Legal Aspects of Virtual Identity

Jacob van Kokswijk, LLM, Msc ICT, PhD Psy

KAIST School of Culture Technology, South-Korea; Strathclyde University, UK; University of Twente, Fontys University, Capgemini Research, The Netherlands;

j.vankokswijk@fontys.nl

Abstract

A Virtual Identity is the representation of an identity in a virtual environment, consisting of a property of objects allowing these objects to be distinguished from each other. It can exist independently from human control and can (inter)act autonomously in an electronic system.

Since the Internet virtual identities (VIDs) are step by step interwoven in (trans)actions of persons but neglected in the law of persons and property. Most people don't realise that they are using VIDs when entering a marketplace (such as eBay), a chat room, or a dating site. They take for granted that an artificial identity is representing them. Given the emerging use of auction and transaction websites the sometimes public backlash against virtual shapes is not proportional to the daily growing accounts that use virtual identities for social and commercial transactions.

This paper describes the legal aspects of virtual identities in the context of virtual environments.

1. Introduction

Virtual identities are not a novelty, neither words such as "cyberian" or "Interreality" are neologisms. Almost 2.500 years ago people used pseudonyms to be anonymous, and were discussed imaginary worlds and the jurisdiction of law. For more than 150 years there was an internet, with chat rooms, virtual affairs and online identities. Going back in history, discussions were also held about shameless youth which handily used technology, about rude colonists who made their own rules in the conquered territories, and about floating people who were hopping between imaginary and realistic societies. Something has really changed: the automatic generated and operated software agents.

1.1. AI Powered Software Agents

The new service oriented applications will deliver and present the user (customer) a package of software, code and content, assembled and personalised by artificial intelligence (AI) 'powered' software agents. One can say that always somewhere is a real person as manager and operator behind the screens, but the practical situation is that the software is programmed to run automatic and autonomous, and to make an occasional choice in content management, individual needs (including the presentation requirements for the used devices) and the service offer in order to achieve the quality of service that is agreed between the user and the supplier (manufacturer). The AI-generated, modified and deleted ad hoc (software) agents behave themselves during their life as virtual identities.

Viewing the legal aspects of this phenomenon raise questions about the legal consequences. When non-human intelligent agents can live with virtual identity such as virtual aliens, who is responsible and liable for their actions in networks and systems on the earth?

Every investigator will question in advance 'who did what where when and how'? And every court will consider the admissibility, before focusing to suspects and evidence. Can a VID have personality? It is a human related identity? Does it have 'human' rights?

2. Hidden Hyperlinked Helpers

Cyberworld seems to expose the same colonialism as in past (e.g. America), with three differences:

1) you have to (and you can) develop your "new world" from scratch (digital space is empty; there is no ground like in the real world; you have to design something like "ground" if you need);

2) you are with your mind in cyberworld but with your body in a physical world (however, senses of your body are connected);

0-7695-3005-2/07 $25.00 © 2007 IEEE
DOI 10.1109/CW.2007.66

3) cyberspace doesn't have (as far as we know now) own base materials or alternative energy sources, to maintenance and survive itself.
Since the Internet virtual identities are step by step interwoven in (trans)actions of persons but neglected in the law of persons and property. Most people don't realise that they are using VIDs when entering a marketplace (such as eBay), a chat room, or a dating site. They take for granted that an artificial identity is representing them in selecting, bidding, or dealing during their absence. They mostly are not aware that a lot of electronic transactions are already completed by 'intelligent agents' (IA), even not when the IA presents itself to them as an artificial (virtual) identity.

On the other hand, Bogdanowivz and Beslay argue that it is generally known that opportunities to create fictitious virtual identities, potentially in fully fictitious environments are highly exploited in a digital context. [1] They say that the creation of virtual identities can be motivated by privacy and security concerns, convenience or leisure. Virtual identities may disappear without leaving traces. Consequently, the concept of these virtual identities is in contra-diction with criteria of permanency and physical reality that are expected in any identification process linking a physical individual to a set of digital data. Consequently the use of multiple 'virtual identities' will have to be regulated in the law of persons.

3. VID in Law of Persons

The VID is recognized in law of persons in applications of secure access (such as public key), information exchange and data mining. The idea of a VID was already used since long time ago by doctors who give each patient a pseudo-identity as provision for medical data. [a] Today the digital pseudo identity is used to let other doctors, pharmacists and lab assistants arrange some actions that are needed for the health of the anonymous but 'real' patient. With the modern advanced technology in hospitals all kinds of autonomous systems will interact.
The personal consequences of having more identities (available) and sometimes using them in an anonymous way seem not to be only fine and fun. On one hand it gives some fun and freedom in exploring your identity and the Internet, but on the other hand the procedures in using an electronic authentication to your real identity are becoming more and more stringent. E.g. in South-Korea where game players have to enter their National ID numbers before participating in an online game. [2]
As the virtual worlds' media, including the virtual communities and online game worlds, also are ruled by terrestrial related authorities (moderators, peer group specialists), sovereigns (e.g. administrators and providers) and treats of sanctions (e.g. blocking the access by a specific IP address), often the question will be 'who am I now?' Virtual worlds will become increasingly important in the future, for reasons that reach beyond games, so the fundamental rights around the individual personality is very important.
So far the three identified most important personal law topics are:
1) Privacy and anonymity in virtual environment;
2) Freedom of speech and thought in virtual environment;
3) Ownership of your virtual identity.
The question is not whether these rights should be allowed. It is self-evident that they should be. The question is how to deal with the consequences, and what other important rights should be addressed along with these.

Networks and computers support and replace information processes of both man and machine, without much ethical objection. Communication tools are used in and between the physical and virtual worlds, such as the emergence of personal parallel networks in both worlds and the resulting total hybrid experience. Although there are flaws and indistinct-nesses in the so-called virtual world, new ways of making contact and new communication channels have developed, such as SMS. These (im)possibilities and the technical characteristics of a modern communication networks as the Internet enable people, in combination with wireless communication systems, to (anonymously) move around in a virtual society and thee by have changing identities, relationships, transactions and habits.
Thanks to technologies as the Internet and mobile telephony, there is innovation not only in the contact and channel, but also in unexpected and unintentional new ways of talking, lurking and communicating have developed, once integrated in so-called virtual worlds. This takes place in one-on-one relationships as well as inside and outside groups, although technology in this area does not match up the required functionality (behaviour) of group communications. New forms of anonymity and dissociation (assuming multiple personalities) are cultivated in this virtual society and they lead to different behaviour patterns. Much

[a] The doctor keeps the relationship between the identity and pseudo-identity of the patient secret. The doctor could, e.g., entrust the identity and corresponding pseudo-identity to a trusted third party. The doctor records the medical data on the patient under his pseudo-identity. Other parties can now have access to the database con-taining medical information without learning the patient's identity.

attention is paid to this phenomenon from a sociological viewpoint in the academic world but less from other single and multi disciplinary research programs.

4. VID in Law of Property.

There are some relations between VIDs en property, mainly in property rights. In some – mostly money driven – cases (Reynolds) [3] the owner wants to claim the intellectual property of his avatars. In other cases the user of a VID in the virtual environment never wants to be associated in real life with 'that' virtual identity. That makes clear the popularity of anonymous participation in blogs, chat rooms and virtual worlds. In some situations that can be unacceptable when the VID executes harmful actions that are not welcomed by the victim.

In many cases law has established that the copyright in software subsists in code. But the way an avatar is displayed (at a screen) interacts with other system elements that are controlled by code; what individuates a specific avatar is not this code (which is common) but a set of data entries stored in a database or other wise. (Lee) [4] Hence rights in the game software do not apply to any given virtual appearance. Also when a player creates and uses a virtual identity such as an avatar (s)he is not creating a piece software open to copyright either.

Rights of publicity try to capture the relationship between identity and expressions of persona that resonate with the relationship between avatar and individual. These IP rights are outdated and wholly alien to what today happens in the virtual world and the cross media environment. Law follows society, but in this particular situation the law did not 'log in' at all. As Jacoby & Zimmerman put it: does it make sense that Tiger Woods could (in theory) own the persona of Michael Jordan? [5]

The economic aspect of virtual items such as avatars and identities has also tended to frame the debate about them in terms of property and an intersection between items, disputed acts, code and the law as it stands (Lastowka and Hunter) [6]. The law most commonly associated with property disputes over virtual world items is about copyright. Reynolds suggests that 'developer-publishers believe that they have a natural property right in virtual items as they create virtual worlds so own every aspect of them. Developer-publishers also tend to believe that the control that property rights grant them is needed for bringing coherence in a virtual world because that is necessary for the good of all players. Many players also believe that they have a natural right of property in both virtual items and especially avatars and identities, this stems also from law and the view that as there is no avatar in the box when the game is purchased so avatars must be created through the application of player effort, hence from labour-desert theory this is naturally their property.' However, keeping the ownership of your own virtual identity is a serious concern. Perhaps some things as virtual identities should not be understood as property.

5. Privacy aspects

The activities of 'intelligent' software agents – with or without virtual identity – will lead to numerous ways of processing personal data, such as the personal data an agent supplies to other agents during transactions, the personal data an agent collects or its user, and the data the agent-provider can extract from the use of his agent. [7]
To defend the privacy of the persons implicated, it is important that these personal data are used with caution, that they are necessary for legal purposes, that the data will not be disclosed to the wrong persons, and that personal data are not processed without the knowledge of the person(s) concerned. Therefore, the use of agents and the processing of personal data have to meet certain conditions that derive from the principles of privacy, which are laid down in most laws and international treaties. From all these conventions, regulations, and directives, we can abstract the privacy principles, be it:

- Anonymity,
- Purpose specification,
- Legitimate grounds,
- Compatible use,
- Proportionality, and
- Data quality.

These are strongly interconnected. Designers, developers, suppliers, and/or providers of software agents (with or without virtual identity) must consider these principles while they plan an agent, and must do so in the light of the fundamental right of an individual to decide when and in which circumstances personal data may be revealed. However, history teaches that every time a barrier arises, the creative developers will react in a contrary way and develop an alternative code or 'crack' to keep their privacy.

Do online personalities also have their right of privacy? The rules for data protection are taking away the privacy rights of personas. Your data is processed in a way you don't like. Warren & Brandeis [8] defined

in 1890 the right to privacy as 'the right to be left alone'. How to deal with all the security cameras and monitoring systems? More and more the Internet also is part of the surveillance, and 'you never be alone'!

In what way the virtual identity source can be used as a tool to preserving anonymity is unknown yet. The EU Ministerial Statement '… where the user can choose to remain anonymous offline, that choice should also be available online' [9], together with the so-called digital cash as trade by barter (as variable of 'give away, take away') enables many Internet users to use at least a real and a virtual identity, even in commercial transactions. 'The various services and activities available over the Internet must be examined, and wherever possible analogies drawn with existing services using older more established modes of communication and means of delivery. Such comparisons will provide a valuable insight into those areas where the possibility to remain anonymous is desirable and those where it is not.' In the proposal it was reported that anonymity on the Internet would be allowed the same free exposure and manifestation as in the physical world.

6. Customary Law in Cyberspace

After implementing the mediation program they instituted for eBay, Katsh et al (p 728) [10] report discovering that: 'As we encountered disputants and observed them as they participated in our process, we began to see eBay not from eBay's perspective, which assumes that eBay is the equivalent of a landlord with little power over how a transaction is finalized, but from the user's perspective. The more we saw of this, the more we became persuaded that disputants were, indeed, participating as if they were *'in the shadow of the law*.' The law whose shadow was affecting them, however, was eBay's law rather than the shadow of any other law.' [b] Thus, eBay is not just a marketing arrangement, but it also is a legal jurisdiction.

Parties agreed to participate in mediation 'at a very high rate' because of eBay law. Their primary concern was in maintaining their eBay reputations. As Katsh et al (p 729) explain, eBay's response to this public safety problem was not to install a police force to deal with problems after they occurred but to use an information process to try to prevent disputes from occurring. Since the public safety problem largely focused on unknown and perhaps untrustworthy sellers and buyers, eBay put in place a process for sellers and buyers to acquire reputations as trustworthy parties. Protecting one's feedback rating looms large in any eBay user's mind. As one guidebook to eBay points out, 'on eBay, all you have is your reputation'.

7. Code as law

Code looks cryptic, intangible, and isolated. But if code were transparent it can be recognisable structure for people, such as by-laws and codes of behaviour. Increasing the openness in code will help understanding the regulation of code. Code is not exclusive for regulators or nerds. By adapting free software and increasing the modularity of the code so that what it does is evident users can have enough control over functionality. The need for transparent code is clear: We need all hands on deck to respond.

The real 'i-war' phase, the use of advanced intelligent agents in the information warfare, has already been reached (Busuttil and Warren); (Busutelli) [11]. Computer nerds, criminals and crime fighters are using the same technology. Much of 'law' is concerned with security, or 'public safety', of course, but in cyberspace the issue is not one of physical safety; it is safety from harms or losses from spam, viruses, worms, fraud, identity theft, and so on. Many on-line providers of services, and many on-line organizations, want to be perceived as a cyber places where the risk of loses from such harms are low. Thus, 'law' is developing through the interaction of individual service providers and their customers and through the interactions of members of various cyber organizations.

8. Future thoughts about Virtual Identity

As in history new technology is regulated by old law. Equally most elements of the Internet usage and service content were regulated in some form or fashion – prior to the arrival of the Internet. Despite the calls by some for the development of Internet-specific law, or cyberspace law – similar to the Law of the Sea – the information technology is changing so rapidly for any 'sui' generic body of law that developing, implementing and maintaining is a lost race against the 24/7 Internet time.

Despite also the technology feed idea that the Internet culture is the same for all contributors, there are and will be local and cultural differentiations in compliance

[b] The terminology, 'in the shadow of the law' is generally attributed to Mnookin and Kornhauser (1979 p 968) in: R Mnookin, and L Kornhauser 'Bargaining in the Shadow of the Law: The Case of Divorce', Yale Law Journal, 880.
As Katsh et al. (2000: 728) imply, non-state made law (i.e. customary law) also casts a shadow. They acknowledge that shadows too, but they are not very significant if they do. Recourse to state-made law and public courts is rarely even mentioned.

with the law. The ‘ad hoc’ way of gradual adaptations of the tried and tested fundamental legal principles, as we have seen in free speech, economics, and in privacy and intellectual property protection, is likely to be more successful. Andersen argues that mediation and arbitration can solve cyber conflicts as it does with high technology disputes. [12] A code of conduct for legal mediation can be helpful.

Kesan and Shah point out that one of the most significant theoretical advancements in the legal academy is the recognition that law is not the only method of social regulation. [13] Other methods of social control include social norms and architecture. They argue that this has led researchers in a variety of disciplines to document how the architecture of information technologies affects our online experiences and activities. The recognition of the role of architecture has led policymakers to consider architectural as well as legal solutions to societal problems. Architectural solutions utilizing information technologies have been proposed for issues such as crime, competition, free speech, privacy, protection of intellectual property, and revitalizing democratic discourse, they say.

Finally, ways are examined in which laws can be used to create positive ethical models in individuals and groups. It is well known by policymakers and lawmakers that the form of societal control by passing a law which restricts the undesirable behaviour is very important. If the law becomes more widely accepted, people begin to reduce misbehaviour on the principle that it is `wrong' to do so.
However, the makers of policy and law are seldom aware of the societal structure of `cyberspace', and for this reason there is the danger that laws they make will not create the desired ethical model, but will instead create a backlash or revolutionary movement against the society. By observing the human behaviour in virtual communities and by continuing to take time to develop realistic policies and effective laws, it is possible to avoid such a backlash.

9. Conclusions

Anonymous identity in the cyberworld is – sooner or later – always legally tangible. Even an autonomic looking virtual identity (such as the bot in the software) is related to – at least one – human action. But – in legal view – being the perpetrator, supervisor or owner of a computer (-system, -network) is not the same as being accountable, responsible, culpable, and/or liable. Dependent to the law in force and to the specific situation a proof of evil intent or malice aforethought is necessary to be judged as guilty of something. The development of new investigation methods and tactics should be more multidiscipline oriented and be open for behavioural lead.

Virtual identities, created by a coincident of facts and autonomous executing, can not be ruled. Normally – same as robots – they have more benefits than disadvantage. As with nature disasters as a result of human interfere (like mud-slide after deforestation) we can’t rule everything after it seems to be out of control. As Rustad argues: ‘In contrast to a traditional crime scene, online intruders or forgers leave few digital footprints. DNA evidence, fingerprints, or other information routinely tracked in law enforcement databases are useless for investigating cyber crimes. In addition, computer records are easier to alter than paper and pencil records. Electronic robbers and forgers leave fewer clues than white-collar criminals who alter checks or intercept promissory notes.’ [14] Life is fun and risk, virtual life too. We accept that a chess computer is an interesting opponent to train your mind in move and countermove, but there could be a moment that we are checkmated by the computer generated chess mate.

Virtual worlds and illusory behaviour are of all time. The significant difference is the used medium, in combination with of the free elements of time and location. Upholding the law needs some adaptation by investigators and judges; however some hands-on experience (and using the power of the information technology) will surely help to understand the case. Many disputes in cases concerning a virtual topic can be solved by extrapolation to an equivalent in our regular physical world. Reason logically, by analogue or *a contrario* with cases in past, and learn from the past that order without law can satisfy too in particular situations.

Keywords:
Cyber, Cybernetic, Legal, Virtual, Identity, Reality, Pseudonymity, Intelligent, Artificial, Agents, Alias, Virtual Reality, Virtual Worlds, HCI.

10. References

[1] M Bogdanowivz, and I Beslay, 'Cyber-security and the future of identity', IPTS report, September, 2002 WWW: <http://www.jrc.es/home/report/english/articles/vol57/ICT4E576.htm>.

[2] 'Korea Produces Safer Online Registration Guidelines' WWW: <http://english.chosun.com/w21data/html/news/200610/200610020023.html>.

[3] R Reynolds, 'Hands off MY avatar ! Issues with claims of virtual property and identity' WWW: <http//www.ren-reynolds.com/downloads/HandsOffMYavatar.htm>.

[4] J Lee, 'Data-Driven Subsystems for MMP Designers: A Systematic Approach', in: Game Developer (2003) V. 10/ 8, pp 34-39.

[5] MB Jacoby, and DL Zimmerman, 'Foreclosing on Fame: Exploring the uncharted boundaries of the right of publicity', *New York University Law Review*, Vol 77 No5. (2002).

[6] GF Lastowka, and D Hunter, 'To Kill an Avatar', *Legal Affairs* (2003) WWW: <http//www.legalaffairs.org/issues/July-August-2003/feature_hunter_julaug03.msp>.

[7] RN Sobol, 'Intelligent agents and Futures Shock: Regulatory Challenges of the Internet', p 25 (Iowa J. Corp. L. 103 1999).

[8] M Warren & LD Brandeis 'The Right to Privacy. The Implicit made Explicit', *Harvard Law Review* (1890) pp 193-220.

[9] EU Ministerial Conference, Bonn, 6-8 July 1997. 'Anonymity on the Internet'. Recommendation 3/97. WWW: <http//europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html> and WWW: <http//europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/PublicHearingPresentations/EuroISPA.html>

[10] E Katch, J Rifkin, and A Gaitenby, 'E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of 'eBay Law', *Ohio State Journal on Dispute Resolution*, 15(2000) pp 705-734. WWW: <http://www.umass.edu/cyber/katsh.pdf>.

[11] T Busuttil, and M Warren, 'Intelligent Agents and Their Information Warfare Implications', 'Proceedings of the 2nd Australian Information Warfare & Security Conference 2001: 'survival in the e-economy', pp. 109-118, We-B Centre, School of Management Information Systems (Edith Cowan University, Perth, WA 2001)

T Busuttil, 'Intelligent Agents and how they can be used within an Information Warfare theatre'. (2006) In; *Journal for Information Warfare*. JIW Vol.6, Issue 1, 2007-03-31

[12] B Andersen, 'Mediation and Arbitration of High Technology Disputes', in: Lodder, Meijboom, and Oosterbaan (eds) '*IT Law - The Global Future: Achievements, Plans and Ambitions'*. Papers from the 20th anniversary International IFCLA conf. Amsterdam, June 1-2, 2006, (Elsevier, 2006).

[13] JP Kesan, and RF Shah, 'Shaping code (social norms)'. *Journal of Internet Law* 9.9 (March 2006): 3(11).

[14] ML Rustad, 'Private Enforcement of Cybercrime on the Electronic Frontier,' *Southern California Inter-disciplinary Law Journal*, 11(2001) p 98 in pp 63-116.

All WWW websites accessed 25-05-2007.