

The Guaranteed Affair service promises a user they will find 'someone special' within three months or they are eligible for a refund (Ashley Madison 2016c). However the service comes with particular conditions. An affair guarantee costs $316 in Australia and affords the member 1000 credits. Credits are used to sustain interaction within the site. As at 21 January 2016 it costs 5 credits to send priority and

open collect mail messages (the 5 credit charge applies only for the first mail message to any given member), an instant Message Session costs 30 credits/30 minutes and 60 credits for 60 minutes and Ashley Gifts - virtual gifts - are available for 20, 30, and 50 credits. During the three-month period of the Guaranteed Affair members have to:

- post a primary photograph in their profile;
- keep their profile visible at all times;
- send at least 18 priority mail messages each month, to members they have previously had no contact with;
- send at least 5 Ashley Gifts per month;
- instant message with members for at least 60 minutes per month through the AshleyMadison.com service (Ashley Madison 2016c).

Therefore a member has to use a minimum of 630 of their 1000 credits in meeting their obligations for the scheme if they wish to claim a refund if they do not meet 'someone special'.

The bots are referred to in the site's terms and conditions of service in some detail (Ashley Madison 2016a). The terms and conditions are approximately 10, 340 words in length. I collected these on the 21 January 2016 and I was able to confirm they were the same as prior to the hack by obtaining a version published 28 February 2015 via the Internet Wayback Machine[ii]. From these terms and conditions, I have selected the bot and profile related excerpts for analysis in the next section (Table 2). Notably, the terms and conditions state 'These profiles [populated by bots] are NOT conspicuously identified as such.'

Table 2. Excerpt from Ashley Madison terms and conditions 21 January 2016

Discussion

As shown in Figure 3 Ashley Madison users accept the site's terms and conditions during the account creation process. As is often the case in these scenarios, the text regarding the link to the terms and conditions is conspicuously small and lightly coloured as compared to the 'I Agree' button. This is important as it is only the in the terms and conditions that the use of bots are mentioned by the company - and they are never called bots.

Figure 3. Accepting terms and conditions

Moreover the welcome page, as shown in Figure 1 clearly signifies to a user that they can find '100% like minded people' on the site. The site's strapline 'life is short, have an affair' reinforces the expectation of meeting humans. The welcome page and terms and conditions are contradictory in nature but ultimately a user is led to believe they are entering a site full of human encounters.

The hack suggests only 70,572 bots existed in June 2015 in a database then consisting of 37 million profiles (Newitz 2015b; Newitz 2015a). It is not possible to determine how many of the 37 million profiles were active, or were profiles waiting to be inhabited by a bot. Perkowski's analysis as detailed in Figure 2 suggests a maximum ratio of bots to female accounts of 5 per cent around the world. These bots are attempting to interact with male users in particular, tens of millions of times, according to the data reported on from the hack.

The bots of Ashley Madison are like financial algorithms in that they are, as Karppi and Crawford (2016) suggest, built to affect and be affected. The question then becomes one of how they are active. Ashley Madison has delegated the speculative work of seeking to engage human users to the bots and the profiles they inhabit. Data from the hack and the terms and conditions of the site (see Table 2) reveal the characteristics and ethics of the encounters involving the bots of Ashley Madison and the profiles they work with.

The bots and profiles are positioned as an aid to users in navigating and learning about the site and the communications they may encounter. The bots and the profiles they work with are characterized as doing good for the community of Ashley Madison. This character of being helpful is also carried through to their role in the collection of data about users and the monitoring user communications to ensure compliance with service terms.

The bots and profiles are also characterized as entertainers. Bot activated profiles may send winks, private keys (to additional content about the character associated with the profile) or Ashley Gifts. The bots are also inscribed with a language of sexually charged playfulness as shown in Table 1. The bots are allowed to have multiple partners, just like guest users and members. This character also involves the generation of a situation where, obviously, a user will never meet the other party in this communication. To reinforce this, the terms and conditions state that "you cannot meet any of the images associated with our profiles in person and you acknowledge and agree that such communications are solely for your entertainment and to encourage your use of our Service". There are two points to make here. First, it may well be the case that a user is fully cognizant of the fact they are engaging with a bot and/or they may be very happy to engage in erotic chat and never meet someone. Second, through this entertainment process, users are encouraged to use the service, generating income for Ashley Madison directly and indirectly.

The direct form of income generation is related to the fact that in order to interact in certain ways within the site it is necessary for users to buy credits from Ashley Madison. Therefore, the bots and profiles seek to engage users in paying for elements of the Ashley Madison service. Indeed, this need for payment can be amplified in certain contexts. For example, if a user subscribes to the Guaranteed Affair, they must spend a substantial number of credits to meet the scheme's rules. The hack revealed that a special bot service was associated with this scheme contradicting the terms and conditions of the service which state that "Our profiles message with Guest users, but not with Members. Members interact only with profiles of actual persons." This use of bots expands upon the speculative potential of chat functionality as described by Race (2014) who, in discussing hook up apps, states that:

"While the pre-specification of identity and desires may take an element of surprise and spontaneity out of the sexual encounter, forestalling the mutual construction of pleasures and desires at this scene, chat facilities also constitute a new medium of erotic exchange among relative strangers, which has considerable speculative potential." (Race 2015b: 503)

In Ashley Madison, bots, as well as relative strangers lubricate this speculative potential. This speculative potential can also be read in two ways. It is present in the sexually charged maneuverings that chat makes possible where it is removed by the pre-structuring of identity in dating and hook up apps as Race suggests. It is also present in the generation of revenue, and activities that can lead to revenue for the site.

Indirectly, the bots and fake profiles (whether inhabited by bots or not at any given time), undertake the work of making Ashley Madison seem populated with (mostly) women willing to engage in a discrete encounter. Their speculative work may result in income for Ashley Madison as described above, or indirectly as members buy credits to spend within the space that seems to offer the potential for a discreet encounter. Moreover, there is extra work performed by the member for Ashley Madison. The presence of a profile of a member in the space, it being updated and present at different times, and in potentially different locations, contributes to the liveness of the space for other guest users and members. Further, where the Guaranteed Affair is purchased, a primary profile picture is mandatory and this animates the site on behalf of Ashley Madison, especially as a requirement is for it to be visible at all times. The requirement for significant levels of interaction initiation during the Guaranteed Affair period also contributes to this animation work. This resonates with earlier work on which points to the roles that users can have in producing economic value for platform owners (Arvidsson 2006; Magnet 2007; Light et al. 2008; Petersen 2008).

Beyond the obvious ethics of capitalism, there is an underlying disclosure here that is unanswerable in this paper. This disclosure rests on the question of the extent to which users understand the presence of non-humans in the space and where these are known, what their feelings about them are. Reporting on the hack and a comparison of this with the terms of service reveals contradictions - where bots approach paying members - as I have indicated earlier. Taking this further, it is worth considering how bots are inscribed with goodness in the sense that they are, according to the terms and conditions, not supposed to bother full paying members. However, the potential exists, if the hack data is correct, that the bots target members when they have purchased a Guaranteed Affair and that these good bots can become bothersome in terms of obfuscating the member attempts at finding a person to hook up with and in becoming a drain on their financial resources. Of course this assumes, guest users and members do not gain pleasure from the bots.

So far in this paper I have not directly addressed the ethical questions at the heart of the raison d'être for the site and how these are, or are not, inscribed within it. Before I approach this, there are two points I wish to make. The site is configured in such a way that single people can meet for discreet encounters. This means that there is the possibility that there are users who are not in a relationship who wish to meet. Indeed, one of those filing a law suit against Avid Life Media is a widower who had reportedly used the site following the death of his wife of 30 years from breast cancer (Pilieci 2015). There is also a particular set of ethics being attached to Ashley Madison in relation to the expected standards of normal behavior in a committed relationship. Some people do have extra-relationship affairs and hook-ups with varying forms of consent from their partner or partners. Moreover, a study of the locative data released as part of the hack has shown significant numbers of men

seeking men in countries where homosexual acts are punishable by death (Cain 2016). Leaving this aside, and focusing upon the popular media coverage of the site, the hacking of it, and how the site positions itself, a normative ethic of intimate relationship arrangements is present.

Ashley Madison seemingly delegates the morality of engaging in an extra-relationship affair to the user, positioning itself as merely an intermediary – the Napster of the naughty if you like. This resonates with Jarrett's (2008) earlier commentary on Web 2.0 producers where she highlights their strategic denial of authority. Ashley Madison further delegates the supposed dirty work of enabling extra-partnership connections by introducing bots that encourage users to engage. That said, the delegation only goes so far. For example, as discussed earlier, the terms and conditions of the Affair Guarantee, and even the name of the service, clearly implicate the site in this ethically charged set of associations. A further instance I uncovered was where the Travellingman functionality encouraged users to 'pursue a little something on the side' (Figure 4) this feature also exists for women (Bort 2013). Ashley Madison and its bots work together to both provide distance from extra-partnership connections and to enable it.

Figure 4. Travellingman functionality

The final point I wish to make is in respect of the mutability of speculative devices. Can speculative devices loose their speculative quality? The answer to this question is somewhat bound up with the relational ontology I have set up in the definition of speculative devices and my subsequent analysis of Ashley Madison using actor-network theory. Evidence from the hack reveals that when the bots were present in the space they generated interactions that generated income. This is clear to see in the data I have presented so far. However, further data from the hack, as shown in Figure 5 reveals that when the bots were turned off income on the site dropped, and when they were turned back on, income levels increased. Here, Ashley Madison, engage in cycles of anticipation that have been associated with algorithms, where algorithm creators attempt (with varying degrees of success) to thoroughly know and predict their users (Gillespie 2014). Reinforcing this position, Avid Life Media have stated that approximately 70 per cent of the revenue from Ashley Madison is from repeat purchases (Avid Life Media 2015).

Figure 5. Turning bots on and off at Ashley Madison (Newitz 2015d)[iii]

Through this example we can see how the bots may loose an element of their speculative character for Ashley Madison because they have an understanding that bots will generate income. Yet, the bots simultaneously retain a speculative character because there is the chance that they will not continue to provide the outcomes expected by Ashley Madison as they come into being with a diverse group of users. In other instances, it is possible that the speculative character of a device is lost because it leads to guaranteed results. In the case created here, Ashley Madison employees could interpret the bots as producing guaranteed results because they appear to generate income. What is speculative then, is relational.

Conclusion

In this paper I have attended to two areas of increasing significance in relation to Web 2.0 since its announcement in 2005. The first is the turn to a focus on the non-human, and the second is the normalisation of dating apps in society. Through my analysis we can see how certain speculative devices operate and why. Moreover, as has been clear since 2005, and as richly illustrated in the preceding critical perspectives on Web 2.0 special issue of First Monday (Zimmer 2008), we can see how commercial interests in the internet continue. In particular, this case sheds light on how commercial interests in the web are transforming due to the spread of in-app economies. In addition, this work challenges the ideology of Web 2.0 in its evangelized version in that it suggests that it fails to anticipate and account for the participation of non-humans[iv].

Non-humans have always been involved in the process of dating and hooking up - the fake profile and the bot are further actors in this context. Moreover, they are actors with expected roles. As speculative devices, it is hoped, according to Ashley Madison that they will entertain, engage, educate and entice. Profiles and bots go beyond the use of the non-human as calculative devices in matchmaking whether this is a database or an actual robot such as Dexter, used for entertainment effect, to mathematically indicate the compatibility of a match on an eighties Australian dating television show (Figure 6). Unlike Dexter, the bots of Ashley Madison get some action.

However, the ultimate aim is for the fake profiles and bots to generate revenue for Ashley Madison. It is also important to acknowledge the role of the user-generated profiles in this context as speculative devices. The profiles users create are also intended to variously entertain, engage, educate and entice. The extent to which users intend for them to have a commercial aspect, for the purposes of escort services and sex work, is less clear. That said, several platforms are known to provide escort services, and links with sex work and thus this would be no surprise. Moreover, there is an increasing presence of businesses using profiles of contemporary dating apps rather than just deploying banner advertisements (e.g. see Young (2016)). For example, Grindr, a geo-locative hook-up app for men seeking sex with men has begun running pop up Uber ads. Need to get to a hook-up, had an alcoholic drink or don't have a car – we've an app for that - is the partnering logic at play. In the future could Ashely Madison see profile based advertisers of hotels and lawyers?

Although I have focused here on profiles and bots, speculative devices can take many forms and this means that they can be part of a variety of associations and their outcomes. For example, an analyst at Target used customer data to predict when women were pregnant so they could send discount vouchers to them. This resulted in the successful prediction of a high school girl's pregnancy and the revealing of this to her father when he found the coupons (Duhigg 2012). Further, Facebook has infamously, engaged the newsfeed in an attempt to manipulate user feelings (Kramer et al. 2014). Finally, and an advance on the unexpected nature of speculative devices is the case of Microsoft's Tay (@Tayandyou on Twitter). Tay was an experimental artificial intelligence infused chat bot released onto Twitter by Microsoft in March 2016. Tay assumed the form of a teenage girl, and was taken offline 16 hours after being released because she learnt from offensive tweeting by human users and became herself, offensive.

It is clear from the case I present here, and these additional examples, that speculative devices are implicated in our ethics. This raises the question of where morality is delegated to the non-human what do we do when we encounter the unexpected, or when we see harms being caused? If we are to continue the project of speculative methods, as we should, then we face difficulties in determining the ethics of our work. One might say that research is always subject to the unexpected. Beyond the obvious legally influenced politics associated with institutional ethics boards, I think we can agree that attending to the process of applying for ethical approval of our work is helpful in trying to anticipate the questions of morality and harm associated with our it.

However, where we deploy speculative method, and devices, we are delegating some of that work to non-humans that can act in arrangements in unexpected ways. These acts hold the potential to harm before we know what has happened and can intervene. If I was going to take an extreme philosophical position on this, I would say it becomes impossible to account for such eventualities in our applications for ethical approval. More realistically, if we engage speculative devices then we need to be clear about what these speculations are and what they could be. This is a similar process to that Crawford and Finn (2014) discuss in relation to the repurposing of social media data in the future, the potentials of the aggregation effect. We need to think through the best and worst of outcomes. However, in addition to just thinking about what might happen with our data and research in the future, we need to consider how, if and when we adjust where harms are caused.

We can never fully know the outcomes of sociotechnical arrangements. Speculative devices have the capacity (which may not be fulfilled) to generate actions, thought and feelings about the past, present and future. As a result of these possibilities, we need to give careful thought to how our research is conducted and understood where speculative devices are concerned in Web 2.0 contexts, and beyond.

Acknowledgements
I would like to thank Stefanie Duguay at QUT for providing comments on an early draft of this work. All images and screen captures in this article are the author's own unless otherwise stated.

Notes
i A journal paper fully describing the method is in review at the moment and a pre-publication draft will be made placed here as soon as one is available: http://benlight.me/the-walkthrough-method/
ii This was the copy available closest to the July 2015 hack.
iii Please note the plot area label in the diagram is in the original image, it is not an error of cutting and pasting.

iv I am grateful to one of the reviewers of this paper for suggesting this point of analysis to me.

References
Arvidsson, A. 2006. "'Quality singles': internet dating and the work of fantasy." *New Media and Society*, volume 8, issue 4, (August) pp. 671-691.

Ashley Madison 2016a Ashley Madison Terms and Conditions volume, issue, Accessed: 20 January 2016, https://www.ashleymadison.com/app/public/tandc.p?c=5.

Ashley Madison 2016b Ashley Madison Welcome Page volume, issue, Accessed: 20 January 2016, https://www.ashleymadison.com.

Ashley Madison 2016c Guaranteed Affair Programe: FAQ volume, issue, Accessed: 25 January 2016, https://www.ashleymadison.com/app/public/guarantee/detailsform.p.

Auger, J. 2013. "Speculative design: crafting the speculation." *Digital Creativity*, volume 24, issue 1, (March) pp. 11-35.

Avid Life Media 2015 Statement from Avid Life Media volume, issue, 31 August 2015. Accessed: 25 January 2016, http://media.ashleymadison.com/statement-from-avid-life-media-monday-august-31-2015/.

Bort, J. 2013 I spent a month on infidelity dating site Ashley Madison and was pleasantly surprise by how nice it was volume, issue, 18 December 2013. Accessed: 29 Jaunary 2016, http://www.businessinsider.com.au/how-to-use-cheating-site-ashley-madison-2013-12.

Brey, P. 2000. "Disclosive computer ethics." *Computers in Society*, volume 30, issue 4, (December) pp. 10-16.

Brunton, F. and G. Coleman 2014. "Closer to the Metal," Media Technologies: Essays on Communication, Materiality, and Society. In T. Gillespie, P. Boczkowski, J. and K. A. Foot (editors). Cambridge, MIT Press. pp. 77-97.

Burgess, J., B. Light and S. Duguay (2015). Digital Methods Preconference Workshop Materials: The Walkthrough. IR16 - Digital Imaginaries. Phoenix, USA.

Cain, P. 2016 What a map we can't show you tells you about your phone's location settings GlobalNews.ca volume, issue, 25 January 2016. Accessed: 29 January 2016, http://globalnews.ca/news/2471012/what-a-map-we-cant-show-you-tells-you-about-your-phones-location-settings/.

Callon, M. 1986. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," Power, Action and Belief: a New Sociology of Knowledge? In J. Law (editor). London, Routledge. pp. 196-223.

Campbell, J. E. 2004. *Getting It On Online: Cyberspace, Gay Male Sexuality and Embodied Identity*. New York, Harrington Parker Press.

Cheney-Lippold, J. 2011. "A new algorithmic identity soft biopolitics and the modulation of control." *Theory, Culture & Society*, volume 28, issue 6, (November) pp. 164-181.

City News 2013 Woman hurt typing fake profiles for dating site, $20M suit alleges City News volume, issue, 10 November 2013. Accessed: 25 January 2016, http://www.citynews.ca/2013/11/10/woman-hurt-typing-fake-profiles-for-dating-site-20m-suit-alleges/.

Correll, S. 1995. "The Ethnography of an Electronic Bar: The Lesbian Cafe." *Journal of Contemporary Ethnography*, volume 24, issue 3, (October) pp. 270-298.

Cox, J. 2015 Ashley Madison Hackers Speak Out: 'Nobody Was Watching' Motherboard volume, issue, 21 August 2015. Accessed: 21 January 2016, http://motherboard.vice.com/read/ashley-madison-hackers-speak-out-nobody-was-watching.

Crawford, K. 2016. "Can an Algorithm be Agonistic? Ten Scenes from Life in Calculated Publics." *Science, Technology & Human Values*, volume 41, issue 1, (January) pp. 77-92.

Crawford, K. and M. Finn 2014. "The limits of crisis data: analytical and ethical challenges of using social and mobile data to understand disasters." *GeoJournal*, volume 80, issue 4, (November) pp. 1-12.

Duhigg, C. 2012 How Companies Learn Your Secrets The New York Times Magazine volume, issue, 16 February 2012. Accessed: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp.

Dunne, A. and F. Raby 2013. *Speculative everything: design, fiction, and social dreaming*. Cambridge, MIT Press.

Feenberg, A. 1992. "From Information to Communication. Videotext," Contexts of Computer-mediated Communication. In M. Lea (editor). London, Harvester Wheatsheaf. pp. 168-187.

Feenberg, A. 1995. *Alternative modernity: The technical turn in philosophy and social theory*. Berkeley, University of California Press.

Gershman, J. 2015 Ashley Madison Data Breach Lawsuits Pose Privacy Test Wall Street Journal - Law Blog volume, issue, 15 December 2015. Accessed: 20 January 2016, http://blogs.wsj.com/law/2015/12/15/ashley-madison-data-breach-lawsuits-pose-privacy-test/.

Gibbs, J. L., N. B. Ellison and R. D. Heino 2006. "Self-presentation in online personals the role of anticipated future interaction, self-disclosure, and perceived success in Internet dating." *Communication Research*, volume 33, issue 2, (April) pp. 152-177.

Gillespie, T. 2003. "The Stories Digital Tools Tell," New Media: Theses on Convergence Media. In J. Caldwell and A. Everett (editors). New York, Routledge. pp. 107-123.

Gillespie, T. 2010. "The politics of 'platforms'." *New Media & Society*, volume 12, issue 3, (May) pp. 347-364.

Gillespie, T. 2014. "The Relevance of Algorithms," Media Technologies: Essays on Communication, Materiality and Society. In T. Gillespie, P. Boczkowski and K. A. Foot (editors). Cambridge, MIT Press. pp. 167-194.

Introna, L. D. 2005. "Disclosive Ethics and Information Technology: Disclosing Facial Recognition Systems." *Ethics and Information Technology*, volume 7, issue 2, (June) pp. 75-86.

Introna, L. D. 2007. "Maintaining the reversibility of foldings: making the ethics (politics) of information technology visible." *Ethics and Information Technology*, volume 9, issue 1, (December) pp. 11-25.

Jarrett, K. 2008 Interactivity is evil! A critical investigation of web 2.0 First Monday 13 volume, issue 3, (March). Accessed: 30 March 2008, http://firstmonday.org/ojs/index.php/fm/article/view/2140/1947.

Johnson, D. G. 2001. *Computer Ethics*. Upper Saddle River, Prentice Hall.

Karppi, T. and K. Crawford 2016. "Social Media, Financial Algorithms and the Hack Crash." *Theory, Culture & Society*, volume 33, issue 1, (January) pp. 73-92.

Kolko, B. E. 2000. "Erasing @Race: Going White in the Inter(face)," Race in Cyberspace. In B. E. Kolko, L. Nakamura and G. B. Rodman (editors). New York, Routledge. pp. 213-232.

Kramer, A. D. I., J. E. Guillory and J. T. Hancock 2014. "Experimental evidence of massive-scale emotional contagion through social networks." *Proceedings of the National Academy of Sciences*, volume 111, issue 24, (June) pp. 8788-8790.

Latour, B. 1992. "Where are the Missing Masses? The Sociology of a Few Mundane Artifacts," Shaping Technology/Building Society: Studies in Sociotechnical Change. In W. E. Bijker and J. Law (editors). London, MIT Press. pp. 225-258.

Latour, B. 2005. *Reassembling the Social: An Introduction to Actor Network Theory*. Oxford, Oxford University Press.

Lezaun, J. and L. Soneryd 2007. "Consulting citizens: technologies of elicitation and the mobility of publics." *Public Understanding of Science*, volume 16, issue 3, (July) pp. 279-297.

Light, B. 2007. "Introducing Masculinity Studies to Information Systems Research: the Case of Gaydar." *European Journal of Information Systems*, volume 16, issue 5, (August) pp. 658-665.

Light, B. 2014. *Disconnecting with Social Networking Sites*. Basingstoke, Palgrave Macmillan.

Light, B., G. Fletcher and A. Adam 2008. "Gay men, Gaydar and the commodification of difference." *Information Technology and People*, volume 21, issue 3, (August) pp. 300-314.

Light, B. and K. McGrath 2010. "Ethics and social networking sites: a disclosive analysis of Facebook." *Information Technology and People*, volume 23, issue 4, (November) pp. 290-311.

Magnet, S. 2007. "Feminist Sexualities, Race and the Internet: An Investigation of Suicidegirls.com." *New Media and Society*, volume 9, issue 4, (August) pp. 577-602.

Michael, M. 2012. "De-signing the object of sociology: toward an 'idiotic'methodology." *The Sociological Review*, volume 60, issue 1, (June) pp. 166-183.

Mowlabocus, S. 2010. *Gaydar Culture : Gay Men Technology and Embodiment in the Digital Age*. Farnham, Ashgate.

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

Newitz, A. 2015a Almost None of the Women in the Ashley Madison Database Ever Used the Site Gizmodo volume, issue, 28 August 2015. Accessed: 14 September 2015, http://gizmodo.com/almost-none-of-the-women-in-the-ashley-madison-database-1725558944.

Newitz, A. 2015b Ashley Madison Code Shows More Women, and More Bots Gizmodo volume, issue, 31 August 2015. Accessed: 20 January 2016, http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924.

Newitz, A. 2015c The Fembots of Ashley Madison Gizmodo volume, issue, 27 August 2015. Accessed: 20 January 2016, http://gizmodo.com/the-fembots-of-ashley-madison-1726670394.

Newitz, A. 2015d One Chart That Shows How Much Money Ashley Madison Made Using Bots Gizmodo volume, issue, 31 August 2015. Accessed: 25 January 2016, http://gizmodo.com/one-chart-that-shows-how-much-money-ashley-madison-made-1727821132.

Petersen, S. M. 2008 Loser Generated content: From Participation to Exploitation First Monday 13 volume, issue 3, (March). Accessed: 20 January 2009, http://www.firstmonday.org.

Phua, V. C., J. Hopper and O. Vazquez 2002. "Sex and Sexuality in Men's Personal Advertisements." *Men and Masculinities*, volume 5, issue 2, (October) pp. 355-363.

Pilieci, V. 2015 Ottawa man's lawsuit aims to penalize Ashley Madison for data breach Ottowacitizen.com volume, issue, 21 August 2015. Accessed: 25 January 2016, http://ottawacitizen.com/news/local-news/ottawa-mans-lawsuit-aims-to-penalize-ashley-madison-for-data-breach.

Race, K. 2015a. "'Party and Play': Online hook-up devices and the emergence of PNP practices among gay men." *Sexualities*, volume 18, issue 3, (March) pp. 253-275.

Race, K. 2015b. "Speculative pragmatism and intimate arrangements: online hook-up devices in gay life." *Culture, Health & Sexuality: An International Journal for Research, Intervention and Care*, volume 17, issue 4, (March) pp. 496-511.

Rogers, R. 2013. *Digital Methods*. Cambridge, MIT Press.

Roth, Y. 2015. "“No Overly Suggestive Photos of Any Kind”: Content Management and the Policing of Self in Gay Digital Communities." *Communication, Culture & Critique*, volume 8, issue 3, (February) pp. 414-432.

Shaw, D. 1997. "Gay men and computer communication: A discourse of sex and identity in cyberspace," Virtual culture: Identity and communication in cybersociety. In S. Jones (editor). London, SAGE Publications Ltd. pp. 133-146.

Wilkie, A., M. Michael and M. Plummer-Fernandez 2015. "Speculative method and Twitter: Bots, energy and three conceptual characters." *The Sociological Review*, volume 63, issue 1, (February) pp. 79-101.

Woll, S. 1986. "So Many to Choose from: Decision Strategies in Videodating." *Journal of Social and Personal Relationships*, volume 3, issue 1, (March) pp. 43-52.

Young, A. 2016 Hiring through Tinder got my business going with a bang The Guardian volume, issue, 14 January 2016. Accessed: 31 January 2016, http://www.theguardian.com/small-business-network/2016/jan/14/hiring-tinder-business-dating-mychefit.

Zetter, K. 2015 Hackers Finally Post Stolen Ashley Madison Data Wired.com volume, issue, 18 August 2015. Accessed: 25 January 2016, http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

Zimmer, M. 2008a Preface: Critical perspectives on web 2.0 First Monday 13 volume, issue 3, (March). Accessed: 30 March 2008, http://firstmonday.org/article/view/2137/1943.

Zimmer, M. 2008b The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0 First Monday 13 volume, issue 3, (March). Accessed: 3 May 2008, http://firstmonday.org/ojs/index.php/fm/article/view/2136/1944

Figures and Tables

Table 1. Bot talk – Adapted from Newitz (2015b)

Examples of initial approaches	Example of a follow up
hi how's it going how r u hello what's up so what brings you here? free to chat?	I'm sexy, discreet, and always up for kinky chat. Would also meet up in person if we get to know each other and think there might be a good connection. Does this sound intriguing?

Table 2. Excerpt from Ashley Madison terms and conditions 21 January 2016

Reasons given for bot/bot profile existence In order to allow persons who are Guests on our Site to experience the type of communications they can expect as Members, we may create profiles that can interact with them. …we may use these profiles in connection with our market research to enable us to analyze user preferences, trends, patterns and information about our customer and potential customer base. We also use such profiles to monitor user communications and use of our Service to measure compliance with the Terms. The purpose of our creating these profiles is to provide our Guest users with entertainment, to allow Guest users to explore our Services and to promote greater participation in our Services. and to assist you navigate and learn about our Site.
Interaction possibilities These profiles allow us to collect messages, instant chat and/or replies from individuals or programs… The messages they send are computer generated. Messages from the profiles we create attempt to simulate communications so that should you become Members you are encouraged to participate in more conversation and to increase interaction among fellow Members. the profiles may offer, initiate or send winks, private keys, and virtual gifts. Any one of these profiles may message with multiple users at the same or substantially the same times just like our users. Our profiles message with Guest users, but not with Members. Members interact only with profiles of actual persons. you cannot meet any of the images associated with our profiles in person and you acknowledge and agree that such communications are solely for your entertainment and to encourage your use of our Service.

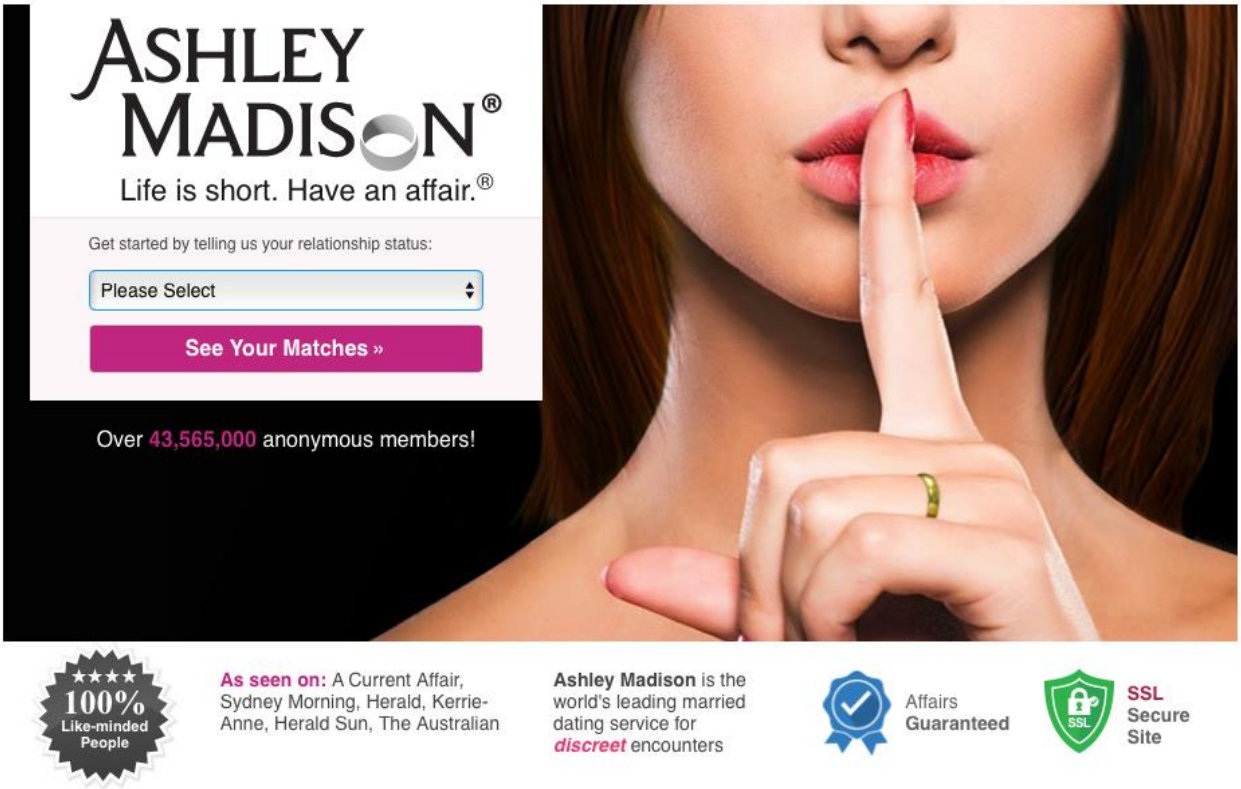

Figure 1. Ashley Madison welcome page (Ashley Madison 2016b).

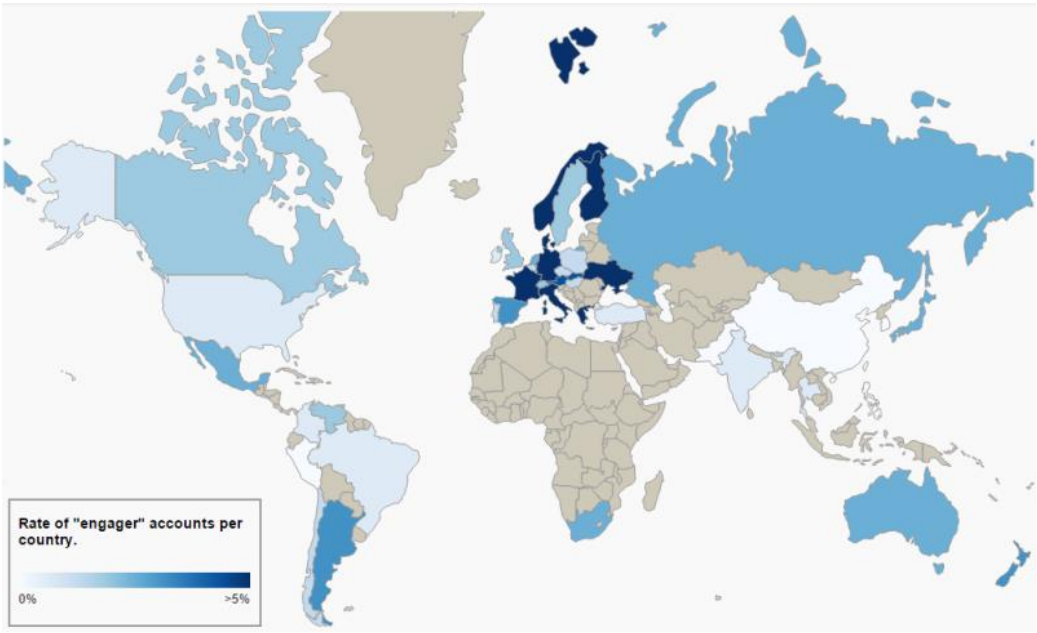

Figure 2. Ratio of engager accounts to female accounts by country Author: Jacob Perkowski see (Newitz 2015b)

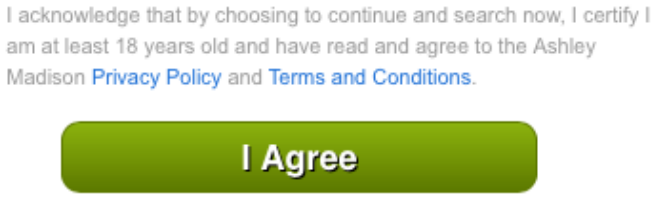

Figure 3. Accepting terms and conditions

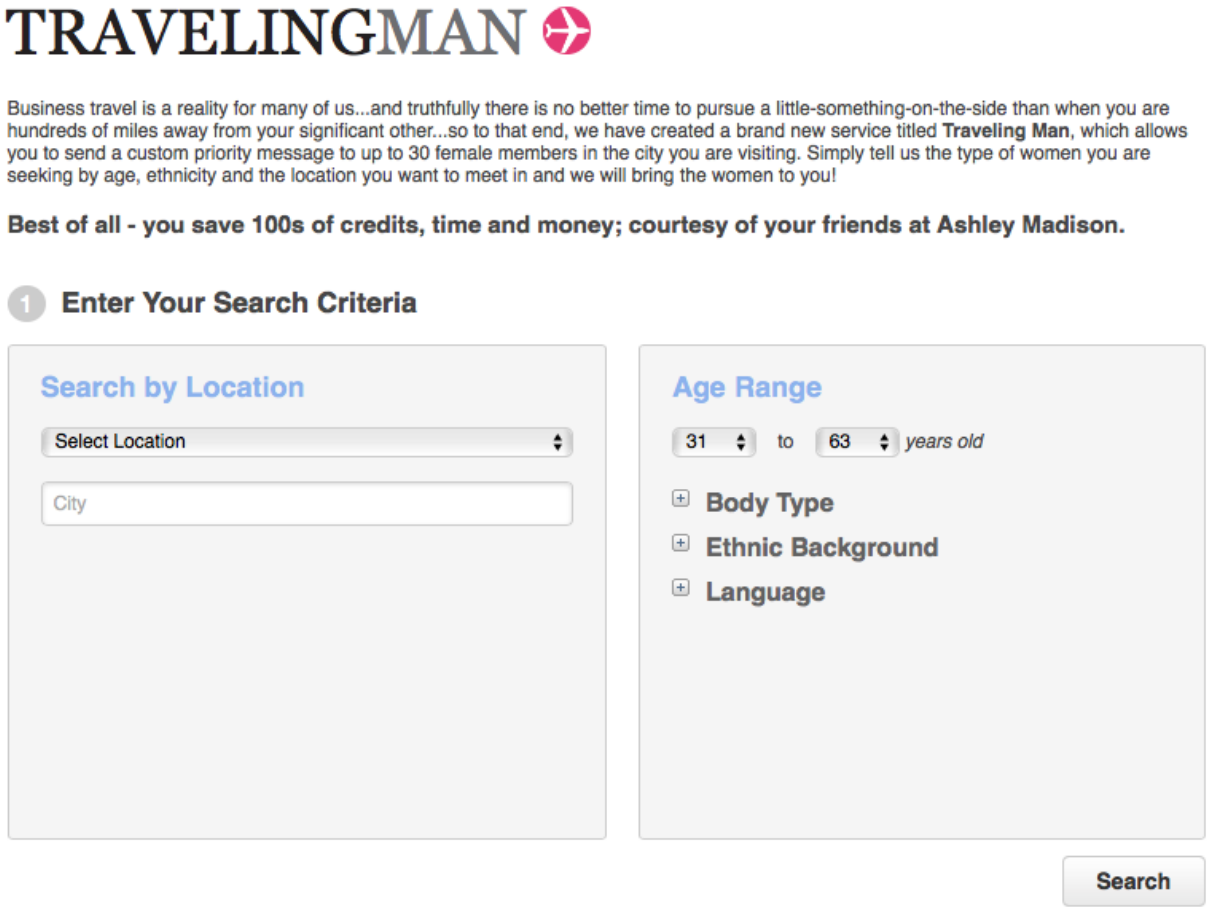

Figure 4. Travellingman functionality

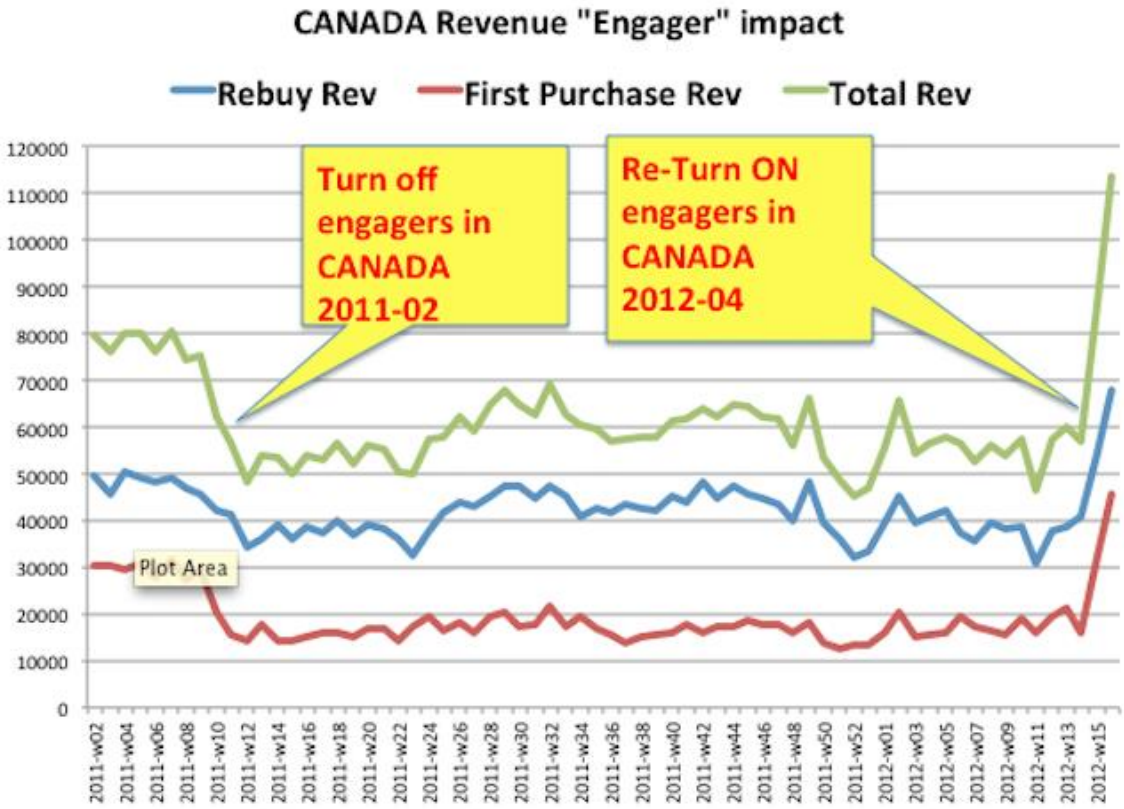

Figure 5. Turning bots on and off at Ashley Madison (Newitz 2015d)

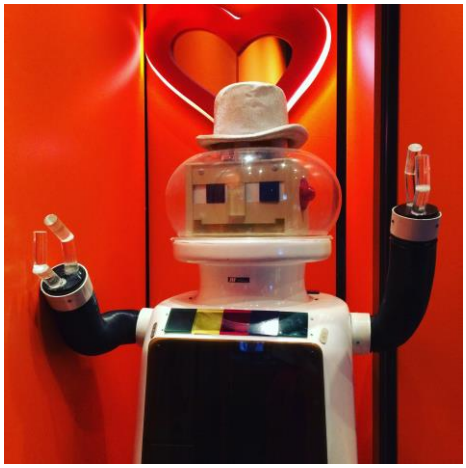

Figure 6. Dexter from *A Perfect Match*