Alan Turing and the Matrix: Intelligent Systems for Law Enforcement in Virtual Worlds

Bart Schermer*

1 Intoduction

The research of professor van den Herik at Leiden University is focused on the following question: *Can a computer administer justice?*[1] At the basis of this question lies a deeper question: *can computers think?* When we look beyond this question, we see it in turn gives rise to fundamental questions such as: *What is intelligence? What defines creatitivity?* and *What makes us human?*

To avoid these difficult, almost unanswerable questions, Alan Turing, the father of modern artificial intelligence (AI) research, formulated the problem of determining whether a computer could think somewhat differently (Turing 1950). In Turing's view we can only determine whether an entity is intelligent on the basis of what we ourselves perceive to be intelligent behavior. If an observer could not distinguish between a computer and a human being in a conversation, the point of what defines intelligence would be moot since in practice there would be no 'functional' difference between men and machine. This concept can be brought in to practice via the well-known 'Turing test'. In this test a human test subject is engaged in conversation with either a computer or another human being. However, the test subject cannot determine through his senses whether he is conversing with the person or the computer. When after a set amount of time the test subject is unable to determine on the basis of the conversation whether is his counterpart is human or computer, the computer is said to be intelligent (Turing, 1950).

While up until now no computer has actually passed the Turing test, computers can perform impressive feats of intelligence in well-defined areas such as theorem proving and problem solving (Kemal, 2006). However, it is possible that computers will ultimately reach (and even surpass) the level of intelligence possessed by human beings (Kurzweil, 2005). How this may affect our society can be seen in science fiction. Since popular culture expands on the ideas of science, it is oftentimes an excellent means by which to infer future developments. When we look at artificial intelligence research we can establish that it is extremely popular within science fiction books and films.

In science fiction, artificial intelligence entities come in all shapes and sizes. There are 'androids' which are physically and mentally indistinguishable from humans, disembodied intelligences that reside inside a computer or network and

* Bart Schermer works at ECP.NL, Platform for eNederland, and is also connected to eLaw@Leiden, Center for Law in the Information Society, Leiden University. Email: b.w.schermer@law.leidenuniv.nl.

[1] Kunnen Computers *Recht*spreken? (Van den Herik, 1991)

do not have physical properties, and artificial intelligence entities that have a physical presence (or more accurate: a physical representation) in a virtual environment. The most striking example of the latter is Agent Smith from the hit movie the Matrix[2].

Agent Smith is an artificial secret agent who operates within a virtual world known as 'The Matrix'. Agent Smith is of particular interest to this article since he demonstrates the possibilities for law enforcement in virtual environments. This example from science fiction raises the question whether virtual worlds such as World of Warcraft and Second Life can be policed by virtual agents akin Agent Smith.[3] As such, I formulate the problem definition for this article as follows:

> *Can an artificial police agent bring a (virtual) criminal before professor van den Herik's artificial judge?*
>
> *And if so, is this artificial police agent bound by the same rules of criminal procedure as his real counterpart, or do we need new rules?*

2 A brave new virtual world

In recent times the popularity of Massively Multiplayer Online Roleplaying Games (MMORPGs) and 'virtual worlds' has surged. In both the MMORPGs and the virtual worlds players assume the role of a digital alter ego (an avatar) through which they interact with the virtual world and engage in social contacts with other players. While the MMORPGs can be best be characterized as games (i.e., they have a competitive element, set goals for the players, and to some extent follow a pre-determined narrative), the virtual worlds are aimed more at social interaction and in general do not have any competitive elements. Examples of MMORPGS are World of Warcraft, Lineage, and Eve Online. Examples of virtual worlds are Second Life and Project Entropia.[4]

Due to the popularity of the MMORPGs and virtual worlds, where millions of people now interact on a daily basis, their relevance is becoming ever greater within our society. This relevance is heightened by the fact that virtual worlds are not isolated from the real world. While it is possible to view the 'virtual world' and the 'physical world' (i.e., the real world) as two distinct environments, they interact to a large extent. As such the boundaries of the physical world and the virtual world become blurred. The area where the virtual world touches upon the real world can best be described as 'interreality' (Kokswijk, 2003). A good example of this phenomenon is people willing to pay real money for virtual goods. Interreality raises all sorts of interesting possibilities for social interaction and economic activities, however it can also lead to various forms of deviant behavior.

[2] Warner Brothers, 1999.

[3] I will not engage in an ethical or political debate about the need or even the desirability of law enforcement in virtual worlds. This article is merely about the possibility for it, and the legal basis that it may require.

[4] See, for instance, `www.wow-europe.com`, `www.lineage2.com`, `www.eve-online.com`, `www.secondlife.com`, and `www.project-entropia.com`.

2.1 Crime in virtual worlds

The notion of crime is somewhat difficult in MMORPGs and virtual worlds. First of all, defining certain types of behavior in virtual worlds as deviant implies almost by definition regulation of the virtual environment by a central authority. For many players however, the different social structures and rules of virtual worlds are reasons to take up a 'second life'. Moreover, particularly in MMORPGs, crimes such as theft and murder are oftentimes an integral and/or accepted part of the game.[5] In virtual worlds this may not necessarily be the case, but still, the rules of social conduct within virtual worlds may differ from those in the real world. Thus, functional equivalence of the rules of criminal law in MMORPGs and virtual worlds is not a given.

Having said this, there are certain types of behavior that could be viewed as deviant. We can distinguish various different possible forms of deviant behavior in MMORPGs and virtual worlds. For the purpose of this article we may differentiate between three types of deviant behavior, viz. cheating, virtual crime, and preparatory actions.

Cheating. Cheating is behavior aimed at breaking or bypassing the rules of the virtual world in order to gain certain benefits within the world (i.e. higher stamina, better equipment, or more experience points). Cheating oftentimes involves altering the game dynamics or otherwise influencing the game without the consent of the maker.[6] In general, the types of behavior that are considered cheating are defined within the End User License Agreement (EULA). Cheating is most prevalent in the MMORPGs since in these types of virtual worlds it is most relevant to gain an illegal edge.

Virtual Crime. I make a distinction between cheating and virtual crime since the latter is a more serious form of illegal conduct within virtual worlds.[7] Whilst cheating is aimed at gaining an advantage within the game and does not harm other players directly, virtual crime can harm other players in several ways. The fact that players and society as a whole are harmed by virtual crime opens up the way for criminal law in virtual worlds (Viersma and Keupink 2006, p. 42). Some ways in which virtual criminals can harm other players are: 1) stealing or embezzling their virtual goods which present a real world value, 2) slander and defamation of avatars and their owners, 3) identity fraud (i.e. hijacking an

[5] For instance, in the MMORPG Eve Online a player named 'Cally' took off with all the funds people deposited in the virtual bank he operated. These funds represented a real world value of over one hundred thousand euros. However, since scamming other players is an integral part of Eve Online's game dynamics, Cally was not prosecuted.

[6] Behavior that is not forbidden might still be considered cheating by a majority of players, however, for this article the defining element of cheating is behaving in violation of the official rules of the virtual world as set forth by the maker.

[7] From this point onward, I shall use the term 'virtual worlds' to indicate both the MMORPGs and the virtual worlds.

avatar, or using personal data gathered in the virtual world for fraud in real life).[8]

The forms of deviant behavior mentioned above, directly impact players in the virtual and/or real world. There is however another type of behavior that might also have a bearing on the real world, albeit indirectly. This is 'in world behavior' that might cross-over to the real world where it can do actual damage. An example of this can be found in Second Life where 'grown up' avatars engage in sexual acts with avatars that look like minors. Since this 'virtual pedophilia' might stimulate pedophilia in real life, Dutch parliament is contemplating the introduction of laws banning virtual sex with virtual minors.[9]

Preparatory Actions. Internet has contributed greatly to the communication capabilities of organized crime and international terrorism. Through websites, email, internet relay chat (IRC), and instant messaging programs (AOL IM, MSN), criminals and terrorists can communicate effectively and in relative safety. However, criminals are also aware of the fact that their modes of electronic communication can be monitored by law enforcement and intelligence agencies. Therefore, they may turn to less conspicuous forms of communication such as interacting with one another in MMORPGs or virtual worlds.

3 Surveillance in Cyberspace

It is likely that with the increasing popularity of virtual worlds, virtual crime will become a more serious problem over time. Therefore, at some point in time law enforcement in virtual worlds may become necessary. When it comes to the policing of cyberspace, surveillance plays an important role. For the context of this article, three levels of surveillance play a particular role, viz. 1) surveillance at the IP level, 2) surveillance at the application level, and 3) surveillance at the interaction level.

At the IP Level. The most rigorous form of surveillance in cyberspace is done at the IP level. By means of lawful interception of internet traffic, law enforcement agencies can monitor all communications from or to a (potential) suspects' computer. While in theory this is the most complete and effective form of internet surveillance, it does raise serious legal and technical issues.

From a technical viewpoint, the main issue with interception of IP traffic is that every single IP packet needs to be intercepted and screened in order to reconstruct messages (Branch 2003). While some of these problems can be solved by installing a 'sniffer' (a device that only records internet traffic to specific IP-addresses), lawful interception of internet traffic remains difficult, in particular when it is unclear which IP addresses need to be screened. From a legal viewpoint

[8] It is possible that when a virtual crime is committed, a normal cybercrime (such as hacking a server) is also committed (see Viersma and Keupink 2006).

[9] http://www.nrc.nl/media/article636285.ece /Kamer_wil_verbod_op_kinderporno_in_Second_Life (in Dutch)

the main objection to the interception of IP traffic is that the infringement of the personal sphere is substantial.

At the Application Level. The second possibility for surveillance in cyberspace is at the application level. Instead of intercepting all internet traffic, only traffic to a particular service (for instance an email service or online game service) is subject to screening (Branch 2003). This screening takes place after the information has reached the provider, eliminating much of the technical and legal issues that arise in the context of lawful interception of IP traffic. While this approach is more feasible than interception of IP traffic, law enforcement agencies must know in advance what applications to monitor.

At the Interaction Level The third level of surveillance is on what I like to call the 'interaction level'. On this level the law enforcement officer takes on the role of a normal user. In this role the officer can browse the internet in search for illegal content, monitor chat conversations, and walk around in virtual worlds. An officer can also interact with other users, including potential suspects.[10] It is this interaction level that could be of particular interest for future law enforcement in virtual worlds.

Law enforcement at the interaction level has the positive effect that law enforcement officers can patrol the virtual world without using infringing investigative methods such as the interception of IP traffic. When a reasonable suspicion has risen at the interaction level, it is possible to use more infringing investigative powers such as lawful interception of IP traffic.

4 Law Enforcement in Virtual Worlds: Human or Machine?

We have established that crime in virtual worlds is a possibility, and that the societal impact of virtual crime might become more significant over time. As such, surveillance and law enforcement in virtual worlds might become necessary. This will put additional strain on the capacity of current law enforcement. It is therefore worthwhile to examine whether intelligent systems can take over some of the surveillance tasks normally executed by law enforcement officers.

When it comes to the automation of law enforcement in virtual worlds, software agents are best suited for the task. A software agent is an intelligent program that is capable of autonomous and flexible action (Luck 2004, p. 3).

It is my belief that software agents can assist humans with the three types of surveillance mentioned in paragraph 3. In the long-term software agents may even replace human law enforcement officers altogether (Schermer 2007). When software agents operate within a virtual world, they can take up several different roles. Below I shall describe three possible roles.

[10] While general surveillance of the internet and virtual worlds may be considered part of the normal police task, actually engaging in interaction with other users must be considered a special investigative power.

Unobtrusive Agents. A first way in which software agents could conduct surveillance tasks, is as part of an invisible infrastructure of surveillance. In this scenario agents are disembodied and do not actively participate in the virtual world itself. Rather they observe the virtual world (or the dataflows that make up the virtual world).[11]

Police Officer. A software agent can also have a presence in the virtual world as an avatar. In this role the software agent looks like just another avatar in the virtual world. When the agent is sufficiently intelligent, it may interact with other players and the environment. In order to distinguish the software agents from other agents, its avatar might be the virtual representation of a real world police officer. In this way the other inhabitants of the virtual world are aware that a law enforcement agent is present. Players could report cheating or virtual crime to these virtual police officers, instead of going through customer support or posting messages on an online forum.[12] This use of software agents provides an interesting alternative to the use of real world support staff and moderators.

Undercover Agents. A final possibility is software agents actually interacting with people, including potential suspects. This is where the vision of Alan Turing as described at the start of this chapter comes clearly into focus. When another player is unable to determine whether he is dealing with a software agent or a real person, software agents can effectively take over the tasks of law enforcement officers. A software agent for instance could take up the shape of a child on Second Life in order to unmask potential pedophiles. Or a software agent could act as an undercover agent and infiltrate a group of suspects (Schafer et al. 2004).[13]

5 Legal Framework

We may conclude that various forms of crime can manifest themselves in virtual worlds, and that software agents might be used to combat these crimes. However, the question is whether software agents are actually allowed to do so. While this is just one of the many questions concerning the legal aspects of software agents, I shall limit myself to a discussion of the legal basis for agent-enabled surveillance.[14]

Legal Basis. The most important issue with the use of virtual agents for law enforcement purposes is establishing the legal basis for their use. In my opinion we must establish the legal basis for the use of software agents in virtual worlds

[11] Given the limited space, I shall exclude this type of agent-enabled surveillance from further discussion.

[12] In many virtual worlds support staff are present to assist players with questions.

[13] In many virtual worlds, in particular in MMORPGs players organize themselves into 'guilds' or 'clans'.

[14] For an overview see: Schermer, Durinck, and Bijmans, 2005.

by examining what they are used for. In this sense I would like to distinguish between the use of agents to detect and prevent cheating, the use of agents to detect and prevent virtual crime, and the use of agents in (pro-active) investigation of 'real world' crime.

It is my opinion that the legal basis for the detection and prevention of cheating can be provided by the End User License Agreement, while the use of agents to detect and prevent virtual crime, and the use of agents in (pro-active) investigation of real crime, require a basis in the law of criminal procedure. The reason I make this distinction is that possible infringements on privacy and liberty will sooner take place in the context of an investigation into criminal acts.

Enforcement of the End User License Agreement (EULA). A first possibility is to use software agents to search for behaviour that is in violation of the EULA (i.e., cheating). The legal basis for this type of enforcement is the EULA itself. To raise awareness under players that software agents are present in the virtual world, software agents could take on the appearance of virtual police officers. This would limit the likelihood of infringements on privacy and could raise the level of trust in the virtual world.

Enforcement of Criminal Law. When it comes to enforcing criminal law (i.e., the detection and prevention of virtual crime, and investigations into the preparatory actions for real world crime), it is my opinion that a basis must be sought in the law of criminal procedure. The reason is that the use of intelligent systems for electronic surveillance and, ultimately, undercover activities, could form a threat to privacy and individual liberty. As such, the legal basis for the use of software agents should be the law of criminal procedure. However, this brings up questions regarding the exact legal status of software agents in the context of law enforcement. Are they merely investigative tools? Must their use be considered a special investigative power? Or do they need a separate status in the law of criminal procedure altogether? (Schermer 2007, p. 158). At this time, answers to these questions cannot be found in the law of criminal procedure in the Netherlands and the United States, since there are no provisions that deal specifically with the use of software agents for law enforcement purposes (Schermer 2007, p. 209). If we are to use software agents to police virtual worlds, it is my opinion that new rules for their use must be put in place.

Due to the limited length of this article I'm unable to go into any detail about these new rules. However I shall make two general remarks. When we examine the use of software agents for surveillance on the interaction level, it is my opinion we must distinguish between software agents that merely 'patrol' cyberspace, and software agents that interact more directly with inhabitants of virtual worlds. For the most part, I feel that the first type of surveillance is part of the normal police task and that as such new rules are not necessary. When software agents actually start interacting with inhabitants of the virtual world, new rules will likely be necessary. The reason for this is that, in general, these

agents will be more intelligent and will operate within the personal sphere of the player, where they could form a greater threat to privacy and liberty.

6 Conclusion

From this article we may conclude that in order to combat cheating and crime in virtual worlds, 'artificial police agents' may be employed. As of yet, these systems are not very advanced and can be used mainly to assist human beings in governing virtual worlds. However, as we move closer to the vision of strong artificial intelligence, more advanced software agents may be employed to combat crime in virtual worlds. When these intelligent systems arrive we must ensure that the legal basis for their use is codified within the law of criminal procedure.

With the rapid advances in artificial intelligence research and the growth of virtual worlds it might well be that in twenty to forty years time, artificial agents will bring (virtual) criminals before professor van den Herik's artificial judge. Fortunately, the important work professor van den Herik has undertaken in the field of artificial intelligence and the law provides the basis for both effective law enforcement in virtual worlds as well as a responsible use of intelligent systems in virtual worlds.

References

1. Branch, P. (2003). Lawful Interception of IP Traffic, Swinburn University of Technology.
2. Herik, H.J. van den (1991). Kunnen Computers *Recht*spreken?, Inaugurele reden Leiden, Arnhem: Gouda Quint.
3. Kemal, D.A., Dayal, U. (2006). AI Re-emerging as Research Into Complex Systems, *Ubiquity*, Volume 7, Issue 38.
4. Kokswijk, van, J. (2003). *Architectuur van een Cybercultuur*, proefschrift Universiteit Twente.
5. Kurzweil, R. (2005). *The Singularity is Near: When Humans Transcend Biology*, New York: Viking.
6. Lodder, A. et al. (ed.) (2006). *Recht in een Virtuele Wereld, Juridische Aspecten van Massive Multiplayer Online Roleplaying Games*, Elsevier Juridisch.
7. Luck, M., Ashri R., D'Iverno M. (2004), *Agent-based Software Development*, Norwoord: ArtechHouse Inc.
8. Schafer, B., Rodriguez-Rico, M., VandenBerghe, W. (2004). *Undercover Agents and Agents Provocateur; Evidence Collection by Autonomous Agents and the Law*, in: Proceedings of the workshop on the Law of Electronic Agents (LEA04), 2004.
9. Schermer, B. W., Durinck, M., Bijmans, L. (2005). *Juridische Aspecten van Autonome Systemen*, Leidschendam: ECP.NL.
10. Schermer, B. W. (2007). *Software Agents, Surveillance, and the Right to Privacy: a Legislative Framework for Agent-enabled Surveillance*, Leiden: Leiden University Press.
11. Turing, A. (1950). Computing Machinery and Intelligence. *Mind*, 59, pp. 4333–460.
12. Viersma, M., Keupink, B. J. V. (2006). Virtuele Criminaliteit: All in the Game. In: Lodder, A. (2006). Recht in een Virtuele Wereld, Juridische Aspecten van Massive Multiplayer Online Roleplaying Games. Elsevier Juridisch.