

Hyves & Privacy

The Social Network as Superpanopticon?

ABSTRACT – More and more people are creating profiles on online social networks. This paper studies the amount of data they reveal in these profiles, and whether the collective profiles can be called a database and consequently act as a Superpanopticon as described by Poster.

Keywords

Panopticon, Superpanopticon, participatory surveillance, online social networks, Hyves

University of Amsterdam
Analyse Nieuwe Media II

08-01-2008

Martijn van Zwieten

1. RISE OF THE SOCIAL NETWORK

Raymond Spanjar is 30 years old, single and lives in Amsterdam. He studied psychology and economics at the University of Amsterdam and later co-founded both IEX.nl and Hyves¹. Raymond likes to listen to the classical works of Bach and lists *Amelie*, *Fight Club* and *Vanilla Sky* as some of his favourite movies. His favourite books include *Catch 22*, *De Ontdekking van de Hemel* and *Tipping Point*, and when he is watching television he frequently tunes in to *Da Ali G Show*, *Friends* or *Temptation Island*. Raymond is not a close personal friend of the author of this work. They have never even met. All this information about Raymond and more is listed on his personal Hyves profile², available for all to see.

Raymond is not the only person to have an online profile exposing a lot of personal details like this. Ever since the foundation of early social networking sites like Classmates.com in 1995 and Sixdegrees.com in 1997, online social networks have become increasingly popular. Especially in the last few years the number of people using online social networks has increased dramatically. Some of the most popular networks include MySpace.com, with a purported 300+ million accounts³, Facebook.com, which currently houses almost 43 million members⁴, and in the Netherlands the ever-growing Hyves has just recently surpassed the 5 million members mark⁵. Alongside these behemoths exists a vast number of other social networks varying in purpose from finding dates to comparing music tastes.

Acquisti and Gross (2005) observe that “while boundaries are blurred, most online networking sites share a core of features: through the site an individual offers a ‘profile’ – a representation of their sel[ves] – to others to peruse, with the intention of contacting or being contacted by others”. So, whatever your goal, if you wish to use these networks to their full extent, you will have to make public at least *some* personal information. And because you do want to use these networks, you will. But what happens to your information once you have created a profile?

It can be argued that every one of these online social networks, especially the ones with a more open character like MySpace and Facebook, effectively constitutes an extensive database full of personal information, available to practically anyone who wishes to take advantage of its contents. In this way, data can be extracted from the profiles for various purposes, thereby reducing the person behind the information to the information itself. People creating profiles at sites such as these are then taking part in what Mark Poster (1990) calls ‘participatory surveillance’. This in turn leads to the formation of a Superpanopticon, “a means of controlling masses in the postmodern, postindustrial mode of information” (Poster, 1990).

The goal of this paper is to show that the Dutch online social networking site Hyves can in fact be viewed as a database, and thus can operate as a Superpanopticon. In order to establish this, first a short overview of the theories of the Foucauldian Panopticon and the Superpanopticon will be given, after which an analysis of the Hyves network will follow. This analysis will consider the similarities and differences between Hyves and the Superpanopticon as described by Poster and Simon. Lastly, the privacy implications the findings of this study raise will be discussed.

¹ <http://www.hyves.nl/> .

² <http://raymond.hyves.nl/> .

³ <http://en.wikipedia.org/wiki/MySpace/> .

⁴ <http://midnightexcess.wordpress.com/2007/11/22/exercise-for-the-reader-facebook-member-stats/> .

⁵ http://hyvers.hyves.nl/blog/6856764/5_million_dollar_party/3HLY/ .

2. THEORETICAL CONSTRUCT

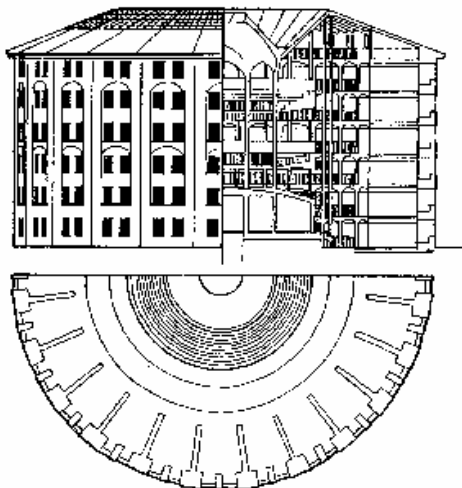
The following paragraphs will briefly describe the theories most important to understanding this writing. Because the theory of the Superpanopticon does not exactly stand on its own, but rather expands on an older theory of Panopticism, first the architectural model of the Panopticon by Jeremy Bentham and the resulting theoretical Panopticon by Michel Foucault will be discussed. After this Mark Poster's Superpanopticon will be explained.

Second, the method used to analyse the actual information published on Hyves will be described. A similar study undertaken by Acquisti and Gross (2005) states that there are three main characteristics that determine the privacy of a given profile. These characteristics will be explained before proceeding to the actual analysis.

2.1 Panopticism

2.1.1. Bentham's Panopticon

The original Panopticon is an architectural plan for a model prison as proposed by eighteenth century Utilitarian philosopher Jeremy Bentham, shown here on the left



(*Figure 1*). Up until then all criminals, regardless of their crime, were simply put together in dirty, overcrowded cells, most of which without even the most basic of provisions (King, 2001). Bentham believed that this prison would dramatically improve the way prisons worked: "Morals reformed – health preserved – industry invigorated – instruction diffused – public burthens lightened – Economy seated, as it were, upon a rock – the gordian knot of the Poor Laws not cut, but untied – all by a simple idea in Architecture!" (Lyon, 1993).

Bentham's Panopticon consisted of a large ring-shaped building with an observation tower located at the centre. The cells, located in the outer section of the building, would each hold a single prisoner. Each cell would have a window on the outside wall as well as the inside wall. The light that falls in from the outside would backlight the prisoners and insure their visibility to the inspector in the centre tower at all times. Through the use of Venetian blinds on the observation ports of the tower and "maze-like connections among tower rooms to avoid glints of light or noise" the observer remains permanently invisible to the prisoners (Barton & Barton, 1993).

In *Discipline and Punish: Birth of the Prison* French philosopher Michel Foucault provides insight in the working of the prison:

Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. So to arrange things that the surveillance is permanent in its effects, even if it is discontinuous in its action; that the perfection of power should tend to render its actual exercise unnecessary; that this architectural apparatus should be a machine for creating and sustaining a power relation independent of the person who exercises it; in short, that the inmates should be caught up in a power situation of which they are themselves the bearers. To achieve this, it is at once too much and too little that

the prisoner should be constantly observed by an inspector: too little, for what matters is that he knows himself to be observed; too much, because he has no need in fact of being so. In view of this, Bentham laid down the principle that power should be visible and unverifiable. Visible: the inmate will constantly have before his eyes the tall outline of the central tower from which he is spied upon. Unverifiable: the inmate must never know whether he is being looked at at any one moment; but he must be sure that he may always be so. [...] The Panopticon is a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without ever being seen (Foucault, 1979).

Now that the basic principles of Bentham's Panopticon are clear, the broader concept of the Panopticon as analogy for modern day western societies as envisaged by Foucault will be discussed.

2.1.2 Foucault's Panopticon

Foucault uses Bentham's Panopticon to illustrate the change in the way western societies punish its citizens. By the end of the eighteenth century people were still publicly punished for their crimes⁶, while in the early nineteenth century there were already tightly managed prisons. The Panopticon symbolizes this radical change in attitude towards punishing criminals: instead of publicly maiming them, they are punished in the relative privacy of the prison through manipulation of the psyche. In other words, punishment has shifted from the corporal to the non-corporal, from the body to the mind (King, 2001).

Foucault explains that the power and efficiency of the Panopticon are not a direct consequence of its architectural form, but rather stem from its disciplinary mechanism. This mechanism combines "surveillance and observation, security and knowledge, individualization and totalization, isolation and transparency" (Foucault, 1979). It is through this mechanism that the observer is able to alter people's behaviour, and through this mechanism that the observer gains power over the prisoners. For Foucault, this power is what is most important in the Panoptic model, which leads him to the conclusion that Panoptic model is not restricted to prisons alone. Rather, it should be viewed as a "generalizable model of functioning, [...] the diagram of a mechanism of power reduced to its ideal form" (Foucault, 1979).

As King (2001) writes, according to Foucault "Panoptic mechanisms, such as isolation, classification, and observation have become 'de-institutionalized' and circulate freely in modern society". In this way, the Panopticon serves as an analogy for the whole of western society, in that everyone is to some extent subject to these mechanisms at all times.

When viewed like this, everyone is constantly being watched and (re-)formed, with people being regarded as objects rather than subjects. Although this rather determinist view of society has been widely criticized for being too focused on (disciplinary) institutions while leaving out human agency, recent works dealing with online surveillance and consumer privacy have argued that Foucault's ideas are very applicable to contemporary, data driven societies nonetheless. Of these works, those

⁶ Foucault begins his book with a vivid description of the punishment of Robert-François Damiens in 1757 for attempted regicide: "the flesh will be torn from his breasts, arms, thighs and calves with red-hot pincers, his right hand, holding the knife with which he committed the said parricide, burnt with sulphur, and, on those places where the flesh will be torn away, poured molten lead, boiling oil, burning resin, wax and sulphur melted together and then his body drawn and quartered by four horses and his limbs and body consumed by fire, reduced to ashes and his ashes thrown to the winds" (Foucault, 1979).

by Mark Poster concerning what he has termed the “Superpanopticon” will now be discussed.

2.2 Superpanopticism

In his book *The Mode of Information* Mark Poster (1990) critiques Foucault for neglecting to notice that modern surveillance technologies are vastly different from those of the nineteenth century, instead of simply an extension of the old patterns. The data driven societies of the twentieth century use whole new methods to control their citizens, a situation that, rather than a Panopticon, Poster calls a Superpanopticon; a “system of surveillance without walls, windows, towers or guards”, that instead relies on databases to control its subjects (Poster, 1990).

These databases use a simple ‘language’ to sort the data inserted in them. Poster gives the example of a simple database where fields could be anything from “an individual’s [...] name, [...] social security number [and] age” to “unpaid parking violations, x-rated video cassettes rented [and] subscriptions to communist periodicals” (Poster, 1990). In this particular database, these parameters constitute the individual. In this way, the personal information contained in the database becomes an entity of its own, a ‘databased self’. Within the system this databased self is considered to be an accurate, or at least an accurate enough representation of the individual. As Bart Simon (2005) writes, “what makes databased selves different from our actual selves is that databased selves are more easily accessible, observable, manageable and predictable than we are”.

Perhaps even more important is the fact that these databased selves also possess a limited form of agency, in the sense that they can allow or restrict access to certain information. Consider for example the Albert Heijn ‘Bonuscard’, which besides giving the customer discounts also allowed the supermarket chain to register what the customer buys. With this information personalized offers can be made to the customer.⁷ As Gilles Deleuze (1992) remarks, “we no longer find ourselves dealing with the mass/individual pair. Individuals have become ‘dividuals’ and masses, samples, data, markets or ‘banks’”.

What becomes clear in the example of the Bonuscard is that apparently people are willing to ‘sell’ personal information for discounts on their groceries. Not just grocery discounts are used to gain personal information from potential customers, though. According to Simon,

the icon for superpanopticism is neither the eye nor the camera but the database or even better the form: the marketing survey, the census form, application forms, medical forms, etc... The operation that occurs at the interface between a subject and a form under superpanopticism is interpellation. We are interpellated by the form and the electronic infrastructure of which it is a part (Simon, 2005).

Through interpellation, “the process by which ideology addresses the (abstract) pre-ideological individual thus effectively producing him as subject proper”⁸, people are persuaded to hand over their personal information. This leads us to “the uncomfortable discovery that the population participates in its own self-constitution as subjects of the normalizing gaze of the Superpanopticon” (Poster, 1990). The Superpanopticon can thus be said to operate through a system of participatory surveillance.

⁷ Eventually AH yielded to the pressure of privacy activists and also made anonymous Bonuscards available.

⁸ <http://en.wikipedia.org/wiki/Interpellation> .

2.3 Analysis Method

Because of the limited scope of this study, only a small group of profiles can be analysed. Therefore only one hyve, a group of users with collective interests within the Hyves network, will be selected as study object. The selected hyve is the Privacy⁹ hyve, because of the relatively small amount of members and its theme. Because this hyve aims to stimulate discussions about online privacy, users within this hyve are suspected to be among the more careful about disclosing their personal information. Findings within this group are thus expected to be more than suitable for generalization to the whole of the Hyves network.

To avoid bias, a 'clean' profile has been created for the sole purpose of conducting this study¹⁰. This will allow for better access to profiles, as the default privacy settings will only allow registered Hyvers to view profiles, while at the same time avoiding any incidental 'friend of a friend' relationships that might occur when using an actual, connected profile.

To determine the scope of the participatory surveillance Hyves arguably enables, the methods as described by Alessandro Acquisti and Ralph Gross (2005) in their analysis of the Facebook network will be used to see how complete the Hyves 'database' really is. The analysis of the available information in the profiles will focus on three characteristics: the type and amount of information disclosed, the data validity and identifiability, and the data visibility and privacy preferences.

2.3.1 Types and Amount of Information Disclosed

This is the main part of the study, and will determine how much personal information is disclosed on each of the profiles and thus how extensive the 'database' is. This section will contain various sections from the study of

2.3.2 Data validity and Data Identifiability

In this part the data disclosed will be analysed for validity and identifiability. Because Facebook encourages its users to only fill in accurate information about their own person, and because a valid email address of an academic institution is required for registration on Facebook, Acquisti and Gross (2005) expected to find very little fake data in the profiles¹¹. Because Hyves allows its users to register with any e-mail address as long as it is valid, the same expectations will not do. This, however, is not expected to be a problem.

To check the validity of the profiles, the stated name on the profile and the provided image will be the primary focus. The stated name will be categorised as either real name – “the name appears to be real”; partial name – “only a first name is given”; fake name – “obviously fake name” (Acquisti & Gross, 2005). The image will similarly be categorised as either identifiable – “image quality is good enough to enable person recognition”; semi-identifiable – “the profile image shows a person, but due to the image composition or face pose the person is not directly recognizable. Other aspects however (e.g. hair color, body shape, etc.) are visible”; group image – “the image contains more than one face and no other profile information (e.g. gender) can be used to identify the user in the image”; joke image – “images clearly not related to a person (e.g. cartoon or celebrity image)” (Acquisti & Gross, 2005).

⁹ <http://www.dossierprivacy.hyves.nl/> .

¹⁰ <http://anm2.hyves.nl/> .

¹¹ It seems that it is no longer required to register an academic e-mail address, as any valid email address will suffice.

2.3.3 Data Visibility and Privacy Preferences

Although profiles on Hyves are by default viewable by anyone on the Hyves network, Hyves allows users to change their preferences to screen their profile from part of the network. This part will evaluate how many users actually use this option to protect their personal information from random users, i.e. make it invisible the “unconnected user (not friend of friend of friend of any profile)” created for this specific use (Acquisti and Gross, 2005). Since it is near impossible to determine if and which of the accessible profiles are only partly accessible, they will simply be classified as either accessible or restricted.

Now that the underlying theories and used methods are clear, it is time to move on to the conducted analysis of the Hyves network, after which it will be shown that it is in many ways similar to Poster’s Superpanopticon.

3. ANALYZING HYVES

As mentioned before, this part will contain the findings of the analysis of the Privacy hyve, which has the relatively small amount of 47 members. The different characteristics will be evaluated in the order mentioned above.

3.1 Types and Amount of Information Disclosed

Below is a chart that shows the most frequently found information on the Privacy hyve along with the percentage of profiles that reveal this information (**Figure 2**).

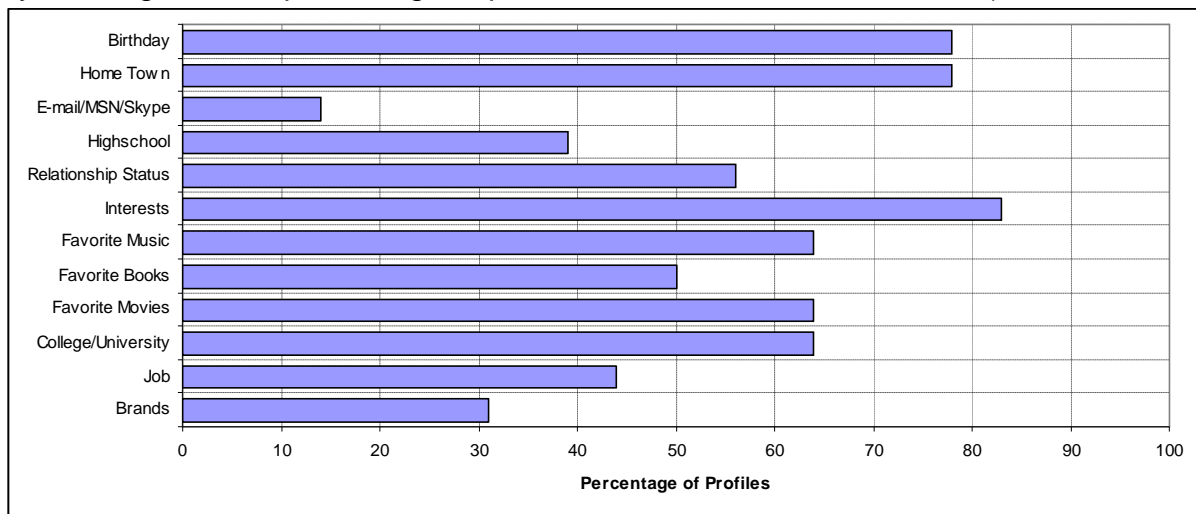


Figure 2 – Percentage of accessible profiles revealing various types of personal information

It should be clear from the graphic that even when someone is not related to you on Hyves, it is still possible to gather a considerable amount of personal data. Each profile had a picture, and most contained at least a birthday, home town and some of their interests. Contact information is not handed out as easily, as only 4 email addresses and 3 online messenger addresses were found. This does not completely protect Hyves members however, as on most profiles it was possible to link their full name to their home town, making it fully possible to contact them.

3.2 Data validity and Data Identifiability

This part showed that the majority of the accessible profiles shows the owners full name, regardless of who is visiting it (*Table 1*). A small group of people showed only their first name, and only 1 person used an alias.

Category	Number of Hyves Profiles	Percentage Hyves Profiles
Real name	28	78%
Partial name	7	19%
Fake name	1	3%

Table 1 – Categorization of name quality

Also, table 2 shows that most of the profiles, including the restricted ones, contained a picture “suitable for direct identification” (Acquisti & Gross, 2005).

Category	Number of Hyves Profiles	Percentage Hyves Profiles
Identifiable	27	57%
Semi-Identifiable	6	13%
Group Image	5	11%
Joke Image	9	19%

Table 2 – Categorization of user identifiability

3.3 Data Visibility and Privacy Preferences

The study showed that, even in this supposedly privacy-aware hyve, the majority of its members still allow other people with whom they have no connection whatsoever to access at least some of their data, if not all. Although available information differed from profile to profile, of the 47 members only 11 (or 23%) have changed the security preferences so as not to show their profiles to anyone outside of their personal network. It is very probable that this percentage is a lot lower when calculated over the whole network.

4. HYVES – A SUPERPANOPTICON?

So, having studied (part of) the Hyves network, is it safe to say that it can be regarded as a Superpanopticon? Well, it can certainly be regarded as a database. Also, the information in this database is in a very literal sense a copy of the individual, in that the profiles aim to convey as accurately as possible a sense of who the people are that they represent. You can't get much closer to Simon's 'databased selves' than this. They certainly are “more easily accessible, observable, manageable and predictable than we are” (Simon, 2005). His analogy of the form is perhaps even more fitting. Filling in your profile on Hyves is for the most part filling in the blanks that the owners of Hyves deemed to be the most important for character profiling. This in itself however does not justify the title of Superpanopticon.

What is missing from it is the theoretically present but for the most part practically absent 'higher power' that supervises this database. There is, not officially anyway, a person or an institution that collects and monitors the profiles stored on Hyves. The supervisor is pretty much the most important figure in the Panopticon as

well as the Superpanopticon, since it is from him that the idea of being watched and manipulated stems. As a result, Hyves and other online social networks alike can not technically be called a Superpanopticon.

They still have the potential to be exactly that, though. Acquisti and Gross themselves downloaded a total of 4540 profiles from Facebook, “virtually the entire [Carnegie Mellon University] population at the time of [the] study” (Acquisti & Gross, 2005). They also reference to an automated script that was used to contact 250.000 Facebook requesting their friendship, of which 75.000 replied positively (Jump, 2005). Apparently it is very possible to gain access to the complete personal profile of about 30% of the people you ask – without them ever knowing who you are. This means it is entirely possible for an organisation to harvest and store large quantities of personal profiles, be they from Hyves, Facebook or other networks, for their own personal use.

In conclusion then, it seems as though online social networks like Hyves cannot technically be called Superpanopticons after all. Through this study it has become clear however that the majority of the members on Hyves either do not know or do not care that their personal information is on display for virtually everyone to see, effectively creating a substantial database. Although no person or institution is known to exist at this time that acts as the supervisor in the Superpanopticon, exercising control over his subjects, it has been shown that it is not terribly difficult collect data from these networks. A database so full of very personal information could be very valuable for various organisations. Especially with more and more people stating their favourite brands, it could be very interesting for manufacturers of certain products to have access to this information. With just a first and last name and a home town it is relatively easy to find someone’s address for advertising purposes, for example. We might not be so far removed from the Superpanopticon as we like to think.

Because the examined group in this study was relatively small, further research could be done within a larger group of users, or perhaps even all of Hyves. Also, insight into why people do not screen off their personal information from complete strangers could prove invaluable for the furthering of online privacy theories. In any case, it has become clear that as long as our personal privacy is on the line, it is of great importance to further study the availability of personal information online and the ways in which this information might be compromised.

REFERENCES

- Acquisti, Alessandro & Gross, Ralph (2005) 'Information Revelation and Privacy in Online Social Networks (The Facebook Case)', *WPES'05*, November 7, 2005, Alexandria, Virginia, USA. Retrieved on Januari 3 from <http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf> .
- Barton, Ben & Barton, Marthalee (1993) 'Modes of Power in Technical and Professional Visuals', *Journal of Business and Technical Communication*, Vol. 7.1, 138-62.
- Deleuze, Gilles (1992) 'Postscript on the Societies of Control', *October*, Vol. 59, 3-7.
- Foucault, Michel (1979) *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan, New York: Vintage, 135-228.
- Jump, K. (2005) 'A New Kind of Fame', *The Columbian Missourian*, September 1
- King, Lyall (2001) 'Information, Society and the Panopticon', *The Western Journal of Graduate Research*, Vol. 10 (1), 40-50.
- Lyon, David (1993) 'An Electronic Panopticon? A Sociological Critique of Surveillance Theory', *The Sociological Review*, Vol. 41, 653-678.
- Poster, Mark (1990), 'Foucault and Databases', in *The Mode of Information* (pp. 69-98). Chicago, IL: University of Chicago Press.
- Simon, Bart (2005) 'The Return of Panopticism: Supervision, Subjection and the New Surveillance', *Surveillance & Society*, Vol. 3 (1), 1-20.