Opinion Piece

Second life, second identity?

Holger Wandt

is Principal Advisor at Human Inference.

Journal of Targeting, Measurement and Analysis for Marketing (2007) **15**, 195–197. doi:10.1057/palgrave.jt.5750046

INTRODUCTION

Information is precious and personal information is perhaps the most valuable information we have. Companies and organisations which collect consumer and customer data use this information to analyse and measure specific behaviour and align their sales techniques to personal needs.

But what about information that is recorded digitally? The average consumer feels that their personal information should be stored correctly, securely and reliably, but how does the same consumer feel about his or her data in community networks, such as the phenomenally popular Second Life? Will we be recording 'virtual' information as well as ordinary personal data in future? And will we then proceed to link this data? The price of information has many forms.

SAFE DATA?

The introduction of the electronic patient file (EPF) in Holland was originally planned for 1st January, 2006. This was, however, postponed for more than a year after it was revealed that security experts had accessed the data of 1.2 million patients. The experts had been able to get into the databases of two hospitals after obtaining permission from the hospitals concerned! Besides the delay in the introduction of the EPF, some very critical questions are brought up by the

security breach; no one is happy about the publication of their private medical information.

There is also a plan to create an electronic database for babies from 2007. This will contain information about the family situation and the environment, updated by doctors and nursing staff from the family healthcare department. In future, the plan is to link both the electronic patient file and the electronic child database to the civilian service number — the Dutch equivalent of National Insurance.

The aim of the civilian service number, which will replace the existing National Insurance number, is to simplify the exchange of data between civilians, government and other organisations. It contains relevant data such as first name, surname, date of birth, address and should reduce the administrative burden. The civilian service number has, however, another statutory framework which allows wider use. Consequently, this personal number can be accessible not only to government agencies, but also to financial organisations. Banks will thus be able to tackle identity fraud better. All this will enable the exchange and accumulation of all kinds of data, whereby the government and a range of other organisations will be given access privileges to certain parts of the file.

Uneasy about the idea? You could say so. The greatest obstacle to the introduction of the civilian service number is currently the fear of identity theft. This may seem contradictory, because one of the supposed aims of the civilian service number is to prevent identity fraud.

Correspondence: Holger Wandt,
E-mail: cdauidson@libertycomms.com

DIGITAL IDENTITY

Despite this fear, a start has nevertheless been made with the digitalisation and linking of personal data. DigiD stands for Digital Identity and is a joint system created by and for the Dutch government. Thanks to DigiD, civilians can use their password to access the online services of more and more government departments, such as councils, the tax department, the social insurance bank and the Center for Work and Income.

Digital identity thus appears to be a familiar concept in the Netherlands. In view of the fact that both government and industry are collecting more and more electronic data, it is interesting to find out where this data actually comes from. Companies are interested in surfing behaviour, transaction data, news consumption, spending patterns and a wealth of other information that can be gleaned from the internet. An extremely interesting phenomenon and an important source of information in this context is the community network Second Life.

VIRTUAL WORLD

Second Life is a 'multi-player online role-playing game'. The game was designed in 2003 by the American company Linden Lab and is based on a science fiction novel by Neal Stephenson. This community network — one of the fastest growing communities on the internet — currently has 2 million members worldwide.

What makes Second Life special is that this virtual world deals in real money. It has a completely integrated economy, in which craftsmanship, risks and innovative ideas are rewarded. The inhabitants create their own virtual products and services and earn Linden Dollars, a virtual currency, which can be exchanged for American dollars through the LindeX currency exchange.

In 2006, Second Life's gross national product was 64m dollars, which is more than that of many third-world countries. It is therefore not surprising that it is becoming increasingly attractive for companies to appear in Second Life. Philips, Reebok, Nike, Coca Cola, Toyota and Adidas have already created a virtual site where people can see and try out their new products.

The interesting question, however, is whether it will be limited to feedback for product innovation. How does Second Life use the data from community members, and how safe is the data actually?

PRIVACY

The first article in the Linden Lab Privacy Policy states: 'We collect personal information and usage statistics to maintain high-quality customer experience and deliver superior customer service'. This is a fairly generic statement, which can be interpreted in many ways. This is essential, because the company understands its commercial success extraordinarily well and explains to the potential participant what information will be used in what way, and how it could be made accessible to third parties.

When registering, the user decides on his/her first name and chooses a surname from a dropdown menu. The list of possible surnames is culturally very diverse. You can state your preference for names like Abdallah, Delgado, Gao, Ivanova, Izumi, Kovacs, Lehmann, Xingpeng, Young and Zwiers. One can only speculate about the reasons for such a list, although it is likely that a user would tend to choose a name that resembles his/her own name and/or fits into his country of origin.

A date of birth (that is also used for verification if a user forgets his/her password — users are encouraged to use their own dates of birth) and an e-mail address are also requested to complete the registration. Linked to the user behaviour in the community, this data provides a wealth of information for any company. The registration is also linked to an IP address, leading to speculation about the linking of virtual data with real personal data.

Of course this is not to insinuate that Linden Lab is involved in fraudulent practices, merely that the digital identity of consumers is closer to their real identity than they might think.

BIG BROTHER OR REALITY?

The ease with which a real identity can be converted into a digital identity and then misused is revealed in the recent judgment against the

owner of the New York company Compulinx. When choosing his favourite victims, this director stayed close to home and concentrated on his own employees. He used their identities to negotiate loans or make credit card applications. Together with his cousin, the fraudulent CEO made over 1 million loan requests in the names of the 50 employees in his company. The director was sentenced to 165 years in prison and given a fine of 5.5m dollars. His cousin faces a possible 35 years in prison and a fine of 1.25m dollars.

This is certainly another of those notorious 'American cases', but it does demonstrate that Big Brother (as in the concept described by George

Orwell in his book '1984' and not the reality television programme) is much of a reality than many might think. Personal information is indeed the most valuable information we have.

Certainly, Second Life and online communities more generally raise the question of data quality in the virtual world. If 'virtual' data is tied closely to real data what are the risks? What protection should be put in place and how do organisations go about ensuring that data is correct? With identity theft a growing phenomenon in the 'real' world — how long before it becomes so in the virtual world, costing both real and virtual money to business and people alike?