The Hacking Monopolism Trilogy

Alessandro Ludovico, Neural, Bari, Italy, E-mail: <a.ludovico@neural.it>.
Paolo Cirio, Brooklyn, USA, E-mail: <info@paolocirio.net>.

Abstract

The three artworks of the *Hacking Monopolism Trilogy* are *Face to Facebook* [1], *Amazon Noir* [2] and *GWEI-Google Will Eat Itself* [3]. These works have much in common in terms of both methodologies and strategies. They all use custom programmed software to exploit three of the biggest online corporations, deploying conceptual hacks that generate unexpected holes in their well-oiled marketing and economic system. All three projects were 'Media Hack Performances' that exploited security vulnerabilities of the internet giants' platforms to raise media attention about their abuse of power. These performances were staged through the global mass media for millions of spectators worldwide. The processes of the projects are always illustrated diagrams that show the main directions and processes under which the software has been developed to execute the performances. Finally, all the installations we exhibited did not use computers or networks, focusing more on the display of the processes than on the technologies.

Keywords: Face to facebook, Amazon Noir, Google will eat itself, hacking, revelatory diagrams, big online corporations.

Face to Facebook is the third work in a series that began with *GWEI-Google Will Eat Itself* and *Amazon Noir* (the last two co-authored with Ubermorgen).
In *GWEI* we wanted to buy Google using its own money, generated by serving Google AdSense text advertisements first on a fake marketing website, and then on a network of hidden web-servers. With the money we got we automatically bought Google shares, so we were able to potentially buy Google via its own advertisements. By establishing this auto-cannibalistic model, we deconstructed the new advertisement mechanisms by rendering them into a surreal click-based economic model.

In *Amazon Noir*, Amazon.com's website was the vulnerable target. We eluded their copyright protection with a sophisticated hack of the 'Search Inside the book' service: by searching the first sentence of a book we obtained the beginning of the second sentence, and then by reiterating a few thousands searches, we obtained the whole text, redistributing it as pdf file through peer-to-peer networks.

In *Face to Facebook*, through special custom software, we collected "public profile" data from more than 1,000,000 Facebook users. Then we studied and customized a face recognition algorithm. The algorithm was programmed to 'group' the huge amount of faces we collected (and their attached data) in a few simple categories ('climber', 'easy going', 'funny', 'mild', 'sly' and 'smug' - working definitions), with some intuitive differences, for both male and female subjects. The software effectively extracted 250,000 faces that were connected to the relevant public data in our database. We established a dating website called *www.Lovely-Faces.com*, importing all the 250,000 profiles. Users trying to contact them ended up at their respective Facebook public profiles.

Fig. 1. Face to facebook installation at Transmediale festival, Berlin, 2011

The trilogy

We found a significant conceptual hole in all of these corporate systems and we used it to expose the fragility of their omnipotent commercial and marketing strategies. In fact, all these corporations established a monopoly in their respective sectors (Google, search engine; Amazon, book selling; Facebook, social media), but despite that, their self-protective strategies are not infallible. And we have been successful in demonstrating this.

There are other common themes in the projects. In all of them we stole data that is very sensitive for the respective corporations. With Google it was the "clicks" on their AdSense Program; with Amazon we started to steal the content of entire books, and with Facebook we stole a huge amount of public data profiles. In all the three projects, the theft is not used to generate money at all, or for personal economic advantage, but only to twist the stolen data or knowledge against the interests of the respective corporations. In *GWEI* it was the shares obtained through the money created by the AdSense program; in *Amazon Noir* it was the pdf books distributed for free; and in *Face To Facebook* it was the collection of profiles moved with no prior notice to a dating website.

Indeed all the projects, independently claim that some of the corporation's "crown jewels", including their brand image and marketing approaches, can be hacked, by focusing only on their established strategies and thinking in a "what if?" fashion. Furthermore, all of the projects were based on a "hacking" idea that, although pursued on a sophisticated level and with custom software, could have been applied by anybody with similar results. This is one of the fundamental values of these projects. Finally, all the installations we exhibited did not use computers or networks. We were trying to be coherent with the projects, but focused more on the display of the processes than on the technologies.

Face-to Facebook, smiling in the eternal party

Social networking is naturally addictive. It's about exploring something very familiar that has never been available before: staying in touch with past and present friends and acquaintances in a

Please reference as: [Author(s)-of-paper] (2013) [Title-of-paper] in Cleland, K., Fisher, L. & Harley, R. (Eds.) *Proceedings of the 19th International Symposium of Electronic Art*, ISEA2013, Sydney. http://ses.library.usyd.edu.au/handle/2123/9475
Page numbering begins at 1 at the start of the paper.

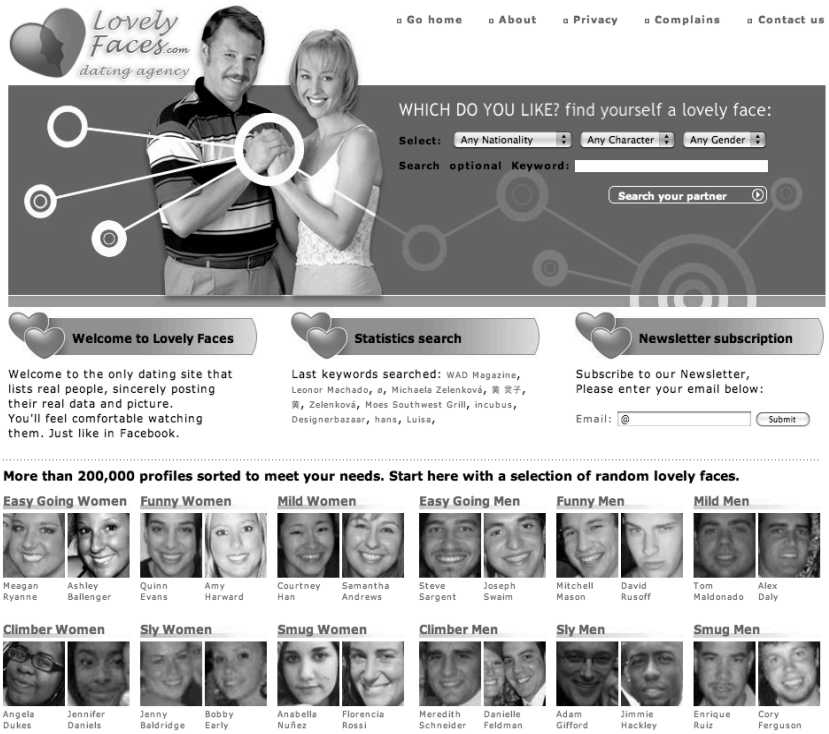
single, potentially infinite, virtual space. The phenomenon challenges us psychologically, creating situations that previously were not possible. Before the rise of social networking, former friends and acquaintances would tend to drift away from us and potentially become consigned to our personal histories. Having a virtual space with (re)active people constantly updating their activities is the basic, powerful fascination of the social network. But there's another attraction, based on the elusive sport (or perhaps urge) to position ourselves. The answer to the fundamental identity question, "who am I?" can be given only in relation to the others that we interact with (friends, family, work colleagues, and so on). And the answer to this question seems clearer after we take a look at our list of social network friends.

So an intimate involvement and (endless) questioning of our online identity (often literally juxtaposing with our physical one) is perpetrated in the social network game. But social network platforms are not public organizations designed to help support social problems, rather they support private corporations. Their mission is not to help people create better social relationships or to help them improve their self-positioning. Their mission is to make money [4]. Economic success for these corporations rests on persuading users to connect to the several hundred people who await them online.

The market value of these companies is proportional to the number of users they have. Facebook is valued at around 50 billion dollars [5]: it has one billion users [6]. The game can often translate into a form of social binging in which the number of friends a user has is never enough to satisfy. But what kind of space is Facebook? Facebook is not home - it is way larger and more crowded. And it's not the street, because you're supposed to know everybody in your space. Facebook is an eternal, illusory party, under surveillance and recorded for all time. Its structure invites you to first replicate and then enhance your real social structures, replicating your experiences on your own personal "screen space".

In this unending party, you meet and join old and new friends, acquaintances and relatives. As with most parties, everything is private, or restricted to the invited guests, but has the potential to become public if accidentally shared. Here the guests' activity and interests are also recorded through their posts in different formats and media (pictures, movies, trips, preferences, comments). It's an induced immaterial labour with instant gratification. Guests produce content by indirectly answering the question "who am I?" and they get new friends and feedback in the process.

Fig. 2. Lovely Faces dating website



In fact, Facebook's subliminal mantra seems then to be "be personal, be popular, never stop." It has even gone so far as to make it difficult to notice when a friend closes their account (you need to check the friend's list to have any idea) [7].

The more successful (and crowded) the party, the more the private funders are happy to put money into it. The price the guests are unconsciously paying is that they are giving away their (constantly updating) virtual identity. Guests, in fact, organize their own space, and therefore their own 'party', offering the party owner (Facebook) a connected, heterogeneous group of people who share interests. As such they offer what can be termed as "crowd-sourced targeting" – the indirect identification of people's targets and desires by the users themselves. In fact the spontaneously posted data provides an endless (almost automatic) mutual profiling, enriching and updating the single virtual identities, in a collective self-positioning. But can profile data be liberated from Facebook's inexorable logic? The answer is yes, but it's important to focus on the core of the Facebook profiles and see how they are recognized as virtual identities. First, the profiles sublimate the owners' (real) social actions and references through their virtual presences. Second, they synthesize their effectiveness in representing real people through a specific element: the profile picture. This picture, an important Facebook interface, more often than not shows a face, and a smiling one at that. Our face is our most private space and simultaneously the most exposed one. How many people are allowed to touch our face, for example? And, generally speaking, the face is also one of the major points of reference we have in the world.

There are even "special" regions of the human brain, such as the fusiform face area (FFA), which may have become specialized at facial recognition [8]. Faces are now so exposed that they do not remain private, but are thrust into the public domain and shared (they can even be "tagged" by other people). So any virtual identity (composed of a face picture and some related data) can be stolen and become part of another identity, through a simple re-contextualization of the same data.

Furthermore, 'face recognition' techniques can be applied to the purpose of grouping vast amount of Facebook pictures. This process is also quite

paradoxical, because the "surveillance" aspects (face recognition algorithms are usually used together with surveillance cameras) here are not used to try to identify a suspect or a criminal, but to capture and group people with similar somatic expressions. The resulting scenario is that different elements forming the identities can be remixed, re-contextualized and reused at will. Facebook data become letters of an unauthorized alphabet to be used to narrate real identities or new identities, forming new characters on a new background.

And this is a potentially open process that anybody can undertake. It becomes more tempting when we realize the vast amount of people who are smiling. When we smile in our profile picture, we are truly smiling at everyone on Facebook.

So any user can easily duplicate any personal picture on his hard disk and then upload it somewhere else with different data. The final step is to be aware that almost everything posted online can have a different life if simply re-contextualized.

Conclusions

Facebook is an endlessly cool place for so many people, and at the same time it's a goldmine for identity theft and dating - unfortunately, without the user's control. But that's the very nature of Facebook and social media in general. If we start to play with the concepts of identity theft and dating, we should be able to unveil how fragile a virtual identity given to a proprietary platform can be, and how fragile enormous capitalization based on exploiting social systems can be. This phenomenon will eventually mutate, from a plausible translation of real identities into virtual management, to something with no assumed guarantee of trust, crumbling the whole market evaluation hysteria that surrounds the crowded, and much hyped, online social platforms.

References and Notes

1. Face to Facebook, http://www.face-to-facebook.net, accessed 1 July 2013.

2. Amazon Noir, http://www.paolocirio.net/work/amazon-noir/amazon-noir.php, accessed 1 July 2013.

3. Google Will Eat Itself, http://www.paolocirio.net/work/gwei/gwei.php, accessed 1 July 2013.

4. Peter Lunenfeld, 'The Secret War between Downloading and Uploading', The MIT Press (2011), p.145.

5. Dominic Rushe, "Goldman Sachs suffers Facebook fiasco," *The Guardian* (2011), <http://www.guardian.co.uk/business/2011/jan/17/goldman-sachs-facebook-private-placement>, accessed 1 July 2013

6. Geoffrey A. Fowler, "Facebook: One Billion and Counting," *The Wall Street Journal* (2012), <http://online.wsj.com/article/SB10000872396390443635404578036164027386112.html>, accessed 1 July 2013.

7. Adam Hyde, Mike Linksvayer, Kanarinka, Michael Mandiberg, Marta Peirano, Sissu Tarka, Astra Taylor, Alan Toner, Mushon Zer-Aviv, 'What is Collaboration Anyway' in ed. by Michael Mandiberg "The Social Media Reader", NYU Press (2012), p.59.

8. Fusiform Face Area, <http://en.wikipedia.org/wiki/Fusiform_face_area>, accessed 1 July 2013.